

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!



Homeland
Security

September 29, 2010

John Greenewald, Jr.
[REDACTED]
[REDACTED]

Dear Mr. Greenewald:

Re: **NPPD09F3722**

This is the electronic final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated July 10, 2009, and received by this office on July 16, 2009. You are seeking “any and all DHS (cyber security) records (final copy memorandum, emails from Directors to the Secretary and Deputy Secretary) indicating what took place and the steps taken to secure our nations network infrastructure concerning the July 2009 cyber attack on the United States causing disruption to major network systems.”

A search of the Office of Cybersecurity and Communications for documents responsive to your request produced a total of 22 pages. Of those pages, I have determined that 14 pages of the records are releasable in their entirety and 8 pages are partially releasable, pursuant to Title 5 U.S.C. § 552 (b)(2)(high), FOIA Exemptions 2(high).

Enclosed are 22 pages with certain information withheld as described below.

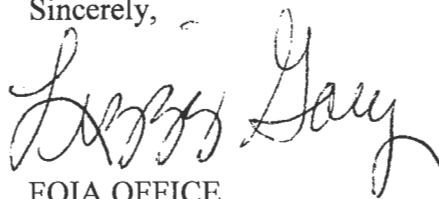
FOIA Exemption 2(high) protects information applicable to internal administrative and personnel matters, such as operating rules, guidelines, and manual of procedures of examiners or adjudicators, to the extent that disclosure would risk circumvention of an agency regulation or statute, impede the effectiveness of an agency’s activities, or reveal sensitive information that may put the security and safety of an agency activity or employee at risk. Whether there is any public interest in disclosure is legally irrelevant. Rather, the concern under high 2 is that a FOIA disclosure should not benefit those attempting to violate the law and avoid detection.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), U.S. Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked “FOIA Appeal.” Copies of the FOIA and DHS regulations are available at www.dhs.gov/foia.

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the \$14 minimum, there is no charge. 6 CFR § 5.11(d)(4).

If you need to contact our office again about this matter, please refer to **NPPD09F3722**. This office can be reached at 703-235-2211.

Sincerely,

A handwritten signature in black ink, appearing to read "Lizzy Gay". The signature is written in a cursive style with a large initial "L" and a long, sweeping tail on the "y".

FOIA OFFICE
National Protection and Programs Directorate

Enclosure(s): Responsive Documents, 22 pages



Unclassified/For Official Use Only

NPPD Information Bulletin

FCKeditor Vulnerability

Executive Summary

US-CERT is aware of reports of a remote file upload vulnerability in FCKeditor version 2.6.4 that is being actively exploited in the wild. Currently, there are no reported exploits in the Federal government. According to open source reports, a new version of FCKeditor that corrects this vulnerability will be made available on Monday, July 6th, 2009.

FCKeditor may be used in any of the following server applications:

- * ASP.Net
- * ASP
- * ColdFusion
- * PHP
- * Java
- * Active-FoxPro
- * Lasso
- * Perl
- * Python

Impact

Currently, there are no known compromises of any government servers. US-CERT will continue to monitor this activity and update the impact assessment as necessary.

Current Actions

US-CERT

- Released an alert to the GFIRST community via the US-CERT portal on July 3, 2009, providing details of the vulnerability as well as recommendations to mitigate the risk until a patch is released.
- Continuing to monitor for further developments.
- More information on this vulnerability can be found at: <http://isc.sans.org/diary.html?storyid=6715>



~~Unclassified/For Official Use Only~~ NPPD Information Bulletin

Potential SQL Injection Vulnerabilities on Government Servers

Executive Summary

On July 3, 2009, US-CERT received notification from a third-party that several government web servers may be vulnerable to a SQL injection attack. US-CERT analysts have reviewed the websites and while the sites are susceptible, there is no evidence of compromise at this time. The websites reported are listed below. Please note these URLs are obfuscated with "hxxp" and "[dot]" to prevent accidental execution.

hxxp://www[dot]okcommerce[dot]gov/index.php?option=com_content&task=view&id=12&Itemid=36'

hxxp://www[dot]senate[dot]michigan[dot]gov/dem/blog.php?id=121'

hxxp://www[dot]openworld[dot]gov/news/frontimages.php?lang=1'

Impact

Currently, there are no known compromises of these sites, therefore the impact to the Federal government is low. If a SQL injection attack were to be leveraged against these servers, there is potential for a root level compromise which could change the impact assessment at that time.

Current Actions

US-CERT

- Coordinated with SANS (the third-party reporter) to obtain more details.
- Notified (b)(2)High of potential vulnerability on their website.
- Coordinated with MS-ISAC to notify affected parties of potentially vulnerable sites.
- Continue to coordinate with (b)(2)High to mitigate potential vulnerabilities.
- Continue to work with MS-ISAC to mitigate potential vulnerabilities in state agency webservers.

MS-ISAC

- Notified affected state agencies of potentially vulnerable web sites.
- Continue to coordinate with agencies and US-CERT to mitigate potential vulnerabilities.

The data contained in this report shall not be altered prior to any redistribution.
Distribution to organizations outside of DHS should be coordinated with US-CERT.

