Reasoning Model for Bot Detection

Interim Report

February 2009

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

Executive Summary

This report describes the preliminary bayesian network model for bot detection. This model is derived from the base rules currently embedded in the HBGary Responder product v1.2. The model described in this report was implemented and tested using the Netica software application. Future versions of the model will be implemented in C and compiled as a DLL for deployment. The API for this model is described in a separate document, "Reasoning Model API".

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

Model Structure

A Bayesian Network model consists of nodes, directed arcs which connect the nodes, and probability tables which represent the influence of each arc (i.e., the influence of the different states of one node on the states of a connected node). The preliminary bot detection model consists of one root node (Bot probability), 14 intermediate nodes which represent different classes of bot-related (malicious) activity, and 59 nodes representing specific bot indicators based on the base rules of HBGary Responder v1.2. The indicator nodes may be considered *input* nodes and the root node as the *output* node. These 74 nodes are connected by 83 arcs and associated probability tables containing 1,322 probability entries. The location of the arcs (node links) were determined by considering which indicators are associated with which malicious activity items. The model structure is shown in Figure 1, and the links between malicious activity items and indicators is summarized in Table 1 (nodes which are linked have a black circle in the corresponding cell). The probability tables for this model are listed in Appendix A, and the Netica source code for the model is in Appendix B.

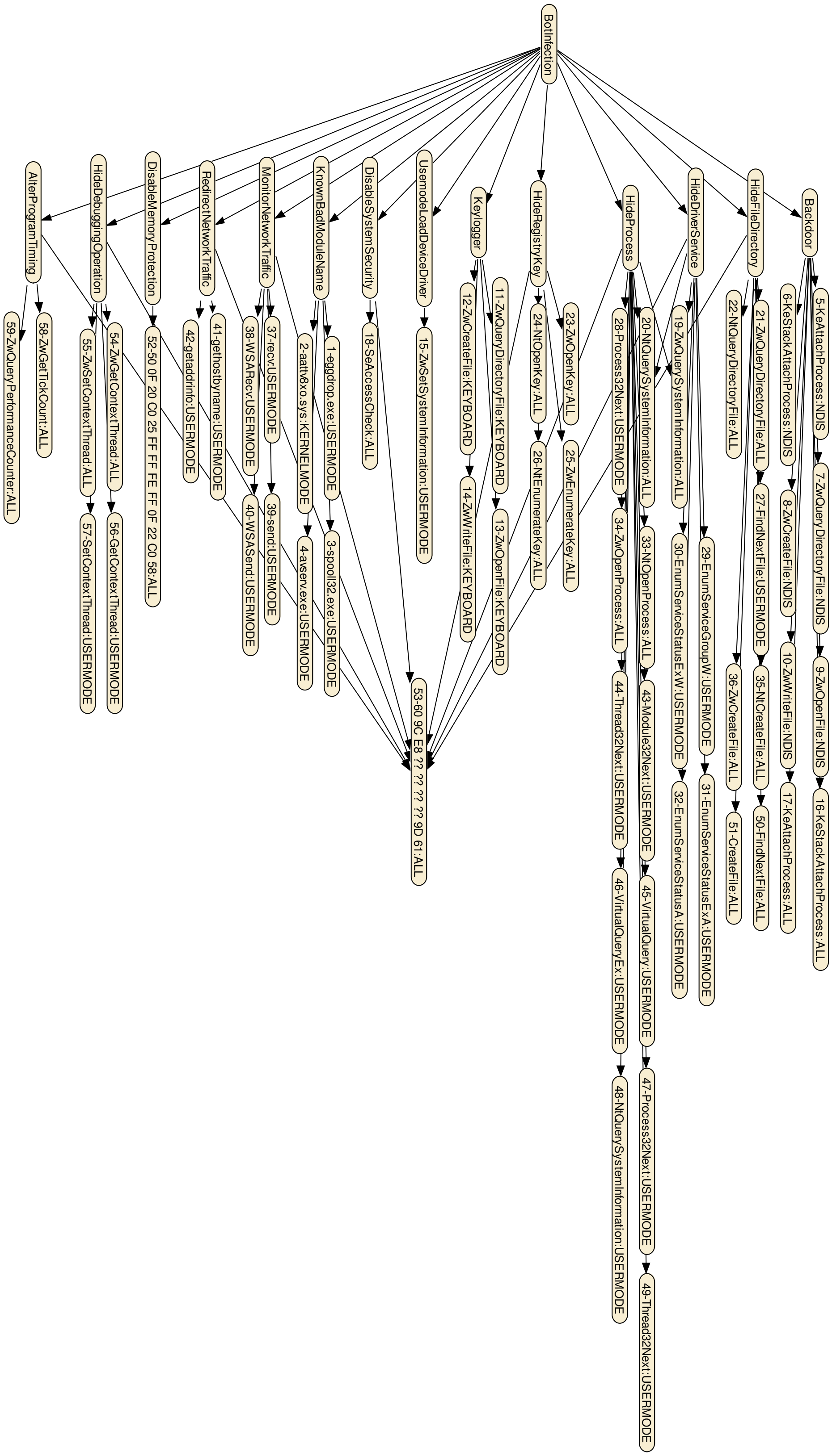
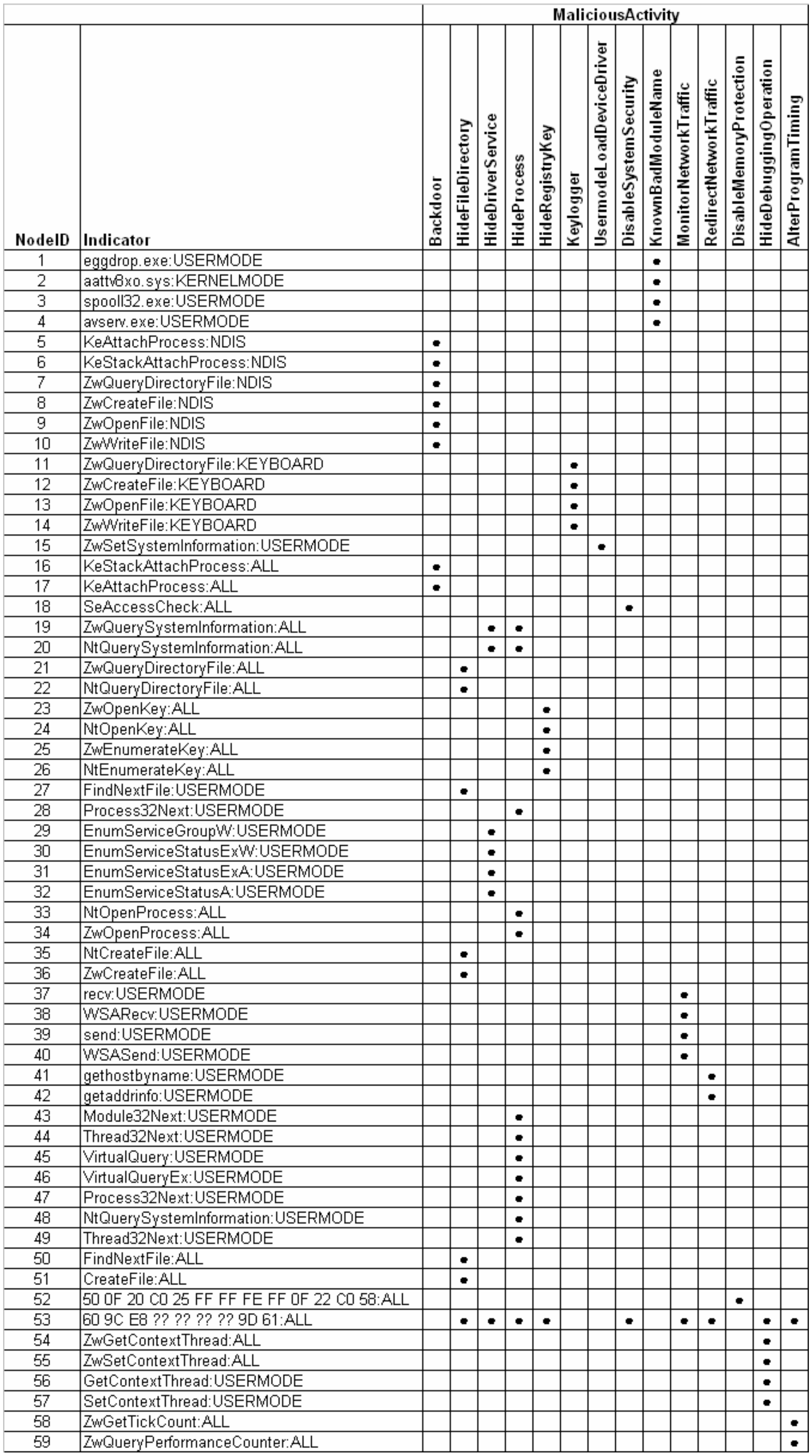


Figure 1: Bayesian Network Structure



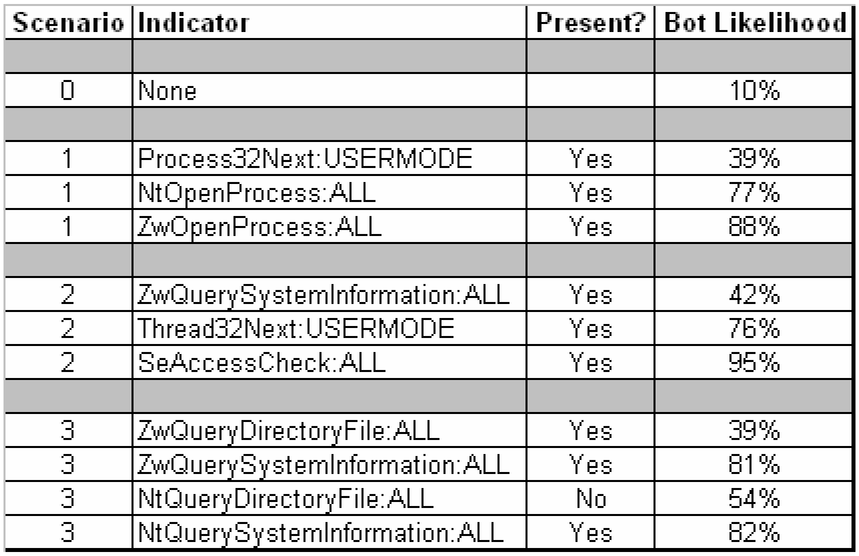
		MaliciousActivity													
NodeID	Indicator	Backdoor	HideFileDirectory	HideDriverService	HideProcess	HideRegistryKey	Keylogger	UsermodeLoadDeviceDriver	DisableSystemSecurity	KnownBadModuleName	MonitorNetworkTraffic	RedirectNetworkTraffic	DisableMemoryProtection	HideDebuggingOperation	AlterProgramTiming
1	eggdrop.exe:USERMODE									•					
2	aattv8xo.sys:KERNELMODE									•					
3	spooll32.exe:USERMODE									•					
4	avserv.exe:USERMODE									•					
5	KeAttachProcess:NDIS	•													
6	KeStackAttachProcess:NDIS	•													
7	ZwQueryDirectoryFile:NDIS	•													
8	ZwCreateFile:NDIS	•													
9	ZwOpenFile:NDIS	•													
10	ZwWriteFile:NDIS	•													
11	ZwQueryDirectoryFile:KEYBOARD						•								
12	ZwCreateFile:KEYBOARD						•								
13	ZwOpenFile:KEYBOARD						•								
14	ZwWriteFile:KEYBOARD						•								
15	ZwSetSystemInformation:USERMODE							•							
16	KeStackAttachProcess:ALL	•													
17	KeAttachProcess:ALL	•													
18	SeAccessCheck:ALL								•						
19	ZwQuerySystemInformation:ALL			•	•										
20	NtQuerySystemInformation:ALL			•	•										
21	ZwQueryDirectoryFile:ALL		•												
22	NtQueryDirectoryFile:ALL		•												
23	ZwOpenKey:ALL					•									
24	NtOpenKey:ALL					•									
25	ZwEnumerateKey:ALL					•									
26	NtEnumerateKey:ALL					•									
27	FindNextFile:USERMODE		•												
28	Process32Next:USERMODE				•										
29	EnumServiceGroupW:USERMODE			•											
30	EnumServiceStatusExW:USERMODE			•											
31	EnumServiceStatusExA:USERMODE			•											
32	EnumServiceStatusA:USERMODE			•											
33	NtOpenProcess:ALL				•										
34	ZwOpenProcess:ALL				•										
35	NtCreateFile:ALL		•												
36	ZwCreateFile:ALL		•												
37	recv:USERMODE										•				
38	WSARecv:USERMODE										•				
39	send:USERMODE										•				
40	WSASend:USERMODE										•				
41	gethostbyname:USERMODE											•			
42	getaddrinfo:USERMODE											•			
43	Module32Next:USERMODE				•										
44	Thread32Next:USERMODE				•										
45	VirtualQuery:USERMODE				•										
46	VirtualQueryEx:USERMODE				•										
47	Process32Next:USERMODE				•										
48	NtQuerySystemInformation:USERMODE				•										
49	Thread32Next:USERMODE				•										
50	FindNextFile:ALL		•												
51	CreateFile:ALL		•												
52	50 0F 20 C0 25 FF FF FE FF 0F 22 C0 58:ALL												•		
53	60 9C E8 ?? ?? ?? ?? 9D 61:ALL		•	•	•	•			•		•	•		•	•
54	ZwGetContextThread:ALL													•	
55	ZwSetContextThread:ALL													•	
56	GetContextThread:USERMODE													•	
57	SetContextThread:USERMODE													•	
58	ZwGetTickCount:ALL														•
59	ZwQueryPerformanceCounter:ALL														•

