R-CISC
Q4 2016
TLP: WHITE

THE RETAIL CYBERSECURITY THREAT REPORT

PREAMBLE

Retail and consumer products/goods/services are an integral component of the US and global economy. From small businesses and individual entrepreneurs to the largest of brands, people rely on consumer facing businesses for nearly every aspect of their daily lives. This economic engine connects the supply chain of manufacturing and production into industries that contribute in excess of $2 trillion dollars annually to the estimated $18 trillion US GDP. In the age of digital commerce, retail is now where the money is for the cybercriminal.

Headlines continue to demonstrate that the threat of cybercrime in retail is significant, and the impact to the business victims is costly while the consumer gets caught in the crossfire. Security programs that aim to prevent successful cyber-attacks, detect intrusions, and respond rapidly to limit the extraction of sensitive information do not do so in isolation. The inter-connected ecosystem of retailers, suppliers, and manufacturers along with the financial processing system that links merchants to banks through processors all create a landscape that requires extensive visibility and insights that enable prioritization towards the most critical threats.

INTRODUCTION

As we described in our 2015 Holiday Threat Report (https://r-cisc.org/wp-content/uploads/2015/11/R-CISC-2015-Hacking-Season-.pdf) , there are several reasons why retailers need a heightened level of awareness during the time between October and January. Sales transactions and overall customer shopping activity see a large increase, particularly on traditional sale days such as “Black Friday” and “Cyber Monday.” This creates time windows in which retailers cannot afford to be slow-moving or offline; and for this reason, many retailers implement change freezes to keep production stable. For criminals taking advantage of the busy season, it’s a good time to hide amidst the traffic, and put time pressure on retailers for purposes of extortion or punishment.

This threat report describes current and trending activity in cybercrime affecting retail, whether the attacks are targeted or opportunistic. The information is drawn from R-CISC member submissions, analysis by associate members and partners, and open source intelligence. Some sources are not directly attributed, by their own request.

PHISHING

Because phishing is the most popular front-end delivery mechanism for attacks – business email scams, credential theft, ransomware, and the many other malware families – we expect the overall volume to increase. On the brand phishing side (targeting consumers), many themes will involve seasonal activities. Since more consumers are ordering online, phishing messages with "order confirmation," "shipment confirmation," and "attempted delivery notification" will come from criminals spoofing the largest retailers.

For phishing attacks directly against retailers, threat actors that are offering phishing-as-a-service (such as the R-CISC Intelligence Task Force suspected in its TA530 report) are expected to drive more business through the holiday season. TA530 appeared to be quiet for a short while, but now appears to be leveraged once again in more campaigns against R-CISC members. The downloaders H1N1 and Hancitor are still being seen in conjunction with retail-targeting campaigns, along with the Adwind Remote Access Tool. Symantec has warned about a reconnaisance trojan called Odinaff (https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks), believed to be related to the Carbanak threat actor group, and sharing some indicators in common with the Oracle MICROS support portal breach.

Attack vectors outside of email still include infected websites, as with the EITest campaign, which according to Palo Alto Networks (http://researchcenter.paloaltonetworks.com/2016/10/unit42-eitest-campaign-evolution-angler-ek-neutrino-rig/) has been using different exploit kits to drop a wide variety of malware families such as Gootkit, Nymaim, Ursnif and Vawtrak, and ransomware such as Cerber, CryptFile2 and Bart.

MITIGATION OPTIONS:

- Since many components of attack tools are being offered as a service or being leveraged with different types of malware, retailers should not assume that they are associated only with one kind of target, such as financial services. A downloader that was previously linked with a banking trojan may be dropping POS malware or ransomware in another campaign.

- If criminals can't find the email addresses, they can't use them. Some retailers have been able to reduce phishing volumes by changing the externally facing addresses of employees who are most heavily targeted.

- Drive-by infections from websites remain a major problem for all organizations, so they should continue to filter and restrict web use wherever possible.

- R-CISC members are exchanging detection and blocking rules and other controls within secure sharing groups; sharing indicators among the 80+ organizations can help ensure that everyone has the widest coverage possible for a given campaign.

POS MALWARE

Some of the visibly active POS malware families include FastPOS, which according to Trend Micro has been updated in preparation for the season (http://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-updates-in-time-for-retail-sale-season/).

Retailers using certain ecommerce platforms should be aware of the newest web injection attacks for stealing customer credentials and card data. RiskIQ describes MageCart (https://www.riskiq.com/blog/labs/magecart-keylogger-injection/), which injects Javascript code into vulnerable websites and has been spotted targeting the Magento, Powerfront CMS, and OpenCart platforms.

Fileless malware such as Kovter, which can be used to drop different things ranging from click fraud to ransomware, is currently being seen in campaigns against retailers. Other malware trends to look for include the use of legitimate web sites for command-and-control communication, to avoid DNS and IP blacklisting. Palo Alto Networks' Unit 42 team describes the technique of posting coded gibberish to forums on Yahoo and Quora (http://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/) to allow the malware to pick up its designated C2 addresses.

MITIGATION OPTIONS:

- Make sure support people are who they say they are. Retailers are seeing social engineering attempts by attackers who impersonate third-party staff in an effort to get remote access tools or malware installed. These spoofing attacks can focus on any part of the retail infrastructure, not just point-of-sale systems.
- Retailers using ecommerce platforms should make sure that they are updated to the very latest software release, particularly if they are any of the platforms listed above.
- Besides monitoring for C2 traffic to unknown and blacklisted IP addresses and domains, retailers may need to examine traffic to known websites where posting is unfiltered, as threat actors can use those as drop points for obfuscated C2 instructions.