~~Unclassified/For Official Use Only~~



~~Unclassified/For Official Use Only~~
NPPD Information Bulletin
Active Exploitation of Unpatched Vulnerability in
Microsoft Video ActiveX Control

Executive Summary

Microsoft has released Security Advisory, 972890, to address reports of an unpatched vulnerability in Microsoft Video ActiveX Control. According to the advisory, an attacker who successfully exploits this vulnerability may be able to gain the same user rights as the local user. Additionally, when using Internet Explorer, remote code execution is possible and may not require any user intervention. Microsoft is aware of attempts to exploit this vulnerability. This vulnerability affects Windows XP and Windows Server 2003.

The Microsoft Video Control Object is an ActiveX control that connects Microsoft DirectShow filters for use in capturing, recording, and playing video. It is the main component that Microsoft Windows Media Center uses to build filter graphs for recording and playing television video. According to the advisory, when the ActiveX Control Object (MPEG2TuneRequest) is used in Internet Explorer, the control may corrupt the system state which could allow an attacker to run arbitrary code.

Microsoft states that Internet Explorer has no by-design uses for this ActiveX Control including all of the Class Identifiers within msvidctl.dll that hosts the control, and therefore recommends removing support for all associated Class Identifiers.

This vulnerability may be exploited via a web-based attack scenario. An attacker could host a web site that contains a specially crafted web page to exploit this vulnerability. In order for a user to become a victim, an attacker would have to lure the user to the compromised website, typically by convincing them to click on a link in an email or Instant Messenger message.

Impact

Currently, there are no known compromises of any Federal government systems.

Current Actions**US-CERT**

- Coordinated with Microsoft to review the advisory prior to its public release.
- Released multiple products to ensure broadest situational awareness of this vulnerability and to provide recommendations to mitigate the risk until a patch is available:
 - Current Activity Entry – public website
 - Vulnerability Note VU#180513– public website
 - Technical Security Alert TA09-187A – public website
 - Cyber Security Alert (non-technical) SA09-187A – public website
 - Situational Awareness Report (SAR) – GFIRST community via the US-CERT portal
 - Critical Infrastructure Information Notice (CIIN) – ISACs and Critical Infrastructure partners via the US-CERT portal and vetted external distribution lists
- Conducting a CIO/CISO Unclassified Conference Call on July 7, 2009 at 11 AM EST to discuss this vulnerability and web security in general.
- More information about this vulnerability is available in the MS Advisory:
<http://www.microsoft.com/technet/security/advisory/972890.mspx>

Microsoft

- Provided the Microsoft Advisory to US-CERT prior to its release.
- Developing a security update to address this vulnerability.

~~Unclassified/For Official Use Only~~



~~Unclassified/For Official Use Only~~
NPPD Information Bulletin

Incident Involving DHS SOC Analyst Account Summary**Executive Summary**

On June 17, 2009, US-CERT observed an alert generated from a DNS query and response on an Einstein 2 sensor. (b)(2)High This alert was reported to the DHS SOC shortly thereafter. On June 20, 2009, DHS SOC notified US-CERT that a DHS SOC analyst's Einstein user account may have been compromised. Later, DHS SOC and US-CERT found no indication that the Einstein account was compromised. US-CERT had the account disabled immediately to protect the integrity of Einstein. After Einstein administrators reviewed account logs, they confirmed the analyst's Einstein account was never logged into.

According to DHS SOC, the analyst was investigating why a PDF file sent to a (b)(2)High (b)(2)High user was not loading properly. During this investigation, the analyst opened the attachment and subsequently infected his system. Further investigation revealed that two (b)(2)High users' systems along with the analyst's system were infected with a key logger. These systems queried a suspicious domain but did not make any connections to the domain itself. The key logger files were sent to US-CERT for analysis which revealed that the DHS analyst was setting up his Secure Shell (SSH) client in order to log into his Einstein user account. There were no indications that the user logged into the account while the key logger was present on his system.

Analysis of the DNS system logs by the DHS SOC and US-CERT showed DHS requests to the suspicious domain but no evidence of sessions that would indicate data exfiltration had taken place.

Impact

Due to the analyst's Einstein account being disabled quickly and the confirmation that the account had not been logged into, the impact to DHS and the Federal government is minimal at this time. Although three systems were infected with the malware, there were no indications of agency data being exfiltrated from the network.

Current Actions**US-CERT**

- Notified DHS SOC of the Einstein 2 alert generated from the DHS query and response.
- Analyzed Einstein data to ensure no further compromises were observed.
- Notified the appropriate system administrator to have the user account disabled.
- Analyzed the key logger files provided by DHS SOC to determine if any connections to the suspicious domain were made.
- Coordinated with DHS SOC to investigate the details of the incident.
- Obtained a copy of the malware for analysis.
- Continue to monitor this activity and provide assistance to the agency as needed.

DHS SOC/DHS (b)(2)High

- Coordinated with US-CERT to provide details of the incident, the related key logger files and associated malware.
- Removed the infected (b)(2)High systems from the network.

~~Unclassified/For Official Use Only~~

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.