Table 1: Summary of Network Links for Layers 1 and 2

Examples

The use case for the model is to input one or more indicators as *present* or *not present*, then to query the root node for the current likelihood that the system in question has a bot infection. The model is designed to indicate whether a single system is infected with a bot or not. The model implementation and associated API are built such that multiple models (for different systems) may be run in parallel. The implementation also supports persistent models so that indicators may be entered over time and the output node queried as needed.

To provide some idea of the model's behavior, several sample scenarios are summarized in Table 2. The first entry represents the probability of a bot prior to the input of any indicator knowledge. The remaining entries summarize scenarios where one or more indicators are known to be present or not. For each scenario, the model begins with no indicators set. The root node is queried after each indicator is input, so that the running P(bot) can be seen. The Bot Likelihood is cumulative within each scenario.



Scenario	Indicator	Present?	Bot Likelihood
0	None		10%
1	Process32Next:USERMODE	Yes	39%
1	NtOpenProcess:ALL	Yes	77%
1	ZwOpenProcess:ALL	Yes	88%
2	ZwQuerySystemInformation:ALL	Yes	42%
2	Thread32Next:USERMODE	Yes	76%
2	SeAccessCheck:ALL	Yes	95%
3	ZwQueryDirectoryFile:ALL	Yes	39%
3	ZwQuerySystemInformation:ALL	Yes	81%
3	NtQueryDirectoryFile:ALL	No	54%
3	NtQuerySystemInformation:ALL	Yes	82%

Table 2: Sample Scenarios

Ongoing Work

Probability Tables. The current probability table values are generic, mostly indicating partial influence in the negative or positive direction. Work is ongoing to collect frequency data for known bots and indicators. This data will be used to refine the values in the model's probability tables.

C Code. The model is being converted to compiled C code which will be packaged as a DLL for implementation. An associated test wrapper is being developed as well.

Indicators. Additional indicators (beyond the base rules) have been researched. These are being incorporated in the frequency tests and will be included as we revise the model.

Appendix A: Model Probability Tables

BotInfection:

Yes	No
0.1	0.9

HideDriverService:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_29:

Present	Absent	HideDriverService
0.8	0.2	Yes
0.1	0.9	No

ID_30:

Present	Absent	HideDriverService
0.8	0.2	Yes
0.1	0.9	No

ID_31:

Present	Absent	HideDriverService
0.8	0.2	Yes
0.1	0.9	No

ID_32:

Present	Absent	HideDriverService
0.8	0.2	Yes
0.1	0.9	No

AlterProgramTiming:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_58:

Present	Absent	AlterProgramTiming
0.8	0.2	Yes

0.1	0.9	No

ID_59:

Present	Absent	AlterProgramTiming
0.8	0.2	Yes
0.1	0.9	No

HideDebuggingOperation:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_54:

Present	Absent	HideDebuggingOperation
0.8	0.2	Yes
0.1	0.9	No

ID_55:

Present	Absent	HideDebuggingOperation
0.8	0.2	Yes
0.1	0.9	No

ID_56:

Present	Absent	HideDebuggingOperation
0.8	0.2	Yes
0.1	0.9	No

ID_57:

Present	Absent	HideDebuggingOperation
0.8	0.2	Yes
0.1	0.9	No

DisableMemoryProtection:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_52:

Present	Absent	DisableMemoryProtection
0.8	0.2	Yes
0.1	0.9	No

RedirectNetworkTraffic:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_41:

Present	Absent	RedirectNetworkTraffic
0.8	0.2	Yes
0.1	0.9	No

ID_42:

Present	Absent	RedirectNetworkTraffic
0.8	0.2	Yes
0.1	0.9	No

MonitorNetworkTraffic:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_37:

Present	Absent	MonitorNetworkTraffic
0.8	0.2	Yes
0.1	0.9	No

ID_38:

Present	Absent	MonitorNetworkTraffic
0.8	0.2	Yes
0.1	0.9	No

ID_39:

Present	Absent	MonitorNetworkTraffic
0.8	0.2	Yes
0.1	0.9	No

ID_40:

Present	Absent	MonitorNetworkTraffic
0.8	0.2	Yes
0.1	0.9	No

KnownBadModuleName:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_1:

Present	Absent	KnownBadModuleName
0.25	0.75	Yes
0	1	No

ID_2:

Present	Absent	KnownBadModuleName
0.25	0.75	Yes
0	1	No

ID_3:

Present	Absent	KnownBadModuleName
0.25	0.75	Yes
0	1	No

ID_4:

Present	Absent	KnownBadModuleName
0.25	0.75	Yes
0	1	No

DisableSystemSecurity:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_18:

Present	Absent	DisableSystemSecurity
0.8	0.2	Yes

0.1	0.9	No

UsermodeLoadDeviceDriver:

Yes	No	BotInfection
0.1	0.9	Yes
0.1	0.9	No

ID_15:

Present	Absent	UsermodeLoadDeviceDriver
0.8	0.2	Yes
0.1	0.9	No

ID_11:

Present	Absent	Keylogger
0.8	0.2	Yes
0.1	0.9	No

ID_12:

Present	Absent	Keylogger
0.8	0.2	Yes
0.1	0.9	No

ID_13:

Present	Absent	Keylogger
0.8	0.2	Yes
0.1	0.9	No

ID_14:

Present	Absent	Keylogger
0.8	0.2	Yes
0.1	0.9	No

Keylogger:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_28:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_23:

Present	Absent	HideRegistryKey
0.8	0.2	Yes
0.1	0.9	No

ID_24:

Present	Absent	HideRegistryKey
0.8	0.2	Yes
0.1	0.9	No

ID_25:

Present	Absent	HideRegistryKey
0.8	0.2	Yes
0.1	0.9	No

ID_26:

Present	Absent	HideRegistryKey
0.8	0.2	Yes
0.1	0.9	No

HideRegistryKey:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_33:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_43:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_45:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_47:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_49:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_34:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_44:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_46:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

ID_48:

Present	Absent	HideProcess
0.8	0.2	Yes
0.1	0.9	No

HideProcess:

Yes	No	BotInfection
0.75	0.25	Yes

0.01	0.99	No

ID_20:

Present	Absent	HideDriverService	HideProcess
0.8	0.2	Yes	Yes
0.8	0.2	Yes	No
0.8	0.2	No	Yes
0.1	0.9	No	No

ID_19:

Present	Absent	HideDriverService	HideProcess
0.8	0.2	Yes	Yes
0.8	0.2	Yes	No
0.8	0.2	No	Yes
0.1	0.9	No	No

[... too big to print ...]

HideFileDirectory:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_21:

Present	Absent	HideFileDirectory
0.8	0.2	Yes
0.1	0.9	No

ID_22:

Present	Absent	HideFileDirectory
0.8	0.2	Yes
0.1	0.9	No

ID_27:

Present	Absent	HideFileDirectory
0.8	0.2	Yes
0.1	0.9	No

ID_35:

Present	Absent	HideFileDirectory
0.8	0.2	Yes
0.1	0.9	No

ID_36:

Present	Absent	HideFileDirectory
0.8	0.2	Yes
0.1	0.9	No

ID_50:

Present	Absent	HideFileDirectory
0.8	0.2	Yes
0.1	0.9	No

ID_51:

Present	Absent	HideFileDirectory
0.8	0.2	Yes
0.1	0.9	No

Backdoor:

Yes	No	BotInfection
0.75	0.25	Yes
0.01	0.99	No

ID_5:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

ID_6:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

ID_7:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

ID_8:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

ID_9:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

ID_10:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

ID_16:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

ID_17:

