POS FRAUD TRENDS AND COUNTER-ACTIONS TO MASS FRAUD

Ken Dunham
iSIGHT Partners, USA

Email kdunham@isightpartners.com

ABSTRACT

Point-of-Sale (POS) e-crime fraud was of little discussion until the fall of 2013. Since then, a large number of retail stores in the US have announced major breaches. The number of infected organizations is in the thousands, with credit card breaches reaching new heights. Some fraudsters are able to capture the PIN values associated with debit cards. In some incidents, POS fraud had taken place on networks for months before the companies realized they had a security breach. In multiple cases it took weeks to properly identify and remove sophisticated POS malware from compromised networks.

POS fraud didn't start in 2013 but many years earlier. Just as was seen in former emergent crimeware markets, including botnets and rootkits, POS fraud is now reaching an apex of emergence for maximum profits. A new industry group has been formed to help battle POS fraud, but will it help? Major credit card companies in the US have stated that they will be moving to Chip-and-PIN technology, but will it stop fraud? How have fraudsters already adjusted to the counter-e-crime efforts seen globally, and how does that paint a picture of what will happen in the next five years for POS fraud?

E-CRIME FOLLOWS AVAILABILITY OF ASSETS

In the 20th century, global transactions took place in a very different way from how they take place in 2015. Today, consumers are increasingly reliant upon the use of credit, debit and pre-paid cards, creating a massive global opportunity for e-crime actors. Today, e-crime actors are able to compromise and rapidly monetize non-cash transactions.

Capgemini-RBS [1] has revealed in its *World Payments Report* that, in 2014, more than 334 billion non-cash transactions took place. Of such transactions, more than 60 per cent were by card. The *Nilson Report* [2] for market shares in 2014 reveals about a 50 per cent increase in use of both credit and debit cards and a 200 per cent increase in pre-paid cards from 2009 to 2014. Globally, *Visa* managed more than 112 billion purchase transactions in 2014, with *MasterCard* coming in at 51 billion and *UnionPay* at close to 20 billion. *UnionPay* (China) grew more than 52 per cent in 2014, with the next nearest growth rate being that of *JCB* (Japan) at almost 22 per cent, followed by *MasterCard* at 13.6 per cent and *Visa* at 10.1 per cent, according to the *Nilson Report*. This anecdotal look at global transactions reveals growth in non-cash transactions, with very rapid growth in the Asian market in particular in the past year.

Consumers are rapidly adopting debit payment systems and pre-paid cards in favour of credit payments, according to *NerdWallet* [3]. Internationally, debit cards grew nearly 30 per cent from 2007 to 2011. This, along with the aforementioned global changes in payment methods, reveals a diverse change in how people are performing transactions in 2015 and going forth. Pre-paid cards are increasingly being used in retail, health care, food services, education and the travel industry.

DOES SIZE MATTER IN POS RISK MANAGEMENT?

The size of an organization *does* impact how POS risk management is performed, as businesses of different sizes commonly have different needs and risks. Small and large organizations each have their advantages and disadvantages when it comes to POS risk management. Anecdotally, smaller organizations typically have simpler solutions and capabilities and fewer resources, while larger organizations tend to have the opposite.

Merchants are eager to enable non-cash/card-type payments as a matter of convenience for customers who are increasingly demanding such methods over traditional forms of payment. Merchant adoption of POS solutions is now much more diverse than it was just a decade ago. Many merchants are opting to rely upon third-party solutions such as value-added resellers or contractors. This has resulted in both dependence and deferred responsibility for much of the risk management associated with POS terminal services, especially amongst small businesses. This can lead to complacence by any organization, large or small.

Smaller organizations are often understaffed with few resources to dedicate to properly securing POS payment systems. In most cases, the reality is that 'It Works!' is all that is required for daily business operations, alongside meeting basic regulatory compliance directly or by farming out POS risk management out to a third party. Generally speaking, many small organizations struggle to address POS risk management properly, making it a juggling act to cost effectively manage operational needs alongside any security needs that go beyond basic regularly compliance.