Unclassified/For Official Use Only

NPPD Information Bulletin

UPDATE DDoS Attacks Against Agency Websites

Executive Summary

On July 4, 2009, US-CERT received a report from the (b)(2)High of a possible Distributed Denial of Service (DDoS) attack against their web servers and those of several components. The DDoS severely degraded the availability of their websites. Following the initial report from (b)(2)High US-CERT proceeded to test the availability of other major public websites operated by executive branch agencies. From July 4-6, 2009, the following agencies either reported experiencing similar attacks or were notified by US-CERT of degraded performance of their websites:

(b)(2)High

On July 6, 2009, US-CERT received an anonymous tip that (b)(2)High was also affected by this DDoS attack. US-CERT contacted (b)(2)High and confirmed that they were experiencing an ongoing DDoS attack, but that their websites were not affected due to carrier level black-holing and broad blocks on PAC-ASIA IP addresses.

At this time, reporting from all impacted parties suggests that the majority of the botnet clients involved in these attacks are located in the Asia Pacific region, although the specific botnet(s) involved are not known.

Impact

US-CERT has contacted all affected agencies to determine if they are back online and if not, the steps they are taking to do so. (b)(2)High is working with Sprint to initiate a carrier level block while (b)(2)High is back online after Verizon initiated a carrier level block. US-CERT is still awaiting responses from the other affected agencies.

Current Actions

US-CERT

- Continues to monitor and analyze Einstein data for signs of additional agencies being attacked.

~~Unclassified/For Official Use Only~~

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

- Reached out to the National Communications Center (NCC) Watch and NCI-JTF to provide situational awareness and issue a request for information for any additional details from other partners in the community.
- Reached out to the impacted agencies for additional information, including log files and other technical data which could be used to diagnose and counter this type of attack.
- Contacting Akamai to obtain more information regarding these attacks.
- Organizing an engineer to engineer call with (b)(2)High to better understand the defensive measures they implemented.
- Conducting a CIO/CISO conference call on Tuesday, July 7, 2009, to review defensive steps agencies can take during a DDoS, web security best practices, and the recent Microsoft Video ActiveX Control vulnerability.
- Requested (b)(2)High contact CIO/CISO's prior to conference call to provide them updated information and also to ask for updated status information.

UPDATE – 7/7/2009 am

- US-CERT/NCC conducted a conference call with the ISPs, including Verizon, Sprint, AT&T, and Qwest. US-CERT agreed to the following actions on the call and has completed all of these.
 - Sent each individual carrier a list of their customers affected.
 - Sent a technical description of the issue to each carrier.
 - Compiled and sent sanitized flow data to each carrier for review.
 - Sent each carrier a technical contact for engineer to engineer collaboration.
- Spoke with Akamai regarding information sharing concerning this incident. Akamai stated they could not share information with US-CERT because US-CERT is not their customer.
- Identified the (b)(2)High web site as a victim web site via their Einstein 1 sensor.
- Requested DHS SOC reach out through (b)(2)High as the customer and request further information concerning this incident.
- Conducted an engineer to engineer call with (b)(2)High to discuss their defensive mitigation strategy.
- Working with NCSD's National Security Deployment branch to develop a script to determine if a department/agency web site is up and returning pages.
- (b)(2)High

UPDATE – 7/7/2009 pm

- Contacted the six affected agencies to determine if their websites and the websites of their components were back up and functioning properly. All affected agencies reported they are back online.
- Conducted a Federal Department and Agency (D/A) CIO/CISO Call:

~~Unclassified/For Official Use Only~~

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

- Encouraged all Departments and Agencies to know their carrier, web provider, or caching provider (i.e. Sprint, AT&T, Verizon, Qwest, etc.), including contact information for use in time of emergency.
- Reviewed the Tactics, Techniques and Procedures of this DDoS.
- Warned the D/As about the dangers of Structured Query Language (SQL) injection attacks as three D/As were shown to be vulnerable to these types of attacks. SQL injection is an attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.
 - Recommended all D/As test their websites for these vulnerabilities and warned that SQL Injection is a favored exploit for the highest threat actors. Additionally, US-CERT reminded the participants that web attacks often led to data exfiltration attacks, not necessarily just web site defacement.
- Reviewed the Microsoft ActiveX vulnerability² and associated mitigation strategies.
- Released a Federal Information Notice (FIN) to the GFIRST community via the US-CERT portal to provide departments and agencies details about these attacks as well as recommendations for detecting and mitigating them.
- Released a Critical Infrastructure Information Notice (CIIN) to the ISACs, Critical Infrastructure partners and U5 communities via the US-CERT portal to provide organizations details about these attacks as well as recommendations for detecting and mitigating them.
- Participated in a telecommunication engineer working group:
 - Received malware binary:
 - [Redacted] (b)(2)High
 - Reverse engineering and analyzing binary code.
 - Malware Analysis produced a file with a target domain list:
 - Contacted additional possible victim sites
 - .mil sites – JTFGNO contacted
 - Nsy.com, usbank.com – [Redacted] (b)(2)High
 - Finance.yahoo.com, usauctionslive.com, washingtonpost.com – contacted these organizations directly
 - [Redacted] (b)(2)High
- Developing a script to test website health.