Present	Absent	Backdoor
0.8	0.2	Yes
0.1	0.9	No

Appendix B: Netica Model Source Code

```
// ~->[DNET-1]->~

// File created by JonesJ at SAIC using Netica 3.24

bnet BN_Model_ver1D7 {
AutoCompile = TRUE;
autoupdate = TRUE;
whenchanged = 1237928409;

visual V1 {
	defdispform = BELIEFBARS;
	nodelabeling = TITLE;
	NodeMaxNumEntries = 50;
	nodefont = font {shape= "Arial"; size= 10;};
	linkfont = font {shape= "Arial"; size= 9;};
	windowposn = (0, -1, 1003, 654);
	resolution = 72;
	magnification = 0.5;
	drawingbounds = (2837, 1819);
	showpagebreaks = FALSE;
	usegrid = TRUE;
	gridspace = (6, 6);
	NodeSet Node {BuiltIn = 1; Color = 0xc0c0c0;};
	NodeSet Nature {BuiltIn = 1; Color = 0xf8eed2;};
	NodeSet Deterministic {BuiltIn = 1; Color = 0xd3caa6;};
	NodeSet Finding {BuiltIn = 1; Color = 0xc8c8c8;};
	NodeSet Constant {BuiltIn = 1; Color = 0xffffff;};
	NodeSet ConstantValue {BuiltIn = 1; Color = 0xffffb4;};
	NodeSet Utility {BuiltIn = 1; Color = 0xffbdbd;};
	NodeSet Decision {BuiltIn = 1; Color = 0xdee8ff;};
	NodeSet Documentation {BuiltIn = 1; Color = 0xf0fafa;};
	NodeSet Title {BuiltIn = 1; Color = 0xffffff;};
	PrinterSetting A {
		margins = (1270, 1270, 1270, 1270);
		landscape = FALSE;
		magnify = 1;
		};
	};

node BotInfection {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Yes, No);
	parents = ();
	probs = 
		// Yes          No
		  (0.1,         0.9);
	title = "BotInfection";
	whenchanged = 1237885943;
	belief = (0.1, 0.9);
	visual V1 {
		center = (79, 186);
		dispform = BELIEFBARS;
```

```
            height = 1;
            };
      };

node Backdoor {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs =
            // Yes          No             // BotInfection
             ((0.75,        0.25),         // Yes
              (0.01,        0.99));        // No           ;
      numcases = 1;
      title = "Backdoor";
      whenchanged = 1237886220;
      belief = (0.084, 0.916);
      visual V1 {
            center = (288, 60);
            dispform = LABELBOX;
            height = 66;
            };
      };

node HideFileDirectory {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs =
            // Yes          No             // BotInfection
             ((0.75,        0.25),         // Yes
              (0.01,        0.99));        // No           ;
      numcases = 1;
      title = "HideFileDirectory";
      whenchanged = 1237886233;
      belief = (0.084, 0.916);
      visual V1 {
            center = (282, 138);
            dispform = LABELBOX;
            height = 58;
            };
      };

node HideDriverService {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs =
            // Yes          No             // BotInfection
             ((0.75,        0.25),         // Yes
              (0.01,        0.99));        // No           ;
      numcases = 1;
```

```
        title = "HideDriverService";
        whenchanged = 1237886239;
        belief = (0.084, 0.916);
        visual V1 {
              center = (270, 222);
              dispform = LABELBOX;
              height = 2;
              };
        };

  node HideProcess {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Yes, No);
        parents = (BotInfection);
        probs =
              // Yes           No              // BotInfection
               ((0.75,         0.25),          // Yes
                (0.01,         0.99));         // No           ;
        numcases = 1;
        title = "HideProcess";
        whenchanged = 1237886263;
        belief = (0.084, 0.916);
        visual V1 {
              center = (276, 462);
              dispform = LABELBOX;
              height = 54;
              };
        };

  node HideRegistryKey {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Yes, No);
        parents = (BotInfection);
        probs =
              // Yes           No              // BotInfection
               ((0.75,         0.25),          // Yes
                (0.01,         0.99));         // No           ;
        numcases = 1;
        title = "HideRegistryKey";
        whenchanged = 1237886271;
        belief = (0.084, 0.916);
        visual V1 {
              center = (288, 564);
              dispform = LABELBOX;
              height = 44;
              };
        };

  node Keylogger {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Yes, No);
```

```
      parents = (BotInfection);
      probs = 
            // Yes          No             // BotInfection
             ((0.75,        0.25),         // Yes
              (0.01,        0.99));        // No          ;
      numcases = 1;
      title = "Keylogger";
      whenchanged = 1237886277;
      belief = (0.084, 0.916);
      visual V1 {
            center = (300, 630);
            dispform = LABELBOX;
            height = 38;
            };
      };

node UsermodeLoadDeviceDriver {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs = 
            // Yes          No             // BotInfection
             ((0.1,         0.9),          // Yes
              (0.1,         0.9));         // No          ;
      numcases = 1;
      title = "UsemodeLoadDeviceDriver";
      whenchanged = 1237886282;
      belief = (0.1, 0.9);
      visual V1 {
            center = (258, 708);
            dispform = LABELBOX;
            height = 32;
            };
      };

node DisableSystemSecurity {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs = 
            // Yes          No             // BotInfection
             ((0.75,        0.25),         // Yes
              (0.01,        0.99));        // No          ;
      numcases = 1;
      title = "DisableSystemSecurity";
      whenchanged = 1237886289;
      belief = (0.084, 0.916);
      visual V1 {
            center = (258, 780);
            dispform = LABELBOX;
            height = 30;
            };
      };
```

```
node KnownBadModuleName {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs =
            // Yes          No              // BotInfection
             ((0.75,        0.25),          // Yes
              (0.01,        0.99));         // No            ;
      numcases = 1;
      title = "KnownBadModuleName";
      whenchanged = 1237886295;
      belief = (0.084, 0.916);
      visual V1 {
            center = (264, 852);
            dispform = LABELBOX;
            height = 25;
            };
      };

node MonitorNetworkTraffic {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs =
            // Yes          No              // BotInfection
             ((0.75,        0.25),          // Yes
              (0.01,        0.99));         // No            ;
      numcases = 1;
      title = "MonitorNetworkTraffic";
      whenchanged = 1237886301;
      belief = (0.084, 0.916);
      visual V1 {
            center = (264, 924);
            dispform = LABELBOX;
            height = 20;
            };
      };

node RedirectNetworkTraffic {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Yes, No);
      parents = (BotInfection);
      probs =
            // Yes          No              // BotInfection
             ((0.75,        0.25),          // Yes
              (0.01,        0.99));         // No            ;
      numcases = 1;
      title = "RedirectNetworkTraffic";
      whenchanged = 1237886308;
      belief = (0.084, 0.916);
```

```
	visual V1 {
		center = (270, 1002);
		dispform = LABELBOX;
		height = 17;
		};
	};

node DisableMemoryProtection {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Yes, No);
	parents = (BotInfection);
	probs = 
		// Yes          No              // BotInfection
		 ((0.75,        0.25),          // Yes
		  (0.01,        0.99));         // No           ;
	numcases = 1;
	title = "DisableMemoryProtection";
	whenchanged = 1237886313;
	belief = (0.084, 0.916);
	visual V1 {
		center = (246, 1068);
		dispform = LABELBOX;
		height = 15;
		};
	};

node HideDebuggingOperation {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Yes, No);
	parents = (BotInfection);
	probs = 
		// Yes          No              // BotInfection
		 ((0.75,        0.25),          // Yes
		  (0.01,        0.99));         // No           ;
	numcases = 1;
	title = "HideDebuggingOperation";
	whenchanged = 1237886319;
	belief = (0.084, 0.916);
	visual V1 {
		center = (264, 1140);
		dispform = LABELBOX;
		height = 10;
		};
	};

node AlterProgramTiming {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Yes, No);
	parents = (BotInfection);
	probs = 
		// Yes          No              // BotInfection
```

```
                ((0.75,         0.25),          // Yes
                 (0.01,         0.99));         // No            ;
        numcases = 1;
        title = "AlterProgramTiming";
        whenchanged = 1237886325;
        belief = (0.084, 0.916);
        visual V1 {
              center = (276, 1218);
              dispform = LABELBOX;
              height = 7;
              };
        };

node ID_5 {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Present, Absent);
        parents = (Backdoor);
        probs =
              // Present      Absent          // Backdoor
               ((0.8,         0.2),           // Yes
                (0.1,         0.9));          // No       ;
        title = "5-KeAttachProcess:NDIS\n";
        whenchanged = 1237926880;
        belief = (0.1588, 0.8412);
        visual V1 {
              center = (444, 60);
              dispform = BELIEFBARS;
              height = 67;
              };
        };

node ID_6 {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Present, Absent);
        parents = (Backdoor);
        probs =
              // Present      Absent          // Backdoor
               ((0.8,         0.2),           // Yes
                (0.1,         0.9));          // No       ;
        title = "6-KeStackAttachProcess:NDIS\n";
        whenchanged = 1237884137;
        belief = (0.1588, 0.8412);
        visual V1 {
              center = (666, 60);
              dispform = BELIEFBARS;
              height = 68;
              };
        };

node ID_7 {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
```

```
      states = (Present, Absent);
      parents = (Backdoor);
      probs = 
            // Present      Absent         // Backdoor
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No       ;
      title = "7-ZwQueryDirectoryFile:NDIS\n";
      whenchanged = 1237884139;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (900, 60);
            dispform = BELIEFBARS;
            height = 69;
            };
      };

node ID_8 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (Backdoor);
      probs = 
            // Present      Absent         // Backdoor
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No       ;
      title = "8-ZwCreateFile:NDIS\n";
      whenchanged = 1237884141;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1104, 60);
            dispform = BELIEFBARS;
            height = 70;
            };
      };

node ID_9 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (Backdoor);
      probs = 
            // Present      Absent         // Backdoor
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No       ;
      title = "9-ZwOpenFile:NDIS\n";
      whenchanged = 1237884143;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1290, 60);
            dispform = BELIEFBARS;
            height = 71;
            };
      };

node ID_10 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (Backdoor);
	probs = 
		// Present      Absent          // Backdoor
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No       ;
	title = "10-ZwWriteFile:NDIS\n";
	whenchanged = 1237884146;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (1476, 60);
		dispform = BELIEFBARS;
		height = 72;
		};
	};

node ID_16 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (Backdoor);
	probs = 
		// Present      Absent          // Backdoor
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No       ;
	title = "16-KeStackAttachProcess:ALL\n";
	whenchanged = 1237884353;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (1692, 60);
		dispform = BELIEFBARS;
		height = 73;
		};
	};

node ID_17 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (Backdoor);
	probs = 
		// Present      Absent          // Backdoor
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No       ;
	title = "17-KeAttachProcess:ALL\n";
	whenchanged = 1237884357;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (1908, 60);
		dispform = BELIEFBARS;
		height = 74;
		};
	};

node ID_21 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideFileDirectory);
	probs =
		// Present      Absent          // HideFileDirectory
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No                ;
	title = "21-ZwQueryDirectoryFile:ALL\n";
	whenchanged = 1237885292;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (462, 138);
		dispform = BELIEFBARS;
		height = 59;
		};
	};

node ID_22 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideFileDirectory);
	probs =
		// Present      Absent          // HideFileDirectory
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No                ;
	title = "22-NtQueryDirectoryFile:ALL\n";
	whenchanged = 1237885293;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (690, 138);
		dispform = BELIEFBARS;
		height = 60;
		};
	};

node ID_27 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideFileDirectory);
	probs =
		// Present      Absent          // HideFileDirectory
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No                ;
	title = "27-FindNextFile:USERMODE\n";
	whenchanged = 1237885324;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (918, 138);
```

```
			dispform = BELIEFBARS;
			height = 61;
			};
		};

	node ID_35 {
		kind = NATURE;
		discrete = TRUE;
		chance = CHANCE;
		states = (Present, Absent);
		parents = (HideFileDirectory);
		probs = 
			// Present      Absent         // HideFileDirectory
			 ((0.8,         0.2),          // Yes
			  (0.1,         0.9));         // No                ;
		title = "35-NtCreateFile:ALL\n";
		whenchanged = 1237885433;
		belief = (0.1588, 0.8412);
		visual V1 {
			center = (1128, 138);
			dispform = BELIEFBARS;
			height = 62;
			};
		};

	node ID_36 {
		kind = NATURE;
		discrete = TRUE;
		chance = CHANCE;
		states = (Present, Absent);
		parents = (HideFileDirectory);
		probs = 
			// Present      Absent         // HideFileDirectory
			 ((0.8,         0.2),          // Yes
			  (0.1,         0.9));         // No                ;
		title = "36-ZwCreateFile:ALL\n";
		whenchanged = 1237885435;
		belief = (0.1588, 0.8412);
		visual V1 {
			center = (1320, 138);
			dispform = BELIEFBARS;
			height = 63;
			};
		};

	node ID_50 {
		kind = NATURE;
		discrete = TRUE;
		chance = CHANCE;
		states = (Present, Absent);
		parents = (HideFileDirectory);
		probs = 
			// Present      Absent         // HideFileDirectory
			 ((0.8,         0.2),          // Yes
			  (0.1,         0.9));         // No                ;
		title = "50-FindNextFile:ALL\n";
		whenchanged = 1237885658;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (1512, 138);
		dispform = BELIEFBARS;
		height = 64;
		};
	};

node ID_51 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideFileDirectory);
	probs = 
		// Present      Absent          // HideFileDirectory 
		 ((0.8,         0.2),           // Yes               
		  (0.1,         0.9));          // No                ;
	title = "51-CreateFile:ALL\n";
	whenchanged = 1237885658;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (1704, 138);
		dispform = BELIEFBARS;
		height = 65;
		};
	};

node ID_53 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideFileDirectory, HideDriverService, HideProcess, 
HideRegistryKey, DisableSystemSecurity, MonitorNetworkTraffic, 
RedirectNetworkTraffic, HideDebuggingOperation, AlterProgramTiming);
	probs = 
		//        Present      Absent                 // 
HideFileDirectory HideDriverService HideProcess HideRegistryKey 
DisableSystemSecurity MonitorNetworkTraffic RedirectNetworkTraffic 
HideDebuggingOperation AlterProgramTiming 
		(((((((((0.8,        0.2),                    // Yes               
Yes               Yes         Yes              Yes                   Yes                   
Yes                    Yes                   Yes                    
		         (0.8,        0.2)),                  // Yes               
Yes               Yes         Yes              Yes                   Yes                   
Yes                    Yes                   No                     
		        ((0.8,        0.2),                   // Yes               
Yes               Yes         Yes              Yes                   Yes                   
Yes                    No                    Yes                    
		         (0.8,        0.2))),                 // Yes               
Yes               Yes         Yes              Yes                   Yes                   
Yes                    No                    No                     
		       (((0.8,        0.2),                   // Yes               
Yes               Yes         Yes              Yes                   Yes                   
No                     Yes                   Yes                    
```

```
                      (0.8,         0.2)),                  // Yes
Yes                Yes         Yes              Yes                   Yes
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
Yes                Yes         Yes              Yes                   Yes
No                      No                      Yes
                      (0.8,         0.2)))),                // Yes
Yes                Yes         Yes              Yes                   Yes
No                      No                      No
                   ((((0.8,         0.2),                   // Yes
Yes                Yes         Yes              Yes                   No
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
Yes                Yes         Yes              Yes                   No
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
Yes                Yes         Yes              Yes                   No
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
Yes                Yes         Yes              Yes                   No
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
Yes                Yes         Yes              Yes                   No
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
Yes                Yes         Yes              Yes                   No
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
Yes                Yes         Yes              Yes                   No
No                      No                      Yes
                      (0.8,         0.2))))),               // Yes
Yes                Yes         Yes              Yes                   No
No                      No                      No
                  (((((0.8,         0.2),                   // Yes
Yes                Yes         Yes              No                    Yes
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
Yes                Yes         Yes              No                    Yes
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
Yes                Yes         Yes              No                    Yes
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
Yes                Yes         Yes              No                    Yes
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
Yes                Yes         Yes              No                    Yes
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
Yes                Yes         Yes              No                    Yes