Larger organizations – which commonly have significantly more resources, larger budgets and better capabilities to manage POS risk – are more likely to struggle with disparate groups, communication and more complex interdependent systems with massive amounts of information. It is common for an IT group and a security group to exist within the same organization but not necessarily have a tight bridge of operational communication between them. While process and procedure exist, most large organizations typically suffer from information overload with so much data flowing in that gaps emerge from the busy work of risk management. For example, some organizations may simply filter logs and events based on anti-virus signatures, ensure that patches are rolled and move on, when in fact more serious threats may exist below the surface if properly handled during research and response.

VECTOR OF ATTACK

POS fraud operations start with a vector of attack. This may be opportunistic, such as a computer that gets compromised through a mass spamming, or more targeted such as an insider looking to cash in at the expense of their company. Vectors commonly involve the following:

- **Insiders:** Embittered, financially struggling and untrusted insiders know where to strike the network and have the greatest access compared with other actors.

- **Contractors:** Infected laptops or VPN connections or compromised credentials used to access client networks are a notable vector of intrusion. POS contractors normally have administrative rights to access all POS-related software and solutions, enabling e-crime actors to rapidly leverage such credentials for cashing in on a compromised POS network.
- **Phishing and exploitation:** Emails sent to users within an organization can lead to the compromise of a host and/or network. Social engineering is often used in this vector of attack. Exploits may also be used via email attachments, links to a remote hostile website, etc.
- **Weak security:** Weak security, such as universal and easily guessed passwords, continues to be practised on a multitude of systems globally. Traditionally, this falls into the category of weak, stolen or misused credentials – an attacker's choice 80 per cent of the time according to the 2013 *Verizon DBIR* [4]. Brute-force attacks against remote desktop applications are associated with the very large-scale Backoff POS campaign reported in 2014. Several tools and tactics exist to brute force such logins. With an increase in reconnaissance and targeted attacks, e-crime actors can identify systems of interest and spend day and night attempting to subvert such systems. Hardening against such attacks can be very difficult. For example, the default logging system may only log bad logins after five failed attempts – this can be exploited by criminals who only perform four attempted logins in a session before terminating and attempting another login. Such tactics can be automated and/or deployed through multiple IPs via proxies for maximum effectiveness.
- **Lateral movement:** Once inside a network, e-crime actors are increasingly able to identify host and network security controls and topology and then move laterally through the network. This enables them to pivot off critical systems within network(s) to perform reconnaissance, maintain persistence, as well as perform exploitation and exfiltration of stolen data even on POS terminals that are not directly Internet-facing. Once a remote actor is inside a network they can essentially act like a malicious insider, performing keylogging, grabbing hashes and attempting to brute force access remotely, and gaining access to admin and domain controller accounts for full access and control within a network.

At the turn of the century, penetration testing and auditing was scant at best on most networks. Today, it is part of common business operations to audit for possible operational and security issues that may exist on a network while one hardens against attack. A wealth of tools and tactics are well developed in the open-source market today, which can be both used and abused as desired. Maturation of such tools and technologies, in conjunction with the rapid adoption of global non-cash transactions, has resulted in e-crime actors aggressively implementing such strategies into attacks and exploitation. Specifically, once an e-crime actor has access to a network they are now looking for POS terminal possibilities, quietly and carefully constructing a more extensive e-crime attack over a period of days, weeks or even months dependent upon the compromised network and organization.

Attacks by e-crime actors today are not necessarily highly sophisticated in terms of technology, but they are increasingly sophisticated regarding *how* they go about penetrating and exploiting a network once 'pwnage' has taken place. This is an important change in how attacks are taking place in general, representing in part more mature adversary skills and capabilities sets for maximum profit.

SUBVERTED SYSTEMS

Counterintelligence plays a part in e-crime operations in 2015. Criminals often know more about our networks than we do. In some cases, they painstakingly identify anti-virus and security solutions on all levels – the host, gateway, etc. Attacks are then customized based on identified risk for e-crime operations, such as ensuring codes are not detected by the anti-virus solution running on a compromised network. In the case of netflow operations, e-crime actors develop their own strategies for transferring data in such a way as to fly under the radar of IDS/IPS-type controls. If POS terminals are segregated from the Internet they must perform payment processing in real time through a Local Area Network (LAN). E-crime actors simply traverse the network from an Internet-facing computer within the compromised network and then tunnel into the LAN of interest – or leverage insider access as needed to gain access to POS terminals. E-crime actors are also smart enough to understand POS systems in great detail – in some cases exploiting specific processes running in memory to capture credit card details before they are encrypted within a payment processing system. Tools used for memory scanning and credit card capture do not have to be very complex; gaining access to a non-Internet based system, tunnelling through a compromised network, and then stealing data and performing exfiltration to scale is increasingly sophisticated and impressive when it comes to larger retail chains suffering POS fraud.