UPDATE – 7/8/2009 (pm)

¹ http://www.us-cert.gov/reading_room/sql200901.pdf

² <http://www.microsoft.com/technet/security/advisory/972890.msp>

Unclassified/For Official Use Only

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

**The data contained in this report shall not be altered prior to any redistribution.
Distribution to organizations outside of DHS should be coordinated with US-CERT.**

- Shared the NPPD Information Bulletin with the DHS NOC for distribution to the White House Situation Room, the Office of Legislative Affairs (OLA) for distribution to the Capitol Hill staff and (b)(2)High
- Participated in a conference call with Senate Majority and Minority Staffers from the Senate Homeland Security and Government Affairs Committee regarding the DDoS event.
- Participated in a conference call with Congressman Langevin and staff regarding the DDoS event.
- (b)(2)High Preliminary reports indicate the malware is known.
- Coordinated with DHS Public Affairs to develop Public Affairs Guidance (PAG) regarding the DDoS attacks and mitigation strategies.
- Contacted the six affected agencies to determine if their websites and the websites of their components were functioning properly and if they had any new information to share with US-CERT. All affected agencies reported their sites are functioning properly and they had no new information to share.
- JTF-GNO reported the effects of the DDoS have been minimized on .mil. JTF-GNO also conducted malware analysis that indicated this malware is known.
- Coordinated information sharing with the New York Stock Exchange (NYSE) regarding the attacking IP addresses and mitigation strategies.
- Shared the malware binary with Antivirus Vendors (Symantec, McAfee, TrendMicro and Microsoft) and Security Information and Event Management (SIEM) tool vendors (ArcSight, EMC/RSA, Symantec, Netwitness) (b)(2)High All indicated this is known malware. Antivirus vendors have current signatures already available and recommend updating antivirus software and scanning systems.
- Conducted conference calls with the various Information Sharing and Analysis Centers (ISACs) and Antivirus Vendors to discuss the status of the DDoS attacks, the latest details surrounding the attacks, indicators and mitigation strategies.
- Assisting (b)(2)High in developing a brief for the President of the United States.
- Shared three command and control IP addresses with Communications ISAC (COMMS-ISAC) that were found in the malware code. COMMS-ISAC is sharing this information with their constituents and requesting the ISPs initiate blocks for those IP addresses.
- (b)(2)High
- Notified the (b)(2)High of a formal request from the Korean Embassy made to the National Cyber Security Division (NCSD) to seize the Command and Control machine determined to have been located in the United States.
- Shared information with Internet Corporation for Assigned Names and Numbers (ICANN) and will continue to work with them regarding this issue.
- Briefed CIO/CISOs with an update on the DDoS activity at the Information Security Identity Management Council (ISIMC).

Unclassified/For Official Use Only

**The data contained in this report shall not be altered prior to any redistribution.
Distribution to organizations outside of DHS should be coordinated with US-CERT.**

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

- Supported the Deputy Undersecretary in connection with Press interviews and inquiries related to the DDoS attacks.
- Developing a technical information product detailing the characteristics of these DDoS attacks as well as detection and mitigation strategies that can be distributed outside the Federal government. This product is being developed due to an overwhelming number of requests for technical information.
- Conducting a conference call with international partners (Usual 5) on Thursday, July 9, 2009 at 7 AM EST.
- Current indicators show that the DDoS attacks within the United States have stabilized while activity in Korea continues at a high rate. US-CERT believes the stabilization within the United States is due to broad carrier level blocks.

UPDATE 7/9/2009

- Conducted a conference call with International Partners (U5) to discuss the status of the DDoS attacks, the latest details surrounding the attacks, indicators and mitigation strategies.
- Participated in a conference call with Opsec-Trust (aka, Ops-Trust) to discuss details of the DDoS attacks and share information across the community. Ops-Trust is a highly vetted community of security professionals focusing on the operational robustness, integrity, and security of the Internet.
- Contacted the Department of State to inquire about open source reporting that stated the American Embassy in Korea was affected by these DDoS attacks. The Department of State reported no observed or reported issues with the American Embassy in Korea.
- Contacted JTF-GNO to confirm open source reporting that usfk.mil was under renewed DDoS attack. JTF-GNO reported no issues.
- (b)(2)High had to fail over to an alternate content site due to concentrated DDoS activity against one of their web servers. The site was offline for six minutes, but has since resumed normal functionality.
- Received detailed malware analysis report from JTF-GNO. US-CERT is reviewing this report.
- Shared details and mitigation strategies for the DDoS attacks with the International Watch and Warning Network.
- Received additional information regarding new command and control IP addresses. US-CERT is currently vetting and confirming this information.
- Conducting a conference call with IT-ISAC on Friday, July 10, 2009 at 2:00 EDT to discuss the details and mitigation strategies of the DDoS attacks.
- Developing a detailed timeline of events surrounding these DDoS attacks.