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
Yes                Yes         Yes              No                    Yes
No                      No                      Yes
                      (0.8,         0.2)))),                // Yes
Yes                Yes         Yes              No                    Yes
No                      No                      No
```

```
                  ((((0.8,         0.2),                  // Yes
Yes               Yes         Yes             No                    No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         Yes             No                    No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         Yes             No                    No
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               Yes         Yes             No                    No
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               Yes         Yes             No                    No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         Yes             No                    No
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         Yes             No                    No
No                     No                     Yes
                     (0.8,         0.2)))))),             // Yes
Yes               Yes         Yes             No                    No
No                     No                     No
                ((((((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              Yes                   Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               Yes         No              Yes                   Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              Yes                   Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // Yes
Yes               Yes         No              Yes                   Yes
No                     No                     No
                  ((((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              Yes                   No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   No
Yes                    No                     Yes
```

```
                     (0.8,         0.2))),                // Yes
Yes               Yes         No              Yes                   No
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              Yes                   No
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         No              Yes                   No
No                     No                     Yes
                     (0.8,         0.2))))),              // Yes
Yes               Yes         No              Yes                   No
No                     No                     No
                 (((((0.8,         0.2),                  // Yes
Yes               Yes         No              No                    Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         No              No                    Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               Yes         No              No                    Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               Yes         No              No                    Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              No                    Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         No              No                    Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // Yes
Yes               Yes         No              No                    Yes
No                     No                     No
                  ((((0.8,         0.2),                  // Yes
Yes               Yes         No              No                    No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              No                    No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               Yes         No              No                    No
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               Yes         No              No                    No
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               Yes         No              No                    No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               Yes         No              No                    No
No                     Yes                    No
```

```
                     ((0.8,          0.2),                    // Yes
Yes                Yes          No               No                     No
No                      No                       Yes
                      (0.8,          0.2))))))),              // Yes
Yes                Yes          No               No                     No
No                      No                       No
                ((((((((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    Yes
Yes                     Yes                      Yes
                      (0.8,          0.2)),                   // Yes
Yes                No           Yes              Yes                    Yes
Yes                     Yes                      No
                     ((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    Yes
Yes                     No                       Yes
                      (0.8,          0.2))),                  // Yes
Yes                No           Yes              Yes                    Yes
Yes                     No                       No
                    (((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    Yes
No                      Yes                      Yes
                      (0.8,          0.2)),                   // Yes
Yes                No           Yes              Yes                    Yes
No                      Yes                      No
                     ((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    Yes
No                      No                       Yes
                      (0.8,          0.2)))),                 // Yes
Yes                No           Yes              Yes                    Yes
No                      No                       No
                   ((((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    No
Yes                     Yes                      Yes
                      (0.8,          0.2)),                   // Yes
Yes                No           Yes              Yes                    No
Yes                     Yes                      No
                     ((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    No
Yes                     No                       Yes
                      (0.8,          0.2))),                  // Yes
Yes                No           Yes              Yes                    No
Yes                     No                       No
                    (((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    No
No                      Yes                      Yes
                      (0.8,          0.2)),                   // Yes
Yes                No           Yes              Yes                    No
No                      Yes                      No
                     ((0.8,          0.2),                    // Yes
Yes                No           Yes              Yes                    No
No                      No                       Yes
                      (0.8,          0.2))))),                // Yes
Yes                No           Yes              Yes                    No
No                      No                       No
                  (((((0.8,          0.2),                    // Yes
Yes                No           Yes              No                     Yes
Yes                     Yes                      Yes
```

```
                     (0.8,         0.2)),                 // Yes
Yes               No          Yes             No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          Yes             No                    Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               No          Yes             No                    Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               No          Yes             No                    Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          Yes             No                    Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          Yes             No                    Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // Yes
Yes               No          Yes             No                    Yes
No                     No                     No
                  ((((0.8,         0.2),                  // Yes
Yes               No          Yes             No                    No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          Yes             No                    No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          Yes             No                    No
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               No          Yes             No                    No
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               No          Yes             No                    No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          Yes             No                    No
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          Yes             No                    No
No                     No                     Yes
                     (0.8,         0.2)))))),             // Yes
Yes               No          Yes             No                    No
No                     No                     No
                ((((((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          No              Yes                   Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               No          No              Yes                   Yes
Yes                    No                     No
```

```
                   (((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          No              Yes                   Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // Yes
Yes               No          No              Yes                   Yes
No                     No                     No
                  ((((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          No              Yes                   No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   No
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               No          No              Yes                   No
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          No              Yes                   No
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          No              Yes                   No
No                     No                     Yes
                     (0.8,         0.2))))),              // Yes
Yes               No          No              Yes                   No
No                     No                     No
                 (((((0.8,         0.2),                  // Yes
Yes               No          No              No                    Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          No              No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          No              No                    Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
Yes               No          No              No                    Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
Yes               No          No              No                    Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
Yes               No          No              No                    Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
Yes               No          No              No                    Yes
No                     No                     Yes
```

```
                      (0.8,          0.2)))),                // Yes
Yes                No          No             No                     Yes
No                      No                      No
                   ((((0.8,          0.2),                   // Yes
Yes                No          No             No                     No
Yes                     Yes                     Yes
                      (0.8,          0.2)),                  // Yes
Yes                No          No             No                     No
Yes                     Yes                     No
                     ((0.8,          0.2),                   // Yes
Yes                No          No             No                     No
Yes                     No                      Yes
                      (0.8,          0.2))),                 // Yes
Yes                No          No             No                     No
Yes                     No                      No
                    (((0.8,          0.2),                   // Yes
Yes                No          No             No                     No
No                      Yes                     Yes
                      (0.8,          0.2)),                  // Yes
Yes                No          No             No                     No
No                      Yes                     No
                     ((0.8,          0.2),                   // Yes
Yes                No          No             No                     No
No                      No                      Yes
                      (0.8,          0.2)))))))),            // Yes
Yes                No          No             No                     No
No                      No                      No
               ((((((((0.8,          0.2),                   // Yes
No                 Yes         Yes            Yes                    Yes
Yes                     Yes                     Yes
                      (0.8,          0.2)),                  // Yes
No                 Yes         Yes            Yes                    Yes
Yes                     Yes                     No
                     ((0.8,          0.2),                   // Yes
No                 Yes         Yes            Yes                    Yes
Yes                     No                      Yes
                      (0.8,          0.2))),                 // Yes
No                 Yes         Yes            Yes                    Yes
Yes                     No                      No
                    (((0.8,          0.2),                   // Yes
No                 Yes         Yes            Yes                    Yes
No                      Yes                     Yes
                      (0.8,          0.2)),                  // Yes
No                 Yes         Yes            Yes                    Yes
No                      Yes                     No
                     ((0.8,          0.2),                   // Yes
No                 Yes         Yes            Yes                    Yes
No                      No                      Yes
                      (0.8,          0.2)))),                // Yes
No                 Yes         Yes            Yes                    Yes
No                      No                      No
                   ((((0.8,          0.2),                   // Yes
No                 Yes         Yes            Yes                    No
Yes                     Yes                     Yes
                      (0.8,          0.2)),                  // Yes
No                 Yes         Yes            Yes                    No
Yes                     Yes                     No
```

```
                    ((0.8,         0.2),                 // Yes
No                Yes         Yes             Yes                   No
Yes                    No                     Yes
                     (0.8,         0.2))),               // Yes
No                Yes         Yes             Yes                   No
Yes                    No                     No
                   (((0.8,         0.2),                 // Yes
No                Yes         Yes             Yes                   No
No                     Yes                    Yes
                     (0.8,         0.2)),                // Yes
No                Yes         Yes             Yes                   No
No                     Yes                    No
                    ((0.8,         0.2),                 // Yes
No                Yes         Yes             Yes                   No
No                     No                     Yes
                     (0.8,         0.2))))),             // Yes
No                Yes         Yes             Yes                   No
No                     No                     No
                 (((((0.8,         0.2),                 // Yes
No                Yes         Yes             No                    Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                // Yes
No                Yes         Yes             No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                 // Yes
No                Yes         Yes             No                    Yes
Yes                    No                     Yes
                     (0.8,         0.2))),               // Yes
No                Yes         Yes             No                    Yes
Yes                    No                     No
                   (((0.8,         0.2),                 // Yes
No                Yes         Yes             No                    Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                // Yes
No                Yes         Yes             No                    Yes
No                     Yes                    No
                    ((0.8,         0.2),                 // Yes
No                Yes         Yes             No                    Yes
No                     No                     Yes
                     (0.8,         0.2)))),              // Yes
No                Yes         Yes             No                    Yes
No                     No                     No
                  ((((0.8,         0.2),                 // Yes
No                Yes         Yes             No                    No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                // Yes
No                Yes         Yes             No                    No
Yes                    Yes                    No
                    ((0.8,         0.2),                 // Yes
No                Yes         Yes             No                    No
Yes                    No                     Yes
                     (0.8,         0.2))),               // Yes
No                Yes         Yes             No                    No
Yes                    No                     No
                   (((0.8,         0.2),                 // Yes
No                Yes         Yes             No                    No
No                     Yes                    Yes
```

```
                      (0.8,         0.2)),                  // Yes
No                 Yes         Yes              No                    No
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         Yes              No                    No
No                      No                      Yes
                      (0.8,         0.2)))))),              // Yes
No                 Yes         Yes              No                    No
No                      No                      No
                 ((((((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   Yes
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               Yes                   Yes
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   Yes
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
No                 Yes         No               Yes                   Yes
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   Yes