POS TERMINALS – MOSTLY WINDOWS

The majority of POS systems now run some version of *Microsoft Windows*, the most commonly attacked operating system to date. This also means that e-crime actors have great opportunity as experienced programmers have existed for this operating system for many years in the traditional e-crime marketplace.

Most POS malware attacks occur on the POS terminal itself, where sensitive credit data is read before being encrypted. This makes it easier for sensitive data to be stolen before it is encrypted, which can greatly increase the speed of monetization for e-crime fraud operations. POS malware may be used anywhere along the chain of the payment process behind the scenes of a retail store, including but not limited to backend databases and payment processing, inventory and customer relationship management (CRM) solutions.

EXPLOSION OF POS FRAUD INCIDENTS

Significant POS malware and e-crime operations emerged in 2013 with an explosion of discovery and disclosure in 2014. Notable victims include but are not limited to: *Target*, *Home Depot*, *Neiman Marcus*, *Kmart*, *UPS*, *Staples*, *Subway*, *Supervalu*, *Goodwill*, *C&K Systems*, *White Lodging* and *Blanchard's Liquors*. In the Backoff case, the FBI publicly stated that more than 1,000 businesses were infected with the

code. Such operations are very large scale, revealing automation and scale akin to the explosion of botnets in 2003 and 2004 following former one-off attacks with trojans in the latter part of the 20th century. In 2015, additional breaches have been revealed, such as that of *Sally Beauty*, as proof of this troubling trend.

A mature marketplace for e-crime POS fraud operations also exists. Recently, a copy of the LusyPOS RAM-scraping malware was offered for sale on the underground for an estimated US$2,000. There is a movement in the underground towards malware as a service, mobile management and solutions similar to those seen in the white hat world.

The explosion of discovery and disclosure in 2013 and 2014 is similar to that seen in rootkits early this century. As e-crime attacks follow assets, notable changes in the marketplace take place which result in new tools and tactics, such as the introduction of stealth and rootkits over a decade ago. In this case, organizations may have heard about such risks in the news but they didn't have the necessary tools, tactics and procedures for identifying and removing them from their own networks. As a result, the industry was caught in a reactive posture, with a flurry of activity taking place once everyone realized what rootkits looked like and how they were being spread. This naturally led to the discovery of rootkits that had happily been maintaining persistence within a large number of networks for months.

POS systems had never before suffered such attacks and breaches as has been seen in 2013, 2014 and beyond. This has resulted in a flurry of activity in the payment processing and associated merchant markets to identify and mitigate these threats. It has also resulted in law enforcement becoming educated in this area and identifying victims in investigations in order to inform them of possible breaches and losses of which they may not previously have been aware. When the first breaches appeared in the news it was really big news; today, another large breach is just noise in the background of all-too-common breach notifications to the public. Meanwhile, a massive tidal wave of POS malware and e-crime attacks continues to slam down on merchant networks globally.

DIVERSITY AND DEPTH OF POS MALWARE

POS malware, such as BlackPOS, Dexter and Alina, serves as an indicator of an e-crime operation's maturity. One of the earliest POS malware families to publicly be reported (in 2011) was Rdasrv, named after the executable in the attack [5], which targeted hospitality and educational institutions. More importantly, mmon (presumably for the name 'memory monitor') was an early underground source code that was later used in BlackPOS and other families of code. It still appears in recent threat reports, such as one by *Visa* [6]. It contains a command line option to scan a specific process ID or can be used to scan all processes in memory for possible credit card data. Mmon.pdb is a debugger string and file reference that can be seen in codes leveraging this early POS malware derivative.

BlackPOS is fairly well known and is associated with other POS malware families such as BrutPOS. BlackPOS was sold on the underground in the spring of 2012 with exploitation seen in the wild by that summer. A number of minor variants exist within the BlackPOS malware family because of how the code was packaged and sold on the underground market. In September 2012, news broke of two Romanians having admitted to POS retail fraud targeting *Subway*, in which more than US$10M was stolen. According to public reports, the attackers brute-forced passwords to gain access to system(s), which they followed up with lateral movement strategies involving keystroke loggers (including POS/card data) and network sniffers. By the end of 2012, Dexter had emerged in the wild.