UPDATE 7/10/2009

- Director of US-CERT briefed Secretary Napolitano on the DDoS incident.
- Director of US-CERT briefed Deputy Secretary Lute on the DDoS incident.
- Director of US-CERT briefed HPSCI staff on the DDoS incident.

Unclassified/For Official Use Only

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.

- Conducted conference calls with MS-ISAC and IT-ISAC to discuss the DDoS attacks.
- Released an updated Federal Information Notice (FIN) to the GFIRST community and an updated Critical Infrastructure Information Notice (CIIN) to the ISACs, Critical Infrastructure partners and U5 communities.
- Released a Malware Initial Findings Report (MIFR) to the GFIRST community, ISACs, Critical Infrastructure partners and international community (U5) via the US-CERT secure portal. This report details initial analysis of the malware related to the DDoS attacks.
 - US-CERT malware analysis has determined that several compromised sites related to this DDoS incident were hosting flash.gif files containing an embedded executable program. This executable program will scan the infected system for specific file extensions. When a match occurs, the malicious executable program will compress the contents of the hard drive into a password protected zip file which will render the system unbootable.

NCC

- NCC/US-CERT conducted a conference call with ISPs to include AT&T, Sprint, Verizon, and Qwest.

Unclassified/For Official Use Only

The data contained in this report shall not be altered prior to any redistribution. Distribution to organizations outside of DHS should be coordinated with US-CERT.



~~Unclassified/For Official Use Only~~
NPPD Information Bulletin
New Variant of Clampi Trojan

Executive Summary

On July 11, 2009, the (b)(2)High reported that an unknown Trojan had infected up to 155 systems. US-CERT Einstein analysis conducted on July 13 did not reveal any significant anomalous activity emitting from (b)(2)High network. On July 15, (b)(2)High CSIRC was able to identify the Trojan as a variant of Clampi.

The Clampi Trojan has been circulating since early 2008. Clampi has the ability to propagate itself across a Windows domain via "psexec" which is a legitimate remote process execution tool provided by Microsoft. (b)(2)High attempted to implement a Group Policy Object (GPO) on July 15 to eliminate all copies of psexec and thus prevent Clampi from spreading. It was then discovered that this variant of Clampi makes duplicates of psexec, changing the filename as it does, which prevents the GPO from stopping the spread of the Trojan.

At approximately 2200 on July 15, (b)(2)High CSIRC contacted US-CERT to update that the Clampi Trojan had spread widely across (b)(2)High networks and was resisting attempts at containment and cleanup. Via interaction with Symantec, (b)(2)High CSIRC had learned that the variant of Clampi infesting their systems is a new variant. Symantec Security Response has stated that an increased number of Clampi infections have been observed since July 1, 2009.

Impact

The impact of this incident to the (b)(2)High is considered to be moderate; although the degree of infection across the network and difficulty of remediation are high, the (b)(2)High has not yet reported a significant impact to mission-critical operations.

Summary of Malware

Associated Active Domains/IPs:

```
78[dot]47[dot]61[dot]229 try[dot]mojitoboom[dot]in
64[dot]22[dot]130[dot]201 direct[dot]matchbox[dot]vc
64[dot]22[dot]131[dot]2 pop3[dot]re-factoring[dot]cn
96[dot]6[dot]147[dot]49 secure[dot]loderunner[dot]in
```

If a user with a privileged account (system administrator) logs onto a compromised system, the malware propagates using a legitimate service (psexec) under the account. If this method of propagation is not available, the malware attempts to connect to three accounts (administrator, guest, noguest) using a blank password. Please note, the malware does not attempt brute force access into the accounts.

The initial infection vector is still being researched at this time, but does include possible delivery via dropper malware.

Initial analysis indicates a low antivirus detection rate for the malware binary.

Current Actions

US-CERT

- Published a GFIRST Alert to warn the community of the threat.

July 16, 2009

Point of contact: US-CERT 703-235-5111

- Contacted partner organizations to include CMU/SEI, JTF-GNO, and NTOC to request more information and analysis of this Trojan.
- Will continue to provide assistance to the (b)(2)High as needed.

Updates from this morning:

- Reviewed Einstein for traffic to the resolving IPs of the domains described in the GFIRST Alert and found no reason to believe any other agencies are experiencing significant outbreaks of this malware at this time.
- Completed an Initial Findings Report analysis of malware samples received from (b)(2)High
- Contacted (b)(2)High CSCIRC at 14:00 to obtain most recent update.

(b)(2)High

- Applying updated AV signatures as they become available, accompanied by more intensive AV scanning and cleaning policies network-wide.

~~Unclassified/For Official Use Only~~



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Critical Infrastructure Information Notice

CIIN-09-188-01A UPDATE

July 10, 2009

Distributed Denial of Service Attacks Against US Web Sites

Overview

US-CERT has confirmed that multiple organizations have been impacted by massive Distributed Denial of Service (DDoS) attacks against their public-facing web sites. These attacks began on July 4, 2009.

US-CERT is issuing this notice to warn organizations of this activity and to help mitigate against continued attacks of a similar nature.