ACCOUNT TAKEOVER

Account takeover (ATO) activity has remained a constant throughout the year, but may well increase during the holiday season. Stolen credentials from breaches as far back as 2012 have a long tail, and are still being sold in underground forums. The reported Yahoo breach of data from over 500 million user accounts (https://www.wired.com/2016/09/hack-brief-yahoo-looks-set-confirm-big-old-data-breach/) will doubtless play a part in account checking activity. Tools such as Sentry MBA remain in active use against retail accounts.

MITIGATION OPTIONS:

- Because there can be a delay of weeks or months between the sale of an account's credentials and the use of that account to commit fraud, retailers may need to review historical data from web and ecommerce activity and correlate it with later fraudulent transactions in order to pinpoint indicators of compromise.
- Where possible, retailers can search publicly available credential dumps for compromised email addresses belonging to employees and customers, and lock the corresponding accounts or reset their passwords.
- With the advent and resale of IoT botnets (see below), credential stuffers may try to fly under the monitoring radar by distributing their attempts among a wider set of sources. Retailers should look for login traffic from IoT devices such as cameras and DVRs.

EXTORTION AND HACKTIVISM (RANSOMWARE, DDOS)

Because of the short time frames within the holiday season, threat actors can put pressure on retailers by impacting availability in a number of ways. Ransomware targets data availability; network- or application-based denial of service (DoS) attacks impede the customer's access to online shopping as well as the retailer's ability to process high volumes of payment transactions.

RANSOMWARE

Some of the currently most active families of ransomware are Locky (seen in waves of several hundred phishing email messages per day), Cerber (which according to Intel 471 is being freshly updated as a service), Stampado (actively being sold according to Flashpoint), and a few others.

MITIGATION OPTIONS:

- Depending on the backup facilities available, organizations may choose to implement a policy not to back up desktops, only networked drives and server disks. In this case, employees are notified to keep work files on servers only, as endpoints will simply be wiped in case of infection. Needless to say, network storage and servers need regularly tested backup and recovery services in place according to the criticality of their data.

- Some security vendors now offer tools for decrypting files hit by certain ransomware families. However, retailers should obtain these only from well known and validated vendor websites.

- Because some types of ransomware now search for cloud-based files to encrypt, retail organizations should have backup and recovery strategies in place for those as well. Staff use of cloud storage should be officially tracked and managed rather than letting employees choose their own services for business-critical data.

DDOS

Headline-grabbing DDoS attacks affected the website of journalist Brian Krebs recently, to the tune of 620 Gbps (https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/), as well as France-based OVH, peaking at over one terabit per second (Tbps). The unprecedented scale of these attacks, which were not even using amplification, was made possible by impressing hundreds of thousands of vulnerable IoT devices such as CCTV cameras and home DVRs into a single botnet identified as Mirai.

Since then, the source code for Mirai has been released, leading to analysis by many security researchers and the open question of how it will be used in the future. In a briefing, Flashpoint's Director of Security Research, Allison Nixon, stated that it is more likely that the record-setting original botnet will be diluted by numerous other parties trying to use the software themselves. From the R-CISC's perspective, a single "DDoS cannon" could only target one victim at a time, so pointing it at a number of retailers would be harder to envision; on the other hand, breaking up such a botnet could allow wider targets, but with a smaller impact.

MITIGATION OPTIONS:

- Regardless of how the IoT botnet trend plays out, retailers should be checking with their DDoS protection providers to make sure the service is still properly configured.

- A retailer that experiences a short-lived DDoS attack may expect a longer one in the future, as some DDoS providers offer a "test attack" to the prospective buyer to demonstrate the quality of their service.

- If an extortion message threatens a DDoS attack unless money is paid, retailers can provide the details to the R-CISC and receive help in determining whether the threat is legitimate.

- Retailers should consider maintaining redundancy in key services such as Domain Name Services (DNS), Internet access, eCommerce website, and email where possible to ensure that these functions can be accessed even if experiencing a DDoS attack.

SUMMARY

Some of the threats change tactics over time, and some stay the same. Although the spectre of massive DDoS attacks may grab headlines, the most common threats will stay under the radar by design, and criminals will shift their methods to whatever channels appear most vulnerable, such as retail support staff who are distracted by the busy season. As always, the key to being able to respond quickly is to exchange intelligence with peers at the appropriate levels for each organization.

It is also likely that the threats highlighted in this report will be used concurrently or simultaneously against retailers. Phishing attacks are used to deliver PoS Malware or ransomware. DDoS attacks may be used to distract retailer cybersecurity teams while other attacks aimed at gaining access or exfiltrating data are launched. Retailers should be prepared for these blended attacks in addition to each individually.

This report was designed to be released publicly, so it does not contain classified details about these threats. For more information, and to share data with a wide variety of retail and commercial services organizations in a trusted environment, please contact the R-CISC at info@r-cisc.org.

TLP: WHITE information may be distributed without restriction, subject to copyright controls.

R-CISC
RETAIL CYBER INTELLIGENCE SHARING CENTER

The R-CISC has provided the information contained within this report and the associated mitigation options as is, and provides no warranty, express or implied that the information is without fault or completeness in terms of the risks that are identified.