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               Yes                   Yes
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   Yes
No                      No                      Yes
                      (0.8,         0.2)))),                // Yes
No                 Yes         No               Yes                   Yes
No                      No                      No
                   ((((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   No
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               Yes                   No
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   No
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
No                 Yes         No               Yes                   No
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   No
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               Yes                   No
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               Yes                   No
No                      No                      Yes
                      (0.8,         0.2))))),               // Yes
No                 Yes         No               Yes                   No
No                      No                      No
```

```
                  (((((0.8,         0.2),                   // Yes
No                 Yes         No               No                     Yes
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               No                     Yes
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               No                     Yes
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
No                 Yes         No               No                     Yes
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
No                 Yes         No               No                     Yes
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               No                     Yes
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               No                     Yes
No                      No                      Yes
                      (0.8,         0.2)))),                // Yes
No                 Yes         No               No                     Yes
No                      No                      No
                   ((((0.8,         0.2),                   // Yes
No                 Yes         No               No                     No
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               No                     No
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               No                     No
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
No                 Yes         No               No                     No
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
No                 Yes         No               No                     No
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 Yes         No               No                     No
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 Yes         No               No                     No
No                      No                      Yes
                      (0.8,         0.2))))))),             // Yes
No                 Yes         No               No                     No
No                      No                      No
                (((((((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                    Yes
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 No          Yes              Yes                    Yes
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                    Yes
Yes                     No                      Yes
```

```
                      (0.8,         0.2))),                 // Yes
No                 No          Yes              Yes                   Yes
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                   Yes
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 No          Yes              Yes                   Yes
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                   Yes
No                      No                      Yes
                      (0.8,         0.2)))),                // Yes
No                 No          Yes              Yes                   Yes
No                      No                      No
                   ((((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                   No
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 No          Yes              Yes                   No
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                   No
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
No                 No          Yes              Yes                   No
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                   No
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 No          Yes              Yes                   No
No                      Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 No          Yes              Yes                   No
No                      No                      Yes
                      (0.8,         0.2))))),               // Yes
No                 No          Yes              Yes                   No
No                      No                      No
                  (((((0.8,         0.2),                   // Yes
No                 No          Yes              No                    Yes
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 No          Yes              No                    Yes
Yes                     Yes                     No
                     ((0.8,         0.2),                   // Yes
No                 No          Yes              No                    Yes
Yes                     No                      Yes
                      (0.8,         0.2))),                 // Yes
No                 No          Yes              No                    Yes
Yes                     No                      No
                    (((0.8,         0.2),                   // Yes
No                 No          Yes              No                    Yes
No                      Yes                     Yes
                      (0.8,         0.2)),                  // Yes
No                 No          Yes              No                    Yes
No                      Yes                     No
```

```
                    ((0.8,         0.2),                  // Yes
No                No          Yes             No                  Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // Yes
No                No          Yes             No                  Yes
No                     No                     No
                  ((((0.8,         0.2),                  // Yes
No                No          Yes             No                  No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
No                No          Yes             No                  No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
No                No          Yes             No                  No
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
No                No          Yes             No                  No
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
No                No          Yes             No                  No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
No                No          Yes             No                  No
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
No                No          Yes             No                  No
No                     No                     Yes
                     (0.8,         0.2)))))),             // Yes
No                No          Yes             No                  No
No                     No                     No
                ((((((0.8,         0.2),                  // Yes
No                No          No              Yes                 Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // Yes
No                No          No              Yes                 Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // Yes
No                No          No              Yes                 Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // Yes
No                No          No              Yes                 Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // Yes
No                No          No              Yes                 Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // Yes
No                No          No              Yes                 Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // Yes
No                No          No              Yes                 Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // Yes
No                No          No              Yes                 Yes
No                     No                     No
                  ((((0.8,         0.2),                  // Yes
No                No          No              Yes                 No
Yes                    Yes                    Yes
```

```
                      (0.8,         0.2)),                  // Yes
No                No           No              Yes                    No
Yes                     Yes                    No
                     ((0.8,         0.2),                   // Yes
No                No           No              Yes                    No
Yes                     No                     Yes
                      (0.8,         0.2))),                 // Yes
No                No           No              Yes                    No
Yes                     No                     No
                    (((0.8,         0.2),                   // Yes
No                No           No              Yes                    No
No                      Yes                    Yes
                      (0.8,         0.2)),                  // Yes
No                No           No              Yes                    No
No                      Yes                    No
                     ((0.8,         0.2),                   // Yes
No                No           No              Yes                    No
No                      No                     Yes
                      (0.8,         0.2))))),               // Yes
No                No           No              Yes                    No
No                      No                     No
                  (((((0.8,         0.2),                   // Yes
No                No           No              No                     Yes
Yes                     Yes                    Yes
                      (0.8,         0.2)),                  // Yes
No                No           No              No                     Yes
Yes                     Yes                    No
                     ((0.8,         0.2),                   // Yes
No                No           No              No                     Yes
Yes                     No                     Yes
                      (0.8,         0.2))),                 // Yes
No                No           No              No                     Yes
Yes                     No                     No
                    (((0.8,         0.2),                   // Yes
No                No           No              No                     Yes
No                      Yes                    Yes
                      (0.8,         0.2)),                  // Yes
No                No           No              No                     Yes
No                      Yes                    No
                     ((0.8,         0.2),                   // Yes
No                No           No              No                     Yes
No                      No                     Yes
                      (0.8,         0.2)))),                // Yes
No                No           No              No                     Yes
No                      No                     No
                   ((((0.8,         0.2),                   // Yes
No                No           No              No                     No
Yes                     Yes                    Yes
                      (0.8,         0.2)),                  // Yes
No                No           No              No                     No
Yes                     Yes                    No
                     ((0.8,         0.2),                   // Yes
No                No           No              No                     No
Yes                     No                     Yes
                      (0.8,         0.2))),                 // Yes
No                No           No              No                     No
Yes                     No                     No
```

```
                    (((0.8,          0.2),                   // Yes
No                 No           No               No                     No
No                      Yes                      Yes
                      (0.8,          0.2)),                  // Yes
No                 No           No               No                     No
No                      Yes                      No
                     ((0.8,          0.2),                   // Yes
No                 No           No               No                     No
No                      No                       Yes
                      (0.8,          0.2))))))))),           // Yes
No                 No           No               No                     No
No                      No                       No
               ((((((((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    Yes
Yes                     Yes                      Yes
                      (0.8,          0.2)),                  // No
Yes                Yes          Yes              Yes                    Yes
Yes                     Yes                      No
                     ((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    Yes
Yes                     No                       Yes
                      (0.8,          0.2))),                 // No
Yes                Yes          Yes              Yes                    Yes
Yes                     No                       No
                    (((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    Yes
No                      Yes                      Yes
                      (0.8,          0.2)),                  // No
Yes                Yes          Yes              Yes                    Yes
No                      Yes                      No
                     ((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    Yes
No                      No                       Yes
                      (0.8,          0.2)))),                // No
Yes                Yes          Yes              Yes                    Yes
No                      No                       No
                   ((((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    No
Yes                     Yes                      Yes
                      (0.8,          0.2)),                  // No
Yes                Yes          Yes              Yes                    No
Yes                     Yes                      No
                     ((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    No
Yes                     No                       Yes
                      (0.8,          0.2))),                 // No
Yes                Yes          Yes              Yes                    No
Yes                     No                       No
                    (((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    No
No                      Yes                      Yes
                      (0.8,          0.2)),                  // No
Yes                Yes          Yes              Yes                    No
No                      Yes                      No
                     ((0.8,          0.2),                   // No
Yes                Yes          Yes              Yes                    No
No                      No                       Yes
```

```
                     (0.8,         0.2))))),               // No
Yes               Yes         Yes              Yes                   No
No                     No                      No
                 (((((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    Yes
Yes                    Yes                     Yes
                     (0.8,         0.2)),                  // No
Yes               Yes         Yes              No                    Yes
Yes                    Yes                     No
                    ((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    Yes
Yes                    No                      Yes
                     (0.8,         0.2))),                 // No
Yes               Yes         Yes              No                    Yes
Yes                    No                      No
                   (((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    Yes
No                     Yes                     Yes
                     (0.8,         0.2)),                  // No
Yes               Yes         Yes              No                    Yes
No                     Yes                     No
                    ((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    Yes
No                     No                      Yes
                     (0.8,         0.2)))),                // No
Yes               Yes         Yes              No                    Yes
No                     No                      No
                  ((((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    No
Yes                    Yes                     Yes
                     (0.8,         0.2)),                  // No
Yes               Yes         Yes              No                    No
Yes                    Yes                     No
                    ((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    No
Yes                    No                      Yes
                     (0.8,         0.2))),                 // No
Yes               Yes         Yes              No                    No
Yes                    No                      No
                   (((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    No
No                     Yes                     Yes
                     (0.8,         0.2)),                  // No
Yes               Yes         Yes              No                    No
No                     Yes                     No
                    ((0.8,         0.2),                   // No
Yes               Yes         Yes              No                    No
No                     No                      Yes
                     (0.8,         0.2)))))),              // No
Yes               Yes         Yes              No                    No
No                     No                      No
                ((((((0.8,         0.2),                   // No
Yes               Yes         No               Yes                   Yes
Yes                    Yes                     Yes
                     (0.8,         0.2)),                  // No
Yes               Yes         No               Yes                   Yes
Yes                    Yes                     No
```

```
                    ((0.8,         0.2),                  // No
Yes               Yes         No              Yes                   Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
Yes               Yes         No              Yes                   Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               Yes         No              Yes                   Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               Yes         No              Yes                   Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // No