Details

A DDoS attack is an attempt to significantly degrade the availability of a system by overloading it with network traffic and/or service requests until it can no longer function as intended. The DDoS attacks addressed by this document appear to utilize at least four different attack vectors:

- **Flooding the target IP address with UDP traffic on port 80.** Since this vector utilizes connectionless UDP instead of TCP, it is possible that the source IP address may be spoofed. UDP port 80 traffic is not normally used for legitimate communications and thus is relatively trivial to detect and block.
- **Flooding the target IP address with TCP traffic on port 80,** generally using SYN packets, but in some cases sending other flags or combinations of flags such as ACK, RST, SYN-RST or RST-ACK. SYN flooding using TCP is difficult to detect and block without affecting legitimate users. As with the UDP floods described above, these attacks may use spoofed addresses as the source IP if the goal of the attack does not require a full-connect handshake to succeed.
- **Full-connect HTTP GET requests (also using TCP port 80) containing valid URLs.** It is not known at this time if these requests can be identified as malicious due to any anomalous attributes;

otherwise, such service requests will appear completely legitimate except for the abnormally high volume at which they are sent to the target.

- **Higher than usual volumes of ICMP Echo Request traffic (PING floods).** This activity is not as consistent and does not carry as significant an impact as the preceding attack vectors. This vector may also utilize spoofed source addresses.

Note that while three of the four attack vectors described above may use spoofed IP addresses, there have been no indications that significant amounts of spoofed source addresses are being used in these attacks at this time. US-CERT does want to caution organizations to practice due diligence in protecting their systems and be aware that source IP addresses related to this attack can and have changed.

UPDATE: Additional Analysis

Malware Analysis has revealed the following list of IPs have been identified command and control (C2) servers associated with this activity. Each of these servers is hosting a “/flash.gif” file, which is retrieved by the infected hosts.

IP Address	Country
117.18.237.20	AP, Asia/Pacific
85.255.198.237	BE, Belgium
85.255.207.100	BE, Belgium
174.142.97.10	CA, Canada
208.70.247.68	CA, Canada
67.205.112.104	CA, Canada
124.131.219.22	CN, China
58.215.76.82	CN, China
58.218.201.187	CN, China
60.191.185.71	CN, China
61.135.133.35	CN, China
61.135.134.251	CN, China
62.193.255.220	FR, France
80.239.186.20	FR, France
80.5.176.140	GB, United
83.138.162.11	GB, United
83.231.143.134	GB, United
200.6.218.194	GT, Guatemala
202.146.4.17	ID, Indonesia
122.208.224.55	JP, Japan
124.83.226.246	JP, Japan
202.143.88.6	JP, Japan
202.210.130.141	JP, Japan
202.222.19.89	JP, Japan
202.232.67.114	JP, Japan

IP Address	Country
202.32.225.45	JP, Japan
202.93.69.243	JP, Japan
203.104.255.196	JP, Japan
203.133.238.86	JP, Japan
210.133.105.115	JP, Japan
210.133.105.162	JP, Japan
210.167.34.106	JP, Japan
210.188.221.82	JP, Japan
211.13.210.84	JP, Japan
219.94.194.237	JP, Japan
43.253.232.40	JP, Japan
43.253.36.45	JP, Japan
43.253.37.80	JP, Japan
58.158.148.185	JP, Japan
61.125.141.51	JP, Japan
61.211.165.140	JP, Japan
210.102.100.150	KR, Korea
211.108.92.4	KR, Korea
211.236.177.177	KR, Korea
211.236.189.240	KR, Korea
211.49.162.205	KR, Korea
201.116.58.131	MX, Mexico
69.175.8.234	--, N/A
93.190.142.11	NL, Netherlands
94.75.218.85	NL, Netherlands
202.14.70.116	PK, Pakistan
195.239.111.51	RU, Russian
92.63.2.118	TR, Turkey
163.19.209.22	TW, Taiwan
203.66.134.19	TW, Taiwan
203.66.138.31	TW, Taiwan
203.66.138.32	TW, Taiwan
218.32.192.107	TW, Taiwan
61.31.202.65	TW, Taiwan
12.129.242.20	US, United
174.129.217.8	US, United
174.35.12.80	US, United
174.36.91.30	US, United
192.150.18.60	US, United
192.150.8.60	US, United
198.172.86.247	US, United
207.199.89.152	US, United
208.112.58.116	US, United

IP Address	Country
208.67.226.9	US, United
208.71.107.54	US, United
209.222.148.148	US, United
209.222.148.150	US, United
216.14.84.61	US, United
216.38.164.142	US, United
63.216.60.71	US, United
67.207.210.208	US, United
67.21.114.16	US, United
68.142.234.143	US, United
69.162.73.154	US, United
69.22.138.89	US, United
69.43.149.237	US, United
72.247.247.35	US, United
74.205.62.39	US, United
75.151.32.182	US, United
8.12.131.30	US, United
8.17.248.8	US, United

UPDATED: Recommendations

US-CERT recommends that organizations implement the following to help detect and mitigate the effects of similar DDoS attacks:

