MS-ISAC

TECHNICAL WHITE PAPER

February 2016

Timely Patching Reduces System Compromises

Authored by: Katelyn Bailey, Cyber Intel Analyst

INTRODUCTION

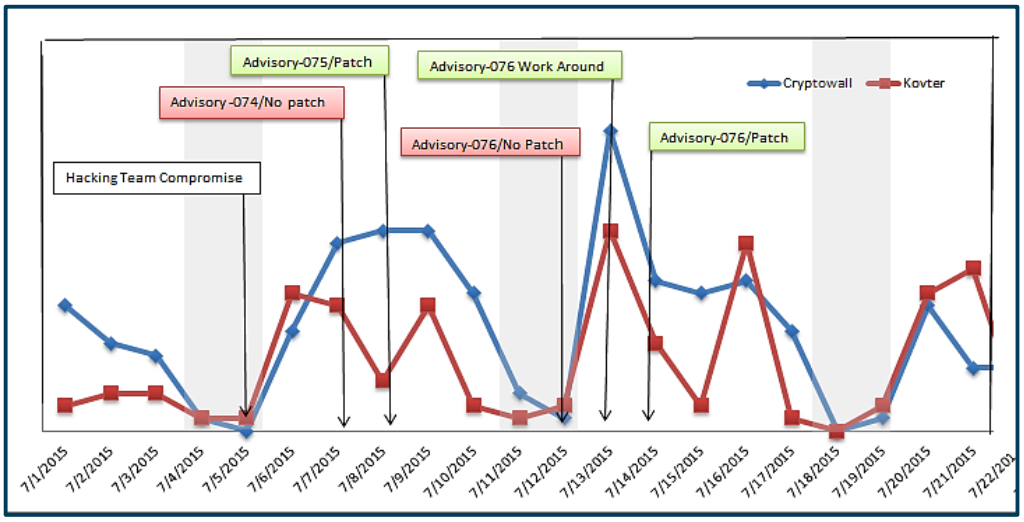
Patching and updating systems is one of the most important cyber security procedures to implement in order to protect a system from being compromised. Analysis of Multi-State Information Sharing and Analysis Center (MS-ISAC) data proves that timely patching can prevent most infections and system compromises.

DETAILS

Patches and security updates address software vulnerabilities that may allow malicious cyber threat actors access to information systems or a network. Once vulnerabilities are publicly announced, the information is available to anyone, including cyber threat actors. It is essential to quickly patch vulnerable systems as the disclosed information makes it easier for cyber threat actors to find and target systems. Research has shown that despite the proven effectiveness of patching, systems often remain vulnerable with out-of-date software and plugins for extended periods.

The primary infection vector in at least 95% of all the incidents investigated by MS-ISAC was an unpatched vulnerability in an operating system, software, or plugin.

In July 2015 cyber threat actors exfiltrated data from an Italian company, which included information on four zero-day exploits that targeted vulnerabilities in common software. The Angler Exploit Kit, which dropped both the CryptoWall and Kovter malware in July 2015, incorporated each of the four exploits immediately following its release to the public. The below graph shows the dates the zero-days were made public, the dates of patch releases and the attempted CryptoWall (blue) and Kovter (red) malware infections detected by MS-ISAC sensors.



MS-ISAC recommends implementing a routine patching program and applying critical patches immediately after appropriate testing.

While a significant increase in malware is observed after the vulnerability is publically announced, a sharp decrease in infections was identified after the patch was released and installed.

System compromises have the potential to cause ramifications beyond the effort required to remediate the immediate issue. Once a malicious actor infiltrates a system through an unpatched operating system, software, or plugin, they could conduct malicious activity affecting the data's confidentiality, availability, and/or integrity. There may be loss of public trust, reputation damage, and substantial costs associated with the compromise, including paying legal fees, or paying for victim's credit monitoring if personally identifiable information (PII) is lost or exposed.

RECOMMENDATIONS

In addition, MS-ISAC recommends organizations follow the recommendations of the National Campaign for Cyber Hygiene to create nationwide awareness of cyber security issues and make measurable and sustainable improvements. More information on the National Campaign for Cyber Hygiene can be found at: https://www.cisecurity.org/cyber-pledge/.

1. Count: Know what's connected to and running on your network.
2. Configure: Implement key security settings to help protect your systems.
3. Control: Limit and manage those who have administrative privileges.
4. Patch: Regularly update all apps, software, and operating systems.
5. Repeat: Repeating each step is essential to maintaining security of your systems.

MS-ISAC recommends developing a "realistic" program for patch management that identifies new patches, identifies which systems are vulnerable, downloads the patch from an authoritative source, tests and verifies the patch in the operating environment, and applies the patch to all devices. Development of a patch management program is not a simple task, and companies ought to prepare for challenges, such as ensuring all devices are regularly updated, even when employees ignore or cancel notifications. The maintenance of updates may prove more of a challenge on some devices, such as systems that may not be on the network, systems which are outsourced (e.g. a company website), take home devices assigned to employees, and those devices that are not used on a regular basis (e.g. conference room systems). Following the steps outlined in the National Campaign for Cyber Hygiene and signing up for the MS-ISAC Cybersecurity Advisories (http://msisac.cisecurity.org/advisories/) is recommended to ensure that organizations remain aware of critical vulnerabilities and the release of security updates.

The Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber Defense, Version 6.0, Control 4 - Continuous Vulnerability Assessment and Remediation describes the recommendations for running automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis to help deliver prioritized lists of the most critical vulnerabilities. Deploying not just a patch management system, but software update tools for operating systems, software, and applications, on all systems for which such tools are available and safe, is another part of CIS Control 4. Patches should be applied to all systems, even systems that are properly air gapped. It is a good idea to apply patches to riskiest vulnerabilities

first, using the list of most critical vulnerabilities identified through scanning. The CIS Controls can be found at: https://www.cisecurity.org/critical-controls.cfm

Develop a patch management program

Don't forget to update plugins!

Sign up for MS-ISAC Advisories

Remember, time is of the essence!

TLP: WHITE The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.

TLP: WHITE The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information, as well as 24x7 cybersecurity assistance for SLTT governments, is available by contacting the MS-ISAC at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/.