Malware Using Exploits from Shadow Brokers Leak Reportedly in the Wild

April 26, 2017

The effects of the recent leak of malware, hacking tools, and exploits by hacking group Shadow Brokers is now coming to light as two malware, whose attack chain were derived from Shadow Brokers's leak, have been reportedly sighted in the wild: AES-NI ransomware (detected by Trend Micro as RANSOM_HPSOREBRECT.SM) and the DoublePulsar backdoor. What can organizations and end users do to mitigate these threats?

AES-NI's Developer Claims to Use EternalBlue Exploit

A version of AES-NI ransomware, so named based on its ransom note and unrelated to the homonymous cryptographic instruction set, purportedly uses the "EternalBlue" exploit, which was one of the many included in the Shadow Brokers leak. The exploit takes advantage of a remote code execution vulnerability in Windows Server Message Block (SMB) server found in almost all Windows operating systems (OS). Microsoft has addressed this via a patch (MS17-010) released last March 14, 2017.

According to reports, AES-NI's developer professed to have successfully used EternalBlue to install his own crafted ransomware to vulnerable systems or servers. His only proof is a screenshot—posted to his now defunct Twitter account—of the developer scanning the targeted server for exploits drawn from Shadow Brokers's dump.

[READ: Protect, Contain, and Recover: How Organizations can Defend against Ransomware]

However, security researchers dismissed the claim, noting that the attacker may not be using the exploit after all, but may instead be abusing Remote Desktop Protocol (RDP) and taking advantage of poorly secured internet-exposed remote desktops or servers. This has been the modus operandi of another ransomware family Crysis (RANSOM_CRYSIS), which Trend Micro initially found targeting Australian and New Zealand businesses in September 2016. Crysis's operators have since ramped up their malicious activities, and were found in February 2017 targeting SMEs and large enterprises worldwide, especially those in healthcare. The attack chain involves the bad guys brute forcing their way into the system, then dropping and executing the payload in the compromised machine.

AES-NI's activity is also consistent with Trend Micro's ongoing monitoring. Despite being a newcomer in the ransomware landscape (our earliest detection and monitoring were in February 2017), the ransomware family had a modest spike in activity that topped out around the week of April 17–24, 2017.

According to the ransom note of AES-NI's "NSA EXPLOIT EDITION" version, infected files are encrypted using AES-256 algorithm in Electronic Codebook (ECB) mode. Victims are urged to contact the developer via email, BitMsg (a web

forum. Other malware analysts cite this version demands a ransom of 1.5 Bitcoins (equivalent to USD $1,900 as of April 25, 2017), with the cybercriminal offering free decryption to victims from the Commonwealth of Independent States.

[READ: What does Shadow Brokers's malware dump mean for enterprises?]

DoublePulsar Infections Soaring

Another notable threat that's currently making headlines—and one that can be traced to Shadow Broker's leak—is DoublePulsar, a remote access Trojan/backdoor that appears to be the payload for many of the exploits found in the dump. DoublePulsar is now apparently being adopted by various threat actors since its public release by Shadow Brokers.

DoublePulsar is a memory-based kernel payload that allows attackers to inject arbitrary Dynamic-link Library (DLL) files to the system processes and execute shellcode payloads, ultimately providing attackers unprecedented access to infected x86 and 64-bit systems. Trend Micro's continuous analysis of the dump suggests that EternalBlue is one of the exploits that also executes DoublePulsar as payload. EternalBlue is part of the Fuzzbunch framework (also found in the dump) responsible for executing the exploits.

The attacks also involve sending malicious SMB requests to the same port where the targeted machine is running the SMB service (Port 445), which is typically left exposed in the Internet. Internet scans for DoublePulsar infections indicate that it is currently increasing, with more than 40,000 SMB-run (and publicly exposed) machines reported to be infected.

DoublePulsar has been addressed by Microsoft via the same update (MS17-010) that patches the security flaws in SMB protocol across various Windows system and server OSes.

[READ: How do backdoors work, and how can they be thwarted?]

How can these threats be mitigated?

While these threats can pose significant risks to businesses and end users alike, many of the exploits and malware recently leaked by Shadow Brokers leverage

applying the latest patches and keeping the systems up-to-date.

