New report undresses 'Russian speaking' APT 28

Insiders are bigger threat than perimeter: report

Anonymous fesses up to DDoS attacks on Turkish servers

December 2015 Issue

Editorial

Let's just call it "The era of IT security"

Subscribe

Archive

Adrian Bridgwater

December 22, 2015

New botnet found popping PoS systems via Windows update vulnerability

Share this article:

- facebook
- twitter
- linkedin

- google
- 0 Comments
- Email
- Print

New research from security analysis firm Trend Micro has highlighted a new strain of point-of-sale (PoS) malware that comes on the back of related incidents in hotel checkout systems.

New botnet Operation Black Atlas spotted in wild

Researchers say the malware they have identified is linked to an early version of a potentially powerful, adaptable and invisible botnet that seeks out PoS systems within networks.

Trend Micro threat analysts Erika Mendoza and Jay Yaneza explain that this malware has already extended its reach to small and medium-sized business networks all over the world, including a healthcare organisation in the US. The name Operation Black Atlas is in reference to BlackPoS, the malware primarily used in this operation.

Multi-state malware multiplier

"Operation Black Atlas has already spread to a multi-state healthcare provider, dental clinics, a machine manufacturer, a technology company focusing on insurance services, a gas station that has a multi-state presence and a beauty supply shop. It continues to spread across small and medium-sized businesses across the globe, using the modular Gorynych/Diamond Fox botnet to exfiltrate stolen data," write Mendoza and Yaneza.

The malware works as follows: the cybercriminals behind the attacks use penetration testing tools (including brute force attacks) to gather information about the networks they seek to infiltrate. A second batch of tools is used to 'enter' the networks in question.

The cyber-criminals then familiarise themselves with the environment they find inside the network before installing the PoS threat including the modular malware Gorynych. The perpetrators are then in a position to start gathering dumps of financial information and other privacy-related data.

Nefarious nerds

Trend Micro explains that most of the penetration testing tools used here are available online. It is only down to the malicious application of this software by the cyber-criminals that these products are used for nefarious means.

The call to action here centres on what amounts to an instruction to network defence engineers to not only enforce stricter policies on password creation and maintenance – they must also configure breach detection systems to log activities like port or vulnerability scanning or brute-force attempts for inspection.

"This is just the latest in a string of attacks aimed at small and medium-sized businesses," said Neill Feather, president of SiteLock, a provider of cloud-based website security.

Feather told SCMagazineUK.com, "These organisations are 'absolutely under assault' by cyber-criminals who have realised that they are, by and large, unequipped and unprepared to withstand sophisticated attacks on their infrastructure and web-facing applications."

Feather says that from h vantage point, "We see the eight million customer websites we protect attacked conti where hackers are looking for the same type of weaknesses identified in PoS systems in this attack. Small businesses are beginning to realise that they need to protect themselves like ger brethren… and that trend is hopefully accelerating."

The PoS threat abuses a legitimate function, the Windows Background Intelligent Transfer Service (BITS) or bitsadmin.exe, which can be used to transfer files to and from Microsoft and is typically used to download upd stems.

"It can easily bypass firewalls and has long been used by malware to sneak in malicious downloads," say Mendoza and Yaneza. "Every network has its own nuances and patterns. As such, applying a single PoS strategy and hoping for the best is out of the question."

The pair recommend all IT administrators to stay up to date on known and latest PoS malware and technical staff in these roles make themselves aware of indicators of compromise (IOCs) lists that can help betray the presence of these threats.

Old device, bigger exp

Research analyst Andrew Conway at Cloudmark spoke to SC to remind us what any researcher will tell you: the longer a e is around, the more time they have to find and exploit hardware and software vulnerabilities. "There are still PoS devices out there running the Windows XP operating system that is no longer supported by Microsoft," he said.

Cloudmark's Conway underlines how important it is for any Internet of Things (IoT) device to have a way for the manufacturer to upgrade the installed firmware or software on the device and to patch any security vulnerabilities that are discovered.

Conway concludes, "However, that upgrade mechanism can itself be a way to compromise the device, as we saw recently in both the Cisco and Jeep hacks. It should be a standard for all IoT devices that they only accept updates that are cryptographically signed by the manufacturer. In the case of PoS devices there are additional problems. Even if an upgrade path exists, the manufacturer cannot apply those fixes directly, but must rely on the retail organisation that purchased them to download and install the fixes. Furthermore, they cannot publish the fixes as soon as they have them. All processing of credit card transactions should satisfy the Payment Card Industry Data Security Standard (PCI DSS). Software should be validated as complying with this standard before publication."

Official advice from Trend Micro specifies that smaller organisations should implement a firewall or ACL on remote access services and change default credentials of PoS systems and other internet-facing devices. The firm says it is monitoring the ongoing activity related to these threats and will make follow-up reports on the situation if necessary.

This article originally appeared on SC Magazine UK.