- Implement bogon¹ blocklists at the network boundary to ensure that attacks using spoofed source IP addresses are automatically blocked if the spoofed IP belongs to an invalid address range. More information regarding bogon address space is available at: <http://www.team-cymru.org/Services/Bogons/>
- Enable SYN Cookie functionality on public-facing servers. This may result in an impact to operations when not under attack.
- Ensure that all contact information for web hosting and internet service providers is up-to-date and that all operations personnel are aware of how to escalate critical information to the appropriate service representatives if a DDoS is detected.
- Monitor network traffic for any increase in UDP port 80, TCP ACK packets with no preceding SYN, or any other anomalous increase in traffic volume targeting a web server. If such increases

¹ "Bogon" is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). - http://en.wikipedia.org/wiki/Bogon_filtering

can be tracked to certain IP addresses with a high degree of confidence, then the IP address in question is participating in a DDoS attack. Consider blocking those IP addresses or address ranges with an Access Control List at the perimeter.

- Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls, in case an attack occurs.
 - A strong candidate for blocking by default on edge routers is UDP port 80.
- Monitor network egress points to ensure your network is not participating in these attacks. If you have internal systems communicating on UDP port 80, or attempting to reach any of the command and control IPs, then your network may be participating in the attacks.
- Establish accurate resource utilization baselines, and ensure that all critical systems have some degree of excess capacity for dealing with exigent circumstances.
- Review US-CERT Cyber Security Tip ST04-015 “Understanding Denial-of-Service Attacks”.

Organizations should follow their established internal procedures if any suspected malicious activity is observed, and report their findings to US-CERT for correlation against other incidents. US-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov

Voice: 1-888-282-0870

Incident Reporting Form: <https://forms.us-cert.gov/report/>

Document FAQ

What is a CIIN? A Critical Infrastructure Information Notice (CIIN) is intended to provide warning to US critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks.

I see that this document is labeled as UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). Can I distribute this to other people? Per the U//FOUO warning, this document is to be distributed only to those parties who have a valid “need to know.” It may be shared within a company, industry association, sector coordinating council, or ISAC/ISO if the receiving person or group has a *direct role in securing networks or systems that enable or support U.S. critical infrastructures*. If necessary, please contact US-CERT for clarification or specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Federal Information Notice-FIN-09-188-01A UPDATE

July 10, 2009

Distributed Denial of Service Attacks Against US Web Sites

Overview

US-CERT has confirmed that multiple federal agencies have been impacted by massive Distributed Denial of Service (DDoS) attacks against their public-facing web sites. These attacks began on July 4, 2009.

US-CERT is issuing this notice to warn agencies and organizations of this activity and to help mitigate against continued attacks of a similar nature.

Details

A DDoS attack is an attempt to significantly degrade the availability of a system by overloading it with network traffic and/or service requests until it can no longer function as intended. The DDoS attacks addressed by this document appear to utilize at least four different attack vectors:

- **Flooding the target IP address with UDP traffic on port 80.** Since this vector utilizes connectionless UDP instead of TCP, it is possible that the source IP address may be spoofed. UDP port 80 traffic is not normally used for legitimate communications and thus is relatively trivial to detect and block.
- **Flooding the target IP address with TCP traffic on port 80,** generally using SYN packets, but in some cases sending other flags or combinations of flags such as ACK, RST, SYN-RST or RST-ACK. SYN flooding using TCP is difficult to detect and block without affecting legitimate users. As with the UDP floods described above, these attacks may use spoofed addresses as the source IP if the goal of the attack does not require a full-connect handshake to succeed.
- **Full-connect HTTP GET requests (also using TCP port 80) containing valid URLs.** It is not known at this time if these requests can be identified as malicious due to any anomalous attributes; otherwise, such service requests will appear completely legitimate except for the abnormally high volume at which they are sent to the target.

This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of the US-CERT Operations Center at 1-888-282-0870. No portion of this report shall be furnished to the media, either in written or verbal form.

- **Higher than usual volumes of ICMP Echo Request traffic (PING floods).** This activity is not as consistent and does not carry as significant an impact as the preceding attack vectors. This vector may also utilize spoofed source addresses.

Note that while three of the four attack vectors described above may use spoofed IP addresses, there have been no indications that significant amounts of spoofed source addresses are being used in these attacks at this time. US-CERT does want to caution federal departments and agencies to practice due diligence in protecting their systems and be aware that source IP addresses related to this attack can and have changed.

UPDATE: Additional Analysis

Malware Analysis has revealed the following list of IPs have been identified command and control (C2) servers associated with this activity. Each of these servers is hosting a “/flash.gif” file, which is retrieved by the infected hosts.

