FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 March 2016

Alert Number

MC-000070-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@ic.fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but not via publicly accessible channels.

The FBI is providing the following information with **high confidence**:

Summary

This report is an update to the FLASH released on 18 February 2016, Alert Number MC-000068-MW. Cyber criminals continue to use the ransomware MSIL/Samas.A to encrypt an infected host's files, allowing them to demand considerable sums of money in return for decryption keys. Actor(s) attempt to infect whole networks with MSIL/Samas.A, increasing the potential of extorting large sums of money from victims. The common method of payment for ransom is Bitcoin (BTC). This update is to provide information about the vulnerabilities and exploits used by the actor(s) for initial intrusion into victim networks.

Technical Details

The FBI previously identified that the actor(s) exploit Java-based Web servers to gain persistent access to a victim network and infect Windows-based hosts. The FBI also indicated that several victims have reported the initial intrusion occurred via JBOSS applications. Further analysis of victim machines indicates that, in at least two cases, the attackers used a Python tool, known as JexBoss, to probe and exploit target systems. Analysis of the JexBoss Exploit Kit identified the specific JBoss services targeted and vulnerabilities exploited. The FBI is distributing these indicators to enable network defense activities and reduce the risk of similar attacks in the future.

FBI indicators based on an ongoing investigation:

The JexBoss tool, publicly available on GitHub.com, prompts attackers to input the target URL for JexBoss to check for any of three vulnerable JBoss services: web-console, jmx-console, and JMXInvokerServlet. Depending on which vulnerabilities are detected, the tool then prompts the user to initiate

corresponding exploits. The tool's exploits are collectively effective against JBoss versions 4, 5, and 6. The payload of each exploit is a Web application Archive (.war) file, "jbossass.war". A successful exploit results in unpackaging the .war file and utilizing jbossass.jsp to deploy an HTTP shell for the attacker.

Following initial infection of the network with MSIL/Samas.A, the actor(s) connect via RDP sessions. An open source tool, known as reGeorg, is used to tunnel the RDP traffic over the established HTTP connection. The actors use the Microsoft tool csvde.exe to determine the hosts reporting to the active directory. A list of all hosts found in the directory is compiled into a .csv file or other similar file type. Finally, the actor(s) distribute the ransomware to each host in the network using a copy of Microsoft's psexec.exe.

An updated complete list of indicators for known variants and associated files is attached to this e-mail.

Disclaimer: Information provided below is still being vetted. Some of the information is taken from private industry reporting.

Relevant JBoss Common Vulnerabilities and Exposures (CVEs):

CVE ID	Affected Service
CVE-2015-5188	web-console
CVE-2010-2493	web-console
CVE-2010-1428	web-console
CVE-2012-3347	jmx-console
CVE-2011-2908	jmx-console
CVE-2010-0738	jmx-console
CVE-2013-4810	JMXInvokerServlet

JexBoss Specific Mitigations

JBoss developers published a guide to configuring and hardening JBoss, available at https://developer.jboss.org/wiki/SecureJboss?_sscc=t.

Many of the known vulnerabilities have been patched in the most recent version of JBoss, now known as Wildfly.

Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey