Raytheon
Blackbird Technologies

20150814-258-Symantec
Black Vine

For

SIRIUS Task Order PIQUE

Submitted to:

U.S. Government

Submitted by:

Raytheon Blackbird Technologies, Inc.
13900 Lincoln Park Drive
Suite 400
Herndon, VA 20171

14 August 2015

(U) Table of Contents

1.0 (U) Analysis Summary

(S//NF) This was a very interesting report on a series of attacks attributed to a suspected Chinese bad actor group known as "Black Vine." Unfortunately, there is very little technical details on how Black Vine's capabilities are implemented. The report does provide a well written executive summary of the group's activities and capabilities.

(S//NF) Black Vine has been active since 2012 and appear to be well funded, highly organized, and has access to 0-day exploits through the underground Elderwood Framework. Black Vine focuses on the energy, aerospace, and health sectors. The group is suspected as being behind the spectacular data theft from Anthem Insurance in early 2014. Black Vine has some association with Topsec, a Chinese IT security company.

(S//NF) The predominant attack vector used by Black Vine is water holing, however the group has been observed using spear phishing email campaigns in rare instances. The overwhelming majority of their attacks are targeted at U.S. entities (83%).

(S//NF) Black Vine has been observed dropping three variants of a simple RAT: Hurix, Sakurel (both detected as Trojan.Sakurel), and Mivast (detected as Backdoor.Mivast). All three RAT variants exhibit miminal RAT functionality that includes:

- Open a pipe backdoor
- Execute files and commands
- Delete, modify, and create registry keys
- Gather and transmit information about the victim machine

There were no technical details on how the RATs are dropped or installed on the victim. There were no description on how the functionality is implemented.

(S//NF) In several attacks, Black Vine use legitimate Korean certificates to sign their malware. Both certificates observed in use by the group have either since expired or been blacklisted.

(S//NF) Black Vine has been observed over the last few years using two 0-day exploits based on Use-After-Free (UAF) vulnerabilities in Microsoft's Internet Explorer. Both UAF 0-day exploits have since been disclosed and designated CVE-2012-4792 and CVE-2014-0322.

(S//NF) As there are no technical details on how the attack code is dropped and loaded or how the RAT varieties functionality is implemented, no PoCs are recommended.

2.0 (U) Description of the Technique

(S//NF) Not applicable as no PoCs are recommended.

3.0 (U) Identification of Affected Applications

(U) Windows and Microsoft Internet Explorer.

4.0 (U) Related Techniques

(S//NF) Generic RAT, Use-After-Free browser vulnerability.

5.0 (U) Configurable Parameters

(U) None.

6.0 (U) Exploitation Method and Vectors

(S//NF) The exploited vulnerabilities discussed are CVE-2012-4792 and CVE-2014-0322, both UAF vulnerabilities in Microsoft Internet Explorer browser. The attack vectors discussed were water holing and spear phishing.

7.0 (U) Caveats

(U) None.

8.0 (U) Risks

(S//NF) Not applicable as no PoCs are recommended.

9.0 (U) Recommendations

(S//NF) Due to lack of technical detail, no PoCs are recommended.