IP Address	Country
117.18.237.20	AP, Asia/Pacific
85.255.198.237	BE, Belgium
85.255.207.100	BE, Belgium
174.142.97.10	CA, Canada
208.70.247.68	CA, Canada
67.205.112.104	CA, Canada
124.131.219.22	CN, China
58.215.76.82	CN, China
58.218.201.187	CN, China
60.191.185.71	CN, China
61.135.133.35	CN, China
61.135.134.251	CN, China
62.193.255.220	FR, France
80.239.186.20	FR, France
80.5.176.140	GB, United
83.138.162.11	GB, United
83.231.143.134	GB, United
200.6.218.194	GT, Guatemala
202.146.4.17	ID, Indonesia
122.208.224.55	JP, Japan
124.83.226.246	JP, Japan
202.143.88.6	JP, Japan
202.210.130.141	JP, Japan
202.222.19.89	JP, Japan
202.232.67.114	JP, Japan
202.32.225.45	JP, Japan
202.93.69.243	JP, Japan

IP Address	Country
203.104.255.196	JP, Japan
203.133.238.86	JP, Japan
210.133.105.115	JP, Japan
210.133.105.162	JP, Japan
210.167.34.106	JP, Japan
210.188.221.82	JP, Japan
211.13.210.84	JP, Japan
219.94.194.237	JP, Japan
43.253.232.40	JP, Japan
43.253.36.45	JP, Japan
43.253.37.80	JP, Japan
58.158.148.185	JP, Japan
61.125.141.51	JP, Japan
61.211.165.140	JP, Japan
210.102.100.150	KR, Korea
211.108.92.4	KR, Korea
211.236.177.177	KR, Korea
211.236.189.240	KR, Korea
211.49.162.205	KR, Korea
201.116.58.131	MX, Mexico
69.175.8.234	--, N/A
93.190.142.11	NL, Netherlands
94.75.218.85	NL, Netherlands
202.14.70.116	PK, Pakistan
195.239.111.51	RU, Russian
92.63.2.118	TR, Turkey
163.19.209.22	TW, Taiwan
203.66.134.19	TW, Taiwan
203.66.138.31	TW, Taiwan
203.66.138.32	TW, Taiwan
218.32.192.107	TW, Taiwan
61.31.202.65	TW, Taiwan
12.129.242.20	US, United
174.129.217.8	US, United
174.35.12.80	US, United
174.36.91.30	US, United
192.150.18.60	US, United
192.150.8.60	US, United
198.172.86.247	US, United
207.199.89.152	US, United
208.112.58.116	US, United
208.67.226.9	US, United

IP Address	Country
208.71.107.54	US, United
209.222.148.148	US, United
209.222.148.150	US, United
216.14.84.61	US, United
216.38.164.142	US, United
63.216.60.71	US, United
67.207.210.208	US, United
67.21.114.16	US, United
68.142.234.143	US, United
69.162.73.154	US, United
69.22.138.89	US, United
69.43.149.237	US, United
72.247.247.35	US, United
74.205.62.39	US, United
75.151.32.182	US, United
8.12.131.30	US, United
8.17.248.8	US, United

UPDATED: Recommendations

US-CERT recommends that agencies implement the following to help detect and mitigate the effects of similar DDoS attacks:

- Implement bogon¹ blocklists at the network boundary to ensure that attacks using spoofed source IP addresses are automatically blocked if the spoofed IP belongs to an invalid address range. More information regarding bogon address space is available at: <http://www.team-cymru.org/Services/Bogons/>
- Enable SYN Cookie functionality on public-facing servers. This may result in an impact to operations when not under attack.
- Ensure that all contact information for web hosting and internet service providers is up-to-date and that all operations personnel are aware of how to escalate critical information to the appropriate service representatives if a DDoS is detected.

¹ "Bogon" is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). - http://en.wikipedia.org/wiki/Bogon_filtering

- Monitor network traffic for any increase in UDP port 80, TCP ACK packets with no preceding SYN, or any other anomalous increase in traffic volume targeting a web server. If such increases can be tracked to certain IP addresses with a high degree of confidence, then the IP address in question is participating in a DDoS attack. Consider blocking those IP addresses or address ranges with an Access Control List at the perimeter.
- Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls, in case an attack occurs.
 - A strong candidate for blocking by default on edge routers is UDP port 80.
- Monitor network egress points to ensure your network is not participating in these attacks. If you have internal systems communicating on UDP port 80, or attempting to reach any of the command and control IPs, then your network may be participating in the attacks.
- Establish accurate resource utilization baselines, and ensure that all critical systems have some degree of excess capacity for dealing with exigent circumstances.
- Review US-CERT Cyber Security Tip [ST04-015 “Understanding Denial-of-Service Attacks”](#).

Agencies should follow their established internal procedures if any suspected malicious activity is observed, and report their findings to US-CERT for correlation against other incidents. US-CERT reminds agencies that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov

Voice: 1-888-282-0870

Incident Reporting Form: <https://forms.us-cert.gov/report/>

Document FAQ

What is a FIN? Generally labeled UNCLASSIFIED//FOR OFFICIAL USE ONLY (FOUO), a Federal Information Notice (FIN) is intended to provide warning to federal agencies when a particular cyber event/activity has affected **three or more** federal agencies. A FIN provides information about the cyber incident and makes recommendations for preventing or mitigating risks.

I see that this document is labeled as UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). Can I distribute this to other people? Per the U//FOUO warning, this document may be shared with personnel who have a valid “need to know” within your federal agency. In the case of a FIN, this is defined as a person or group that has a direct role in securing federal networks. If necessary, please contact US-CERT for clarification or specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.