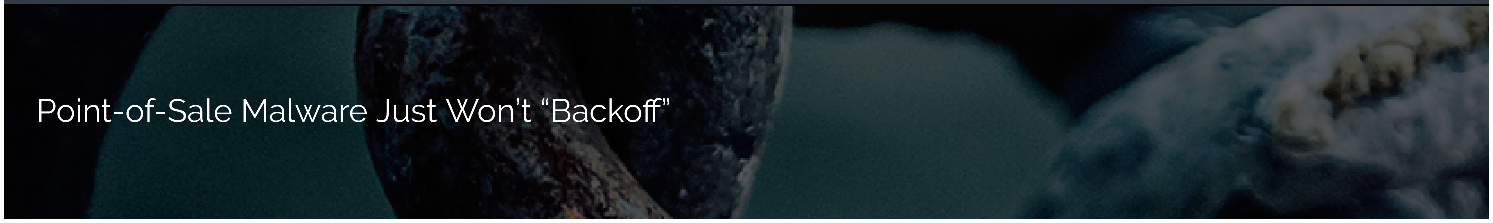

Point-of-Sale Malware Just Won’t “Backoff”

04
AUG

Point-of-Sale Malware Just Won't "Backoff"

August 4, 2014 / Ryan Nolette / Advanced Threat Protection, Community Perspectives, Detection and Response, Tech Toolbox

The latest POS (point-of-sale) malware to make the news is being referred to as "Backoff." "Backoff" is a family of retail malware that has been witnessed recently in multiple forensic investigations.

The malware typically consists of the following four core capabilities:

- RAM scraping
- Keylogger
- Command and Control
- Process injection

The US-CERT elaborates on these capabilities in a recent advisory: "The malicious stub that is injected into explorer.exe is responsible for persistence in the event the malicious executable crashes or is forcefully stopped. The malware is responsible for scraping memory from running processes on the victim machine and searching for track data. Keylogging functionality is also present in most recent variants of "Backoff." Additionally, the malware has a C2 component that is responsible for uploading discovered data, updating the malware, downloading/executing further malware, and uninstalling the malware."

This advisory is important because it confirms that although Backoff is the latest release in POS malware, it doesn't actually employ any new techniques or innovative infection methods.

Backoff is what is often referred to as a stage-two attack. In this context, this means that Backoff is leveraged after attackers force their way in through remote desktop applications.

Once the attackers have accessed the remote desktop, they begin recon for any POS devices and attempt to install Backoff or similar POS malware. Hearing about how easy it's been for attackers to accomplish this feat should push companies to reflect on what machines really need remote access. It should also indicate that they should be using two-factor authentication for those machines.

Now for the big question, "How do you stop Backoff?

Bit9 in high-enforcement mode will stop this type of attack.

- Yes, the RDP aspect of it will be successful because the attacker is exploiting a weak password or out-of-date application.
- Yes, the attacker will be able to drop files on the host.
- No, the attacker *will not be able to execute* these files and infect the machine.

Leveraging the integrated Bit9 + Carbon Black solution gives you the ability to track even more indicators. These include writing new binaries on specific systems, any unsigned process executing, a binary or process using specific DNS resolvers, a particular registry key being written, and much more.

You can detect all these different indicators or you can choose high enforcement and just stop the attackers from running anything new on your endpoints.

How do we know that high enforcement will stop this attack?

Analyses of samples of Backoff confirm the requirement for endpoint-based binaries to execute to administer the RAM scraping malware. This is also confirmed by US-CERT, as noted above.

Because this attack requires a file artifact for initial infection and then for persistence, having Bit9 installed and in high-enforcement mode would stop this attack. The malware dropped onto the system would simply not be allowed to run and the attack would fail. This means that even though the attackers can own every other application in the attack chain, *your POS system will still be safe and malware free because of Bit9*.

For more information, the US-CERT has created a post that contains file indicators that you can check to see if you are infected. We also suggest banning these hashes via Bit9 immediately and creating a Carbon Black watchlist for these indicators.

Stay safe and remember to ask, when are point-of-sale systems going to get the point of security?

Tags: Backoff Malware C2 Keylogger malware detection point-of-sale pos RAM Scraper Retail

More Posts

May 11, 2016 / *by Ryan Murphy*

May 11, 2016 – Morning Cyber Coffee Headlines – National Twilight Zone Day

Good morning! Sit with Carbon Black this morning over a cup of coffee (or tea) and browse a few industry headlines to get the