Data Theft in Aisle 9: A FireEye Look at Threats to Retailers

fireeye.com/blog/threat-research/2014/10/data-theft-in-aisle-9-a-fireeye-look-at-threats-to-retailers.html

While cybercriminals continue to target the payment card and banking information of individual users, they seem increasingly aware that compromising retailers is more lucrative. Targeting retailers is not new; Albert Gonzales infamously targeted retailers nearly a decade ago. What has changed, however, is the wide availability of tools and know-how that make it possible for even relatively unskilled cybercriminals to commit large-scale attacks. The results speak for themselves – significant breaches at retailers have increased over the last few years, and the trend continues. In fact, the Verizon Data Breach Investigations Report called 2014 the “year of the retailer breach” due to the number of large-scale attacks.

Not only are breaches at retailers occurring more regularly, FireEye researchers have noticed another startling new trend: while much of this activity is not *initially* targeted in nature, it can easily transition to a targeted attack when the attackers realize the value of the network they have compromised. The convergence of the wide availability of malware tools specifically built for point-of-sale (POS) systems and indiscriminate botnets, combined with targeted attack activity, suggest that network defenders struggle to determine the levels of threat severity and adversary sophistication. Simply put: What may initially seem like a “simple” crimeware infection may actually be a vector through which targeted actors can purchase or rent access to their victims.

POS Malware: A History Lesson

Since 2013 we have seen a dramatic increase in the number of malware threats specifically focused on POS systems. This uptick is like any other market dynamic — there's a lot of data residing in retailers' networks, and threat actors are adapting and evolving to take advantage of what's at stake. Robust underground markets and an enterprise-like cyber criminal ecosystem enable threat actors to develop and trade their wares. What follows is a summary of some of the most major POS malware families and their similarities:

> Backoff POS – The Backoff attacks were publicly disclosed in July 2014 but the campaign itself was active in October 2013. The attackers reportedly brute forced remote desktop servers and installed the Backoff malware. Backoff is capable of extracting payment card data by scraping memory, and exfiltrating data over HTTP. Backoff's Command-and-Control (C2) servers are connected to servers used to host Zeus, SpyEye and Citadel, suggesting Backoff may be connected to a broader series of attacks.
>
> BrutPOS – The BrutPOS malware was documented in July 2014. This botnet scans specified ranges of IP addresses for remote desktop servers and if a POS system is found, the attackers may deploy another variant that scans the memory of running processes to extract payment card information. BrutPOS exfiltrates data over FTP.
>
> Soraya – The Soraya POS malware was disclosed in June 2014. It iterates through running processes and accesses memory to extract payment card data. Soraya also has form-grabbing capabilities and exfiltrates data over HTTP.
>
> Nemanja – The details of the Nemanja were disclosed in May 2014 and the botnet is believed to have been active throughout 2013. The attackers compromised an array of POS machines worldwide running a variety of POS software. The attackers were reportedly directly engaged in the production of fake payment cards and money laundering using mobile POS solutions.
>
> JackPOS – The JackPOS malware was reported in February 2014 and was reportedly originally spread using "drive-by" download attacks. The malware, which appears to be somewhat related to the Alina malware, is capable of scraping memory to acquire payment card data and exfiltrate it over HTTP. JackPOS is now widely available on underground forums and is used by a variety of actors.
>
> Decebal – The Decebal POS malware was first reported in January 2014. The malware enumerates running processes and extracts payment card information, which is then exfiltrated over HTTP.

ChewBacca – The ChewBacca malware was first disclosed in December 2013. This malware enumerates running processes and accesses memory to extract information using two regular expressions that match payment card data formats. This malware uses the Tor anonymity network for data exfiltration.

BlackPOS – The BlackPOS malware, sold on underground forums by an individual believed to be "ree4," was first reported March 2013 and is now widely available. This malware, which has a variant also known as KAPTOXA, scrapes memory to obtain payment card data. This data is typically transferred to a local staging point and then exfiltrated using FTP. The malware is best known for its reported role in several highly publicized breaches.

Alina – The Alina POS malware, first disclosed in February 2013, is believed to have been developed by the same actor, known as "dice," who developed the Dexter POS malware. This malware has been reportedly distributed via Citadel botnets. The Alina POS malware iterates through running processes (except those on a blacklist) and dumps the memory, looking for payment card data before exfiltrating it over HTTP. While this malware initially was used by a select few, it was subsequently sold on underground forums.

vSkimmer – The vSkimmer malware was first disclosed in January 2013. It is available on a variety of underground forums and is used by multiple threat actors. The malware iterates through running processes and accesses memory to extract payment card information. The data is exfiltrated over HTTP.

Dexter – The Dexter POS malware was first disclosed in December 2012 and is believed to have been developed by an actor known as "dice," (who may also have been involved with the development of the Alina POS malware); the actual use of the tool has been connected to an individual known as "Rome0". The malware iterates through running processes, accesses memory looking for payment card data, and exfiltrates it over HTTP.

Most of these malware families use a similar approach of enumerating running processes and using pattern matching to extract payment card information from running processes. However, in at least one case, a BlackPOS variant was configured to only access a specific process. This not only makes it less noisy, but indicates that the attackers knew what process to target on the compromised system. This development, along with some hardcoded network paths and usernames, may indicate specific targeting by the attackers.

Indiscriminate vs. Targeted Attacks

While some malware appears to have been used exclusively by particular threat actors, some variants are now widely available. In many cases, it appears that the POS-specific malware was used as a “second stage” attack, while the initial vector remains unclear. In the case of Alina and BackOff, for example, the POS malware was connected to Citadel, Zeus and SpyEye botnets. While the details remain unclear, the attackers may be selling or trading access to particular targets.

In other cases, the attackers appear to be much more specific with their targeting. One particular threat group will engage in periods of reconnaissance for months before engaging with the target. We also observed this group using SQL injection as an attack vector, deploying POS-specific malware after moving laterally through the compromised network.

Conclusion

These developments challenge the traditional conceptions of risk when it comes to network defense. While targeted attacks (including those associated with APT activity) can be tracked and clustered over time (by understanding the tools, techniques and procedures used by the threat actors, as well as their timing, scope and targeting preferences), it is difficult to prioritize incidents that began indiscriminately and transitioned into targeted attack activity. Is a simple, indiscriminate Zeus infection a noteworthy incident? Or will it pass largely unnoticed … only to transform into a significant breach?

Acknowledgements

We would like to thank Kyle Wilhoit, Jen Weedon and Chris Nutt.