Yes               Yes         No              Yes                   Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // No
Yes               Yes         No              Yes                   Yes
No                     No                     No
                  ((((0.8,         0.2),                  // No
Yes               Yes         No              Yes                   No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               Yes         No              Yes                   No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
Yes               Yes         No              Yes                   No
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
Yes               Yes         No              Yes                   No
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               Yes         No              Yes                   No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               Yes         No              Yes                   No
No                     Yes                    No
                    ((0.8,         0.2),                  // No
Yes               Yes         No              Yes                   No
No                     No                     Yes
                     (0.8,         0.2))))),              // No
Yes               Yes         No              Yes                   No
No                     No                     No
                 (((((0.8,         0.2),                  // No
Yes               Yes         No              No                    Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               Yes         No              No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
Yes               Yes         No              No                    Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
Yes               Yes         No              No                    Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               Yes         No              No                    Yes
No                     Yes                    Yes
```

```
                      (0.8,          0.2)),                 // No
Yes                Yes         No               No                     Yes
No                      Yes                     No
                     ((0.8,          0.2),                  // No
Yes                Yes         No               No                     Yes
No                      No                      Yes
                      (0.8,          0.2)))),               // No
Yes                Yes         No               No                     Yes
No                      No                      No
                   ((((0.8,          0.2),                  // No
Yes                Yes         No               No                     No
Yes                     Yes                     Yes
                      (0.8,          0.2)),                 // No
Yes                Yes         No               No                     No
Yes                     Yes                     No
                     ((0.8,          0.2),                  // No
Yes                Yes         No               No                     No
Yes                     No                      Yes
                      (0.8,          0.2))),                // No
Yes                Yes         No               No                     No
Yes                     No                      No
                    (((0.8,          0.2),                  // No
Yes                Yes         No               No                     No
No                      Yes                     Yes
                      (0.8,          0.2)),                 // No
Yes                Yes         No               No                     No
No                      Yes                     No
                     ((0.8,          0.2),                  // No
Yes                Yes         No               No                     No
No                      No                      Yes
                      (0.8,          0.2))))))),            // No
Yes                Yes         No               No                     No
No                      No                      No
                (((((((0.8,          0.2),                  // No
Yes                No          Yes              Yes                    Yes
Yes                     Yes                     Yes
                      (0.8,          0.2)),                 // No
Yes                No          Yes              Yes                    Yes
Yes                     Yes                     No
                     ((0.8,          0.2),                  // No
Yes                No          Yes              Yes                    Yes
Yes                     No                      Yes
                      (0.8,          0.2))),                // No
Yes                No          Yes              Yes                    Yes
Yes                     No                      No
                    (((0.8,          0.2),                  // No
Yes                No          Yes              Yes                    Yes
No                      Yes                     Yes
                      (0.8,          0.2)),                 // No
Yes                No          Yes              Yes                    Yes
No                      Yes                     No
                     ((0.8,          0.2),                  // No
Yes                No          Yes              Yes                    Yes
No                      No                      Yes
                      (0.8,          0.2)))),               // No
Yes                No          Yes              Yes                    Yes
No                      No                      No
```

```
                  ((((0.8,         0.2),                  // No
Yes               No          Yes             Yes                   No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          Yes             Yes                   No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          Yes             Yes                   No
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
Yes               No          Yes             Yes                   No
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               No          Yes             Yes                   No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          Yes             Yes                   No
No                     Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          Yes             Yes                   No
No                     No                     Yes
                     (0.8,         0.2))))),              // No
Yes               No          Yes             Yes                   No
No                     No                     No
                 (((((0.8,         0.2),                  // No
Yes               No          Yes             No                    Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          Yes             No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          Yes             No                    Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
Yes               No          Yes             No                    Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               No          Yes             No                    Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          Yes             No                    Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          Yes             No                    Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // No
Yes               No          Yes             No                    Yes
No                     No                     No
                  ((((0.8,         0.2),                  // No
Yes               No          Yes             No                    No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          Yes             No                    No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          Yes             No                    No
Yes                    No                     Yes
```

```
                     (0.8,         0.2))),                // No
Yes               No          Yes             No                    No
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               No          Yes             No                    No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          Yes             No                    No
No                     Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          Yes             No                    No
No                     No                     Yes
                     (0.8,         0.2)))))),             // No
Yes               No          Yes             No                    No
No                     No                     No
                ((((((0.8,         0.2),                  // No
Yes               No          No              Yes                   Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          No              Yes                   Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          No              Yes                   Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
Yes               No          No              Yes                   Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               No          No              Yes                   Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          No              Yes                   Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          No              Yes                   Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // No
Yes               No          No              Yes                   Yes
No                     No                     No
                  ((((0.8,         0.2),                  // No
Yes               No          No              Yes                   No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          No              Yes                   No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
Yes               No          No              Yes                   No
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
Yes               No          No              Yes                   No
Yes                    No                     No
                   (((0.8,         0.2),                  // No
Yes               No          No              Yes                   No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
Yes               No          No              Yes                   No
No                     Yes                    No
```

```
                      ((0.8,           0.2),                    // No
Yes                 No           No                Yes                     No
No                       No                        Yes
                       (0.8,           0.2))))),                // No
Yes                 No           No                Yes                     No
No                       No                        No
                   (((((0.8,           0.2),                    // No
Yes                 No           No                No                      Yes
Yes                      Yes                       Yes
                       (0.8,           0.2)),                   // No
Yes                 No           No                No                      Yes
Yes                      Yes                       No
                      ((0.8,           0.2),                    // No
Yes                 No           No                No                      Yes
Yes                      No                        Yes
                       (0.8,           0.2))),                  // No
Yes                 No           No                No                      Yes
Yes                      No                        No
                     (((0.8,           0.2),                    // No
Yes                 No           No                No                      Yes
No                       Yes                       Yes
                       (0.8,           0.2)),                   // No
Yes                 No           No                No                      Yes
No                       Yes                       No
                      ((0.8,           0.2),                    // No
Yes                 No           No                No                      Yes
No                       No                        Yes
                       (0.8,           0.2)))),                 // No
Yes                 No           No                No                      Yes
No                       No                        No
                    ((((0.8,           0.2),                    // No
Yes                 No           No                No                      No
Yes                      Yes                       Yes
                       (0.8,           0.2)),                   // No
Yes                 No           No                No                      No
Yes                      Yes                       No
                      ((0.8,           0.2),                    // No
Yes                 No           No                No                      No
Yes                      No                        Yes
                       (0.8,           0.2))),                  // No
Yes                 No           No                No                      No
Yes                      No                        No
                     (((0.8,           0.2),                    // No
Yes                 No           No                No                      No
No                       Yes                       Yes
                       (0.8,           0.2)),                   // No
Yes                 No           No                No                      No
No                       Yes                       No
                      ((0.8,           0.2),                    // No
Yes                 No           No                No                      No
No                       No                        Yes
                       (0.8,           0.2)))))))),             // No
Yes                 No           No                No                      No
No                       No                        No
                ((((((((0.8,           0.2),                    // No
No                  Yes          Yes               Yes                     Yes
Yes                      Yes                       Yes
```

```
                      (0.8,         0.2)),                  // No
No                 Yes         Yes             Yes                   Yes
Yes                     Yes                     No
                     ((0.8,         0.2),                   // No
No                 Yes         Yes             Yes                   Yes
Yes                     No                      Yes
                      (0.8,         0.2))),                 // No
No                 Yes         Yes             Yes                   Yes
Yes                     No                      No
                    (((0.8,         0.2),                   // No
No                 Yes         Yes             Yes                   Yes
No                      Yes                     Yes
                      (0.8,         0.2)),                  // No
No                 Yes         Yes             Yes                   Yes
No                      Yes                     No
                     ((0.8,         0.2),                   // No
No                 Yes         Yes             Yes                   Yes
No                      No                      Yes
                      (0.8,         0.2)))),                // No
No                 Yes         Yes             Yes                   Yes
No                      No                      No
                   ((((0.8,         0.2),                   // No
No                 Yes         Yes             Yes                   No
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // No
No                 Yes         Yes             Yes                   No
Yes                     Yes                     No
                     ((0.8,         0.2),                   // No
No                 Yes         Yes             Yes                   No
Yes                     No                      Yes
                      (0.8,         0.2))),                 // No
No                 Yes         Yes             Yes                   No
Yes                     No                      No
                    (((0.8,         0.2),                   // No
No                 Yes         Yes             Yes                   No
No                      Yes                     Yes
                      (0.8,         0.2)),                  // No
No                 Yes         Yes             Yes                   No
No                      Yes                     No
                     ((0.8,         0.2),                   // No
No                 Yes         Yes             Yes                   No
No                      No                      Yes
                      (0.8,         0.2))))),               // No
No                 Yes         Yes             Yes                   No
No                      No                      No
                  (((((0.8,         0.2),                   // No
No                 Yes         Yes             No                    Yes
Yes                     Yes                     Yes
                      (0.8,         0.2)),                  // No
No                 Yes         Yes             No                    Yes
Yes                     Yes                     No
                     ((0.8,         0.2),                   // No
No                 Yes         Yes             No                    Yes
Yes                     No                      Yes
                      (0.8,         0.2))),                 // No
No                 Yes         Yes             No                    Yes
Yes                     No                      No
```

```
                    (((0.8,          0.2),                    // No
No                 Yes          Yes              No                     Yes
No                       Yes                     Yes
                      (0.8,          0.2)),                   // No
No                 Yes          Yes              No                     Yes
No                       Yes                     No
                     ((0.8,          0.2),                    // No
No                 Yes          Yes              No                     Yes
No                       No                      Yes
                      (0.8,          0.2)))),                 // No
No                 Yes          Yes              No                     Yes
No                       No                      No
                    (((0.8,          0.2),                    // No
No                 Yes          Yes              No                     No
Yes                      Yes                     Yes
                      (0.8,          0.2)),                   // No
No                 Yes          Yes              No                     No
Yes                      Yes                     No
                     ((0.8,          0.2),                    // No
No                 Yes          Yes              No                     No
Yes                      No                      Yes
                      (0.8,          0.2))),                  // No
No                 Yes          Yes              No                     No