Here are some best practices that enterprises and individual users can adopt to mitigate these threats:

- Disable unnecessary, outdated, and unsupported components (or applications/software that use them); blocking them at the network level (like blocking TCP Port 445 and related protocols) is also recommended
- Deploy firewalls as well as intrusion detection and prevention systems to monitor and validate the traffic traversing in and out of the network
- Apart from fostering security awareness in the workplace, provide actionable instructions like requiring employees to employ virtual private network (VPN) when remotely accessing company assets
- Provide additional layers of security to remote connections—from authentication and least privilege principle to encryption of remote desktops
- On top of keeping systems up-to-date, enforce a stronger patch management policy, and employ virtual patching
- Migrating to newer operating systems and software can also reduce the risks caused by the use of unsupported software
- Employ network segmentation to limit access to sensitive data (and networks), as well as data categorization to lessen the impact of a breach

Trend Micro Solutions:

Trend Micro™ Deep Security™ and Vulnerability Protection provide virtual patching that protects endpoints from threats that abuse unpatched vulnerabilities. OfficeScan's Vulnerability Protection shields endpoints from identified and unknown vulnerability exploits even before patches are deployed. Trend Micro™ Deep Discovery™ provides detection, in-depth analysis, and proactive response to attacks using exploits through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect similar threats even without any engine or pattern update.

Trend Micro's Hybrid Cloud Security solution, powered by XGen™ security and features Trend Micro™ Deep Security™, delivers a blend of cross-generational threat defense techniques that have been optimized to protect physical, virtual, and cloud workloads/servers.

TippingPoint's Integrated Advanced Threat Prevention provides actionable security intelligence, shielding against vulnerabilities and exploits, and

XGen™ security, use a combination of technologies such as deep packet inspection, threat reputation, and advanced malware analysis to detect and block attacks and advanced threats.

Deep Discovery Inspector protects customers from AES-NI ransomware's malicious network via this DDI Rule:

- DDI Rule ID 1078: 'Possible TOR node certificate detected'

TippingPoint protects customers from AES-NI ransomware via this ThreatDV filter:

- 30623: TLS: Suspicious SSL Certificate (DGA)

TippingPoint customers are protected against EternalBlue via this MainlineDV filter:

- 27928: SMB: Microsoft Windows SMB Remote Code Execution Vulnerability (EternalBlue)

An in-depth information on Trend Micro's detections and solutions for Trend Micro Deep Security, Vulnerability Protection, TippingPoint and Deep Discovery Inspector can be found in this technical support brief.

Posted in Cybercrime & Digital Threats, Vulnerabilities

Related Posts

A Record Year for Enterprise Threats

US Cities Exposed in Shodan

New Windows SMB Zero-Day Leads to Denial of Service on Vulnerable Systems

Netgear Vulnerability Calls for Better Router Security across Businesses and Homes

A Rundown of the Biggest Cybersecurity Incidents of 2016

Recent Posts

Malware Using Exploits from Shadow Brokers Leak Reportedly in the Wild

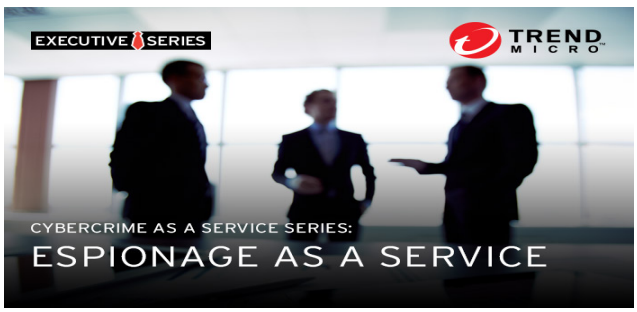
BrickerBot Malware Emerges, Permanently Bricks IoT Devices

Ransomware Recap: Threats from Open Source Code on the Rise

We Recommend

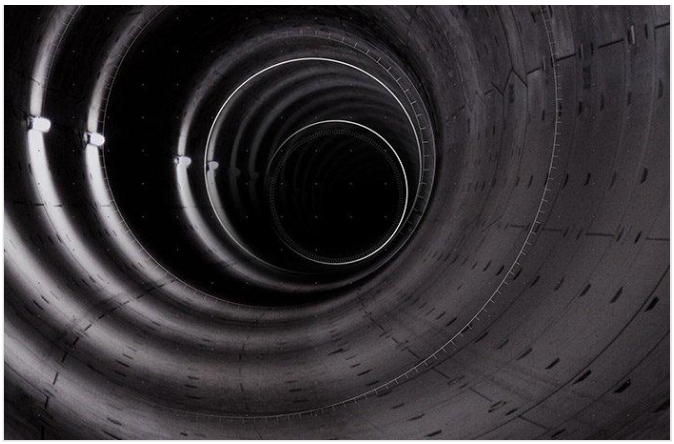
Ransomware Recap: Expanding Distribution Methods

A Record Year for Enterprise Threats



Espionage as a Service: A Means to Instigate Economic Espionage

Leaked D&B Database Highlights the Risks of Data Collection



The latest research and information on the deep web and the cybercriminal underground.
Learn more about the Deep Web

From business process compromise to cyberpropaganda: the security issues that are expected to matter in 2017.
View the 2017 Security Predictions