Yes                      No                      No
                    (((0.8,          0.2),                    // No
No                 Yes          Yes              No                     No
No                       Yes                     Yes
                      (0.8,          0.2)),                   // No
No                 Yes          Yes              No                     No
No                       Yes                     No
                     ((0.8,          0.2),                    // No
No                 Yes          Yes              No                     No
No                       No                      Yes
                      (0.8,          0.2)))))),               // No
No                 Yes          Yes              No                     No
No                       No                      No
                 ((((((0.8,          0.2),                    // No
No                 Yes          No               Yes                    Yes
Yes                      Yes                     Yes
                      (0.8,          0.2)),                   // No
No                 Yes          No               Yes                    Yes
Yes                      Yes                     No
                     ((0.8,          0.2),                    // No
No                 Yes          No               Yes                    Yes
Yes                      No                      Yes
                      (0.8,          0.2))),                  // No
No                 Yes          No               Yes                    Yes
Yes                      No                      No
                    (((0.8,          0.2),                    // No
No                 Yes          No               Yes                    Yes
No                       Yes                     Yes
                      (0.8,          0.2)),                   // No
No                 Yes          No               Yes                    Yes
No                       Yes                     No
                     ((0.8,          0.2),                    // No
No                 Yes          No               Yes                    Yes
No                       No                      Yes
```

```
                     (0.8,         0.2)))),               // No
No                Yes         No            Yes                   Yes
No                     No                    No
                  ((((0.8,         0.2),                  // No
No                Yes         No            Yes                   No
Yes                    Yes                   Yes
                     (0.8,         0.2)),                 // No
No                Yes         No            Yes                   No
Yes                    Yes                   No
                    ((0.8,         0.2),                  // No
No                Yes         No            Yes                   No
Yes                    No                    Yes
                     (0.8,         0.2))),                // No
No                Yes         No            Yes                   No
Yes                    No                    No
                   (((0.8,         0.2),                  // No
No                Yes         No            Yes                   No
No                     Yes                   Yes
                     (0.8,         0.2)),                 // No
No                Yes         No            Yes                   No
No                     Yes                   No
                    ((0.8,         0.2),                  // No
No                Yes         No            Yes                   No
No                     No                    Yes
                     (0.8,         0.2))))),              // No
No                Yes         No            Yes                   No
No                     No                    No
                 (((((0.8,         0.2),                  // No
No                Yes         No            No                    Yes
Yes                    Yes                   Yes
                     (0.8,         0.2)),                 // No
No                Yes         No            No                    Yes
Yes                    Yes                   No
                    ((0.8,         0.2),                  // No
No                Yes         No            No                    Yes
Yes                    No                    Yes
                     (0.8,         0.2))),                // No
No                Yes         No            No                    Yes
Yes                    No                    No
                   (((0.8,         0.2),                  // No
No                Yes         No            No                    Yes
No                     Yes                   Yes
                     (0.8,         0.2)),                 // No
No                Yes         No            No                    Yes
No                     Yes                   No
                    ((0.8,         0.2),                  // No
No                Yes         No            No                    Yes
No                     No                    Yes
                     (0.8,         0.2)))),               // No
No                Yes         No            No                    Yes
No                     No                    No
                  ((((0.8,         0.2),                  // No
No                Yes         No            No                    No
Yes                    Yes                   Yes
                     (0.8,         0.2)),                 // No
No                Yes         No            No                    No
Yes                    Yes                   No
```

```
                      ((0.8,         0.2),                    // No
No                 Yes          No               No                      No
Yes                     No                       Yes
                       (0.8,         0.2))),                  // No
No                 Yes          No               No                      No
Yes                     No                       No
                     (((0.8,         0.2),                    // No
No                 Yes          No               No                      No
No                      Yes                      Yes
                       (0.8,         0.2)),                   // No
No                 Yes          No               No                      No
No                      Yes                      No
                      ((0.8,         0.2),                    // No
No                 Yes          No               No                      No
No                      No                       Yes
                       (0.8,         0.2))))))),              // No
No                 Yes          No               No                      No
No                      No                       No
                 (((((((0.8,         0.2),                    // No
No                 No           Yes              Yes                     Yes
Yes                     Yes                      Yes
                       (0.8,         0.2)),                   // No
No                 No           Yes              Yes                     Yes
Yes                     Yes                      No
                      ((0.8,         0.2),                    // No
No                 No           Yes              Yes                     Yes
Yes                     No                       Yes
                       (0.8,         0.2))),                  // No
No                 No           Yes              Yes                     Yes
Yes                     No                       No
                     (((0.8,         0.2),                    // No
No                 No           Yes              Yes                     Yes
No                      Yes                      Yes
                       (0.8,         0.2)),                   // No
No                 No           Yes              Yes                     Yes
No                      Yes                      No
                      ((0.8,         0.2),                    // No
No                 No           Yes              Yes                     Yes
No                      No                       Yes
                       (0.8,         0.2)))),                 // No
No                 No           Yes              Yes                     Yes
No                      No                       No
                    ((((0.8,         0.2),                    // No
No                 No           Yes              Yes                     No
Yes                     Yes                      Yes
                       (0.8,         0.2)),                   // No
No                 No           Yes              Yes                     No
Yes                     Yes                      No
                      ((0.8,         0.2),                    // No
No                 No           Yes              Yes                     No
Yes                     No                       Yes
                       (0.8,         0.2))),                  // No
No                 No           Yes              Yes                     No
Yes                     No                       No
                     (((0.8,         0.2),                    // No
No                 No           Yes              Yes                     No
No                      Yes                      Yes
```

```
                     (0.8,         0.2)),                 // No
No                No          Yes             Yes                   No
No                     Yes                    No
                    ((0.8,         0.2),                  // No
No                No          Yes             Yes                   No
No                     No                     Yes
                     (0.8,         0.2))))),              // No
No                No          Yes             Yes                   No
No                     No                     No
                 (((((0.8,         0.2),                  // No
No                No          Yes             No                    Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          Yes             No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
No                No          Yes             No                    Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
No                No          Yes             No                    Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // No
No                No          Yes             No                    Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          Yes             No                    Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // No
No                No          Yes             No                    Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // No
No                No          Yes             No                    Yes
No                     No                     No
                  ((((0.8,         0.2),                  // No
No                No          Yes             No                    No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          Yes             No                    No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
No                No          Yes             No                    No
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
No                No          Yes             No                    No
Yes                    No                     No
                   (((0.8,         0.2),                  // No
No                No          Yes             No                    No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          Yes             No                    No
No                     Yes                    No
                    ((0.8,         0.2),                  // No
No                No          Yes             No                    No
No                     No                     Yes
                     (0.8,         0.2)))))),             // No
No                No          Yes             No                    No
No                     No                     No
```

```
                ((((((0.8,         0.2),                  // No
No                No          No              Yes                   Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          No              Yes                   Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
No                No          No              Yes                   Yes
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
No                No          No              Yes                   Yes
Yes                    No                     No
                   (((0.8,         0.2),                  // No
No                No          No              Yes                   Yes
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          No              Yes                   Yes
No                     Yes                    No
                    ((0.8,         0.2),                  // No
No                No          No              Yes                   Yes
No                     No                     Yes
                     (0.8,         0.2)))),               // No
No                No          No              Yes                   Yes
No                     No                     No
                  ((((0.8,         0.2),                  // No
No                No          No              Yes                   No
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          No              Yes                   No
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
No                No          No              Yes                   No
Yes                    No                     Yes
                     (0.8,         0.2))),                // No
No                No          No              Yes                   No
Yes                    No                     No
                   (((0.8,         0.2),                  // No
No                No          No              Yes                   No
No                     Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          No              Yes                   No
No                     Yes                    No
                    ((0.8,         0.2),                  // No
No                No          No              Yes                   No
No                     No                     Yes
                     (0.8,         0.2))))),              // No
No                No          No              Yes                   No
No                     No                     No
                 (((((0.8,         0.2),                  // No
No                No          No              No                    Yes
Yes                    Yes                    Yes
                     (0.8,         0.2)),                 // No
No                No          No              No                    Yes
Yes                    Yes                    No
                    ((0.8,         0.2),                  // No
No                No          No              No                    Yes
Yes                    No                     Yes
```

```
                     (0.8,         0.2))),                // No
No                No          No               No                    Yes
Yes                    No                      No
                   (((0.8,         0.2),                  // No
No                No          No               No                    Yes
No                     Yes                     Yes
                     (0.8,         0.2)),                 // No
No                No          No               No                    Yes
No                     Yes                     No
                    ((0.8,         0.2),                  // No
No                No          No               No                    Yes
No                     No                      Yes
                     (0.8,         0.2)))),               // No
No                No          No               No                    Yes
No                     No                      No
                  ((((0.8,         0.2),                  // No
No                No          No               No                    No
Yes                    Yes                     Yes
                     (0.8,         0.2)),                 // No
No                No          No               No                    No
Yes                    Yes                     No
                    ((0.8,         0.2),                  // No
No                No          No               No                    No
Yes                    No                      Yes
                     (0.8,         0.2))),                // No
No                No          No               No                    No
Yes                    No                      No
                   (((0.8,         0.2),                  // No
No                No          No               No                    No
No                     Yes                     Yes
                     (0.8,         0.2)),                 // No
No                No          No               No                    No
No                     Yes                     No
                    ((0.8,         0.2),                  // No
No                No          No               No                    No
No                     No                      Yes
                     (0.1,         0.9))))))))));         // No
No                No          No               No                    No
No                     No                      No                 ;
      title = "53-60 9C E8 ?? ?? ?? ?? 9D 61:ALL\n";
      whenchanged = 1237928338;
      belief = (0.2244839, 0.7755162);
      visual V1 {
            center = (1500, 744);
            dispform = BELIEFBARS;
            height = 57;
            };
      };

node ID_19 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDriverService, HideProcess);
      probs = 
            // Present      Absent          // HideDriverService
HideProcess
            (((0.8,         0.2),           // Yes                Yes
              (0.8,         0.2)),          // Yes                No
             ((0.8,         0.2),           // No                 Yes
              (0.1,         0.9)));         // No                 No
;
      title = "19-ZwQuerySystemInformation:ALL\n";
      whenchanged = 1237928398;
      belief = (0.178162, 0.821838);
      visual V1 {
            center = (480, 294);
            dispform = BELIEFBARS;
            height = 56;
            };
      };

node ID_20 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDriverService, HideProcess);
      probs =
            // Present      Absent          // HideDriverService
HideProcess
            (((0.8,         0.2),           // Yes                Yes
              (0.8,         0.2)),          // Yes                No
             ((0.8,         0.2),           // No                 Yes
              (0.1,         0.9)));         // No                 No
;
      title = "20-NtQuerySystemInformation:ALL\n";
      whenchanged = 1237928409;
      belief = (0.178162, 0.821838);
      visual V1 {
            center = (480, 372);
            dispform = BELIEFBARS;
            height = 55;
            };
      };

node ID_29 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDriverService);
      probs =
            // Present      Absent         // HideDriverService
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                ;
      title = "29-EnumServiceGroupW:USERMODE\n";
      whenchanged = 1237885371;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (750, 222);
            dispform = BELIEFBARS;
            height = 3;
            };
      };

node ID_30 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDriverService);
      probs = 
            // Present      Absent         // HideDriverService
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                ;
      title = "30-EnumServiceStatusExW:USERMODE\n";
      whenchanged = 1237885373;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1038, 222);
            dispform = BELIEFBARS;
            height = 4;
            };
      };

node ID_31 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDriverService);
      probs = 
            // Present      Absent         // HideDriverService
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                ;
      title = "31-EnumServiceStatusExA:USERMODE\n";
      whenchanged = 1237885375;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1332, 222);
            dispform = BELIEFBARS;
            height = 5;
            };
      };

node ID_32 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDriverService);
      probs = 
            // Present      Absent         // HideDriverService
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                ;
      title = "32-EnumServiceStatusA:USERMODE\n";
      whenchanged = 1237885378;
      belief = (0.1588, 0.8412);
```

```
	visual V1 {
		center = (1614, 222);
		dispform = BELIEFBARS;
		height = 6;
		};
	};

node ID_28 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideProcess);
	probs =
		// Present      Absent          // HideProcess
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No           ;
	title = "28-Process32Next:USERMODE\n";
	whenchanged = 1237885344;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (468, 492);
		dispform = BELIEFBARS;
		height = 39;
		};
	};

node ID_33 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideProcess);
	probs =
		// Present      Absent          // HideProcess
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No           ;
	title = "33-NtOpenProcess:ALL\n";
	whenchanged = 1237885412;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (702, 420);
		dispform = BELIEFBARS;
		height = 45;
		};
	};

node ID_34 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideProcess);
	probs =
		// Present      Absent          // HideProcess
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No           ;
```

```
      title = "34-ZwOpenProcess:ALL\n";
      whenchanged = 1237885415;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (684, 492);
            dispform = BELIEFBARS;
            height = 50;
            };
      };

node ID_43 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideProcess);
      probs =
            // Present      Absent         // HideProcess
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No          ;
      title = "43-Module32Next:USERMODE\n";
      whenchanged = 1237885587;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (906, 420);
            dispform = BELIEFBARS;
            height = 46;
            };
      };

node ID_44 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideProcess);
      probs =
            // Present      Absent         // HideProcess
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No          ;
      title = "44-Thread32Next:USERMODE\n";
      whenchanged = 1237885590;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (894, 492);
            dispform = BELIEFBARS;
            height = 51;
            };
      };

node ID_45 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideProcess);
      probs =
            // Present      Absent         // HideProcess
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No          ;
      title = "45-VirtualQuery:USERMODE\n";
      whenchanged = 1237885592;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1128, 420);
            dispform = BELIEFBARS;
            height = 47;
            };
      };

node ID_46 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideProcess);
      probs =
            // Present      Absent         // HideProcess
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No          ;
      title = "46-VirtualQueryEx:USERMODE\n";
      whenchanged = 1237885595;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1128, 492);
            dispform = BELIEFBARS;
            height = 52;
            };
      };

node ID_47 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideProcess);
      probs =
            // Present      Absent         // HideProcess
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No          ;
      title = "47-Process32Next:USERMODE\n";
      whenchanged = 1237885598;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1350, 420);
            dispform = BELIEFBARS;
            height = 48;
            };
      };

node ID_48 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideProcess);
      probs =
            // Present      Absent         // HideProcess
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No           ;
      title = "48-NtQuerySystemInformation:USERMODE\n";
      whenchanged = 1237885601;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1410, 492);
            dispform = BELIEFBARS;
            height = 53;
            };
      };

node ID_49 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideProcess);
      probs =
            // Present      Absent         // HideProcess
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No           ;
      title = "49-Thread32Next:USERMODE\n";
      whenchanged = 1237885604;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1578, 420);
            dispform = BELIEFBARS;
            height = 49;
            };
      };

node ID_23 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideRegistryKey);
      probs =
            // Present      Absent         // HideRegistryKey
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No               ;
      title = "23-ZwOpenKey:ALL\n";
      whenchanged = 1237885295;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (438, 564);
            dispform = BELIEFBARS;
            height = 40;
            };
      };

node ID_24 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideRegistryKey);
	probs = 
		// Present      Absent          // HideRegistryKey
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No               ;
	title = "24-NtOpenKey:ALL\n";
	whenchanged = 1237885296;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (618, 564);
		dispform = BELIEFBARS;
		height = 41;
		};
	};

node ID_25 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideRegistryKey);
	probs = 
		// Present      Absent          // HideRegistryKey
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No               ;
	title = "25-ZwEnumerateKey:ALL\n";
	whenchanged = 1237885298;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (804, 564);
		dispform = BELIEFBARS;
		height = 42;
		};
	};

node ID_26 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideRegistryKey);
	probs = 
		// Present      Absent          // HideRegistryKey
		 ((0.8,         0.2),           // Yes
		  (0.1,         0.9));          // No               ;
	title = "26-NtEnumerateKey:ALL\n";
	whenchanged = 1237885299;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (996, 564);
		dispform = BELIEFBARS;
		height = 43;
		};
```

```
      };

node ID_11 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (Keylogger);
      probs =
            // Present      Absent          // Keylogger
             ((0.8,         0.2),           // Yes
              (0.1,         0.9));          // No        ;
      title = "11-ZwQueryDirectoryFile:KEYBOARD\n";
      whenchanged = 1237884287;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (480, 636);
            dispform = BELIEFBARS;
            height = 34;
            };
      };

node ID_12 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (Keylogger);
      probs =
            // Present      Absent          // Keylogger
             ((0.8,         0.2),           // Yes
              (0.1,         0.9));          // No        ;
      title = "12-ZwCreateFile:KEYBOARD\n";
      whenchanged = 1237884288;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (726, 636);
            dispform = BELIEFBARS;
            height = 35;
            };
      };

node ID_13 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (Keylogger);
      probs =
            // Present      Absent          // Keylogger
             ((0.8,         0.2),           // Yes
              (0.1,         0.9));          // No        ;
      title = "13-ZwOpenFile:KEYBOARD\n";
      whenchanged = 1237884289;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (942, 636);
            dispform = BELIEFBARS;
            height = 36;
            };
      };

node ID_14 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (Keylogger);
      probs =
            // Present      Absent          // Keylogger
             ((0.8,         0.2),           // Yes
              (0.1,         0.9));          // No        ;
      title = "14-ZwWriteFile:KEYBOARD\n";
      whenchanged = 1237884292;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1152, 636);
            dispform = BELIEFBARS;
            height = 37;
            };
      };

node ID_15 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (UsermodeLoadDeviceDriver);
      probs =
            // Present      Absent          // UsermodeLoadDeviceDriver
             ((0.8,         0.2),           // Yes
              (0.1,         0.9));          // No
;
      title = "15-ZwSetSystemInformation:USERMODE\n";
      whenchanged = 1237884293;
      belief = (0.17, 0.83);
      visual V1 {
            center = (498, 708);
            dispform = BELIEFBARS;
            height = 33;
            };
      };

node ID_18 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (DisableSystemSecurity);
      probs =
            // Present      Absent          // DisableSystemSecurity
             ((0.8,         0.2),           // Yes
              (0.1,         0.9));          // No                       ;
      title = "18-SeAccessCheck:ALL\n";
```

```
	whenchanged = 1237884449;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (444, 780);
		dispform = BELIEFBARS;
		height = 31;
		};
	};

node ID_1 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (KnownBadModuleName);
	probs = 
		// Present      Absent         // KnownBadModuleName
		 ((0.25,        0.75),         // Yes
		  (0,           1));           // No                 ;
	title = "1-eggdrop.exe:USERMODE";
	whenchanged = 1237926786;
	belief = (0.021, 0.979);
	visual V1 {
		center = (456, 852);
		dispform = BELIEFBARS;
		height = 26;
		};
	};

node ID_2 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (KnownBadModuleName);
	probs = 
		// Present      Absent         // KnownBadModuleName
		 ((0.25,        0.75),         // Yes
		  (0,           1));           // No                 ;
	title = "2-aattv8xo.sys:KERNELMODE\n";
	whenchanged = 1237926795;
	belief = (0.021, 0.979);
	visual V1 {
		center = (672, 852);
		dispform = BELIEFBARS;
		height = 27;
		};
	};

node ID_3 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (KnownBadModuleName);
	probs = 
		// Present      Absent         // KnownBadModuleName
```

```
                ((0.25,        0.75),         // Yes
                 (0,           1));           // No                   ;
        title = "3-spooll32.exe:USERMODE\n";
        whenchanged = 1237926805;
        belief = (0.021, 0.979);
        visual V1 {
              center = (888, 852);
              dispform = BELIEFBARS;
              height = 28;
              };
        };

  node ID_4 {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Present, Absent);
        parents = (KnownBadModuleName);
        probs =
              // Present      Absent         // KnownBadModuleName
                ((0.25,        0.75),         // Yes
                 (0,           1));           // No                   ;
        title = "4-avserv.exe:USERMODE\n";
        whenchanged = 1237926811;
        belief = (0.021, 0.979);
        visual V1 {
              center = (1092, 852);
              dispform = BELIEFBARS;
              height = 29;
              };
        };

  node ID_37 {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Present, Absent);
        parents = (MonitorNetworkTraffic);
        probs =
              // Present      Absent         // MonitorNetworkTraffic
                ((0.8,         0.2),          // Yes
                 (0.1,         0.9));         // No                      ;
        title = "37-recv:USERMODE\n";
        whenchanged = 1237885470;
        belief = (0.1588, 0.8412);
        visual V1 {
              center = (438, 924);
              dispform = BELIEFBARS;
              height = 21;
              };
        };

  node ID_38 {
        kind = NATURE;
        discrete = TRUE;
        chance = CHANCE;
        states = (Present, Absent);
```

```
      parents = (MonitorNetworkTraffic);
      probs = 
            // Present      Absent         // MonitorNetworkTraffic
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                    ;
      title = "38-WSARecv:USERMODE\n";
      whenchanged = 1237885471;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (630, 924);
            dispform = BELIEFBARS;
            height = 22;
            };
      };

node ID_39 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (MonitorNetworkTraffic);
      probs = 
            // Present      Absent         // MonitorNetworkTraffic
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                    ;
      title = "39-send:USERMODE\n";
      whenchanged = 1237885473;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (822, 924);
            dispform = BELIEFBARS;
            height = 23;
            };
      };

node ID_40 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (MonitorNetworkTraffic);
      probs = 
            // Present      Absent         // MonitorNetworkTraffic
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                    ;
      title = "40-WSASend:USERMODE\n";
      whenchanged = 1237885474;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (1014, 924);
            dispform = BELIEFBARS;
            height = 24;
            };
      };

node ID_41 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (RedirectNetworkTraffic);
      probs = 
            // Present      Absent         // RedirectNetworkTraffic
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                     ;
      title = "41-gethostbyname:USERMODE\n";
      whenchanged = 1237885492;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (468, 996);
            dispform = BELIEFBARS;
            height = 18;
            };
      };

node ID_42 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (RedirectNetworkTraffic);
      probs = 
            // Present      Absent         // RedirectNetworkTraffic
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                     ;
      title = "42-getaddrinfo:USERMODE\n";
      whenchanged = 1237885493;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (696, 996);
            dispform = BELIEFBARS;
            height = 19;
            };
      };

node ID_52 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (DisableMemoryProtection);
      probs = 
            // Present      Absent         // DisableMemoryProtection
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                      ;
      title = "52-50 0F 20 C0 25 FF FF FE FF 0F 22 C0 58:ALL\n";
      whenchanged = 1237885680;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (510, 1068);
            dispform = BELIEFBARS;
            height = 16;
            };
      };
```

```
node ID_54 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDebuggingOperation);
      probs =
            // Present      Absent         // HideDebuggingOperation
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                        ;
      title = "54-ZwGetContextThread:ALL\n";
      whenchanged = 1237885736;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (462, 1140);
            dispform = BELIEFBARS;
            height = 11;
            };
      };

node ID_55 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDebuggingOperation);
      probs =
            // Present      Absent         // HideDebuggingOperation
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                        ;
      title = "55-ZwSetContextThread:ALL\n";
      whenchanged = 1237885736;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (678, 1140);
            dispform = BELIEFBARS;
            height = 12;
            };
      };

node ID_56 {
      kind = NATURE;
      discrete = TRUE;
      chance = CHANCE;
      states = (Present, Absent);
      parents = (HideDebuggingOperation);
      probs =
            // Present      Absent         // HideDebuggingOperation
             ((0.8,         0.2),          // Yes
              (0.1,         0.9));         // No                        ;
      title = "56-GetContextThread:USERMODE\n";
      whenchanged = 1237885736;
      belief = (0.1588, 0.8412);
      visual V1 {
            center = (912, 1140);
            dispform = BELIEFBARS;
```

```
		height = 13;
		};
	};

node ID_57 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (HideDebuggingOperation);
	probs = 
		// Present      Absent         // HideDebuggingOperation
		 ((0.8,         0.2),          // Yes
		  (0.1,         0.9));         // No                       ;
	title = "57-SetContextThread:USERMODE\n";
	whenchanged = 1237885736;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (1164, 1140);
		dispform = BELIEFBARS;
		height = 14;
		};
	};

node ID_59 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (AlterProgramTiming);
	probs = 
		// Present      Absent         // AlterProgramTiming
		 ((0.8,         0.2),          // Yes
		  (0.1,         0.9));         // No                   ;
	title = "59-ZwQueryPerformanceCounter:ALL\n";
	whenchanged = 1237885750;
	belief = (0.1588, 0.8412);
	visual V1 {
		center = (684, 1212);
		dispform = BELIEFBARS;
		height = 9;
		};
	};

node ID_58 {
	kind = NATURE;
	discrete = TRUE;
	chance = CHANCE;
	states = (Present, Absent);
	parents = (AlterProgramTiming);
	probs = 
		// Present      Absent         // AlterProgramTiming
		 ((0.8,         0.2),          // Yes
		  (0.1,         0.9));         // No                   ;
	title = "58-ZwGetTickCount:ALL\n";
	whenchanged = 1237885750;
	belief = (0.1588, 0.8412);
```

```
      visual V1 {
            center = (450, 1212);
            dispform = BELIEFBARS;
            height = 8;
            };
      };
ElimOrder = (ID_5, ID_6, ID_7, ID_8, ID_9, ID_10, ID_16, ID_17,
Backdoor, ID_21, ID_22, ID_27, ID_35, ID_36, ID_50, ID_51, ID_29,
ID_30, ID_31, ID_32, ID_28, ID_33, ID_34, ID_43, ID_44, ID_45, ID_46,
ID_47, ID_48, ID_49, ID_23, ID_24, ID_25, ID_26, ID_11, ID_12, ID_13,
ID_14, Keylogger, ID_15, UsermodeLoadDeviceDriver, ID_18, ID_1, ID_2,
ID_3, ID_4, KnownBadModuleName, ID_37, ID_38, ID_39, ID_40, ID_41,
ID_42, ID_52, DisableMemoryProtection, ID_54, ID_55, ID_56, ID_57,
ID_59, ID_58, ID_19, ID_20, BotInfection, HideFileDirectory,
HideDriverService, HideProcess, HideRegistryKey, DisableSystemSecurity,
MonitorNetworkTraffic, RedirectNetworkTraffic, HideDebuggingOperation,
AlterProgramTiming, ID_53);
};
```