In 2013, POSRAM emerged as part of the KAPTOXA campaign. In the same year, VSkimmer, ChewBacca and the infamous Alina POS malware families also emerged in the wild. A convergence of marketplace readiness, following transaction assets and maturation of criminal skills and capabilities led to rapid exploitation of mmon and similar source codes to subvert POS payment systems.

By 2014, identification and disclosure of POS malware had erupted in the public eye. JackPOS, Decebal, Soray, BrutPOS and new variants of BlackPOS have all been reported by various public sources. While no international naming convention exists for malware, it is clear from public reports that a massive development in diversity and successful exploitation took place between late 2013 and 2014.

Early codes, such as mmon, were sometimes used with crude scripts such as a batch file to run in a loop, scanning all processes all the time for possible credit card data. Later variants became more refined or were deployed in a more precise manner, scanning only specific processes for possible credit card data. Some intrusions even involved actors performing reconnaissance, following initial intrusion, to then identify a payment system process in memory, followed by a custom memory-scraping code designed for that particular process and data structure.

Maturation of POS malware has also taken place in terms of the architecture of an attack. Instead of single codes, like backdoor trojans of the late 1990s, POS malware is part of an attack set that may involve backdoor trojans, compression and transfer utilities, memory scrapers and so on. Naturally, these have matured over time, as can be seen in public reports regarding the KAPTOXA campaign in 2013 and 2014. Bad actors sometimes make mistakes in programs or need to learn what works for moving laterally through a network and/or performing exfiltration of stolen data. Updates to such codes naturally take place over time, with improvements seen as attacks maintain persistence and/or campaigns mature with new victims. Naturally, this also involves improvements in obfuscation and/or encryption, especially regarding secure communications for both intrusion and exfiltration of data from a POS payment system network.

PoSeidon is a newer POS malware family that has a unique capability amongst POS malware to date: the ability to self-update and execute new code. In the trojan and bot world, this is a common concept used to avoid detection, where new private builds are often uploaded after a more public build has been uploaded during the initial infection. This helps avoid detection and removal of the malware even if the more public build is identified and removed, thus increasing persistence for the malware in most cases. The ability to run updates and new code, from every component of a PoSeidon-related code, enables PoSeidon to install other codes as needed or desired, such as for lateral movement, counterintelligence actions, exfiltration or even to install

complete new malware families not associated with such campaigns to date. In short, it's much more powerful based upon whatever nodes an actor may have access to within a compromised network. Bad actors are clearly working actively to maintain a moving target that cannot easily be identified or removed from POS payment systems. In the case of PoSeidon they are even beginning to clean up stolen data, for example by using the Luhn formula to verify card validity upon capture.

More recent developments include multiple new families of POS malware and a movement towards automation (specifically, combining bot-type malware such as Andromeda with NitlovePOS, as reported in 2015). Another such example is that of the Neutrino Exploit kit used to spread Neverquest, which has been upgraded to include POS-scraping capabilities [7]. Automation of such operations introduces massive new challenges for the world of POS risk management, just as was seen with the evolution of backdoor trojans to bots close to the turn of the century. This is now coupled with rapid monetization, including infrastructure and operational capabilities to subvert two-factor authentication (2FA) via mobile devices, capturing one-time-pin (OTP) values from victims, and so on.

STEALTH MATTERS IN POS FRAUD

Stealth in POS e-crime operations is more about network intrusion and survivability than it is about the POS malware or keylogging components used in such an attack. In a common e-crime case, malware is installed on a host as an endpoint. It is relatively easy to identify and mitigate modularly. In POS e-crime cases, a suite of utilitarian programs may be used, including legitimate programs commonly used by security professionals. Each component may not indicate a POS malware attack but instead look like a common downloader trojan or legitimate security tool on a computer with unknown means or motive. This helps the intrusion to remain undetected in stark contrast with that of, say, a host-based ransomware code that infects a node and/or encrypts files across the network in a very observable fashion.

POS fraud operations are also made stealthy by leveraging pen-testing tactics to stay below the radar. In many cases attackers know the network well and know exactly how to move around in and through a network including for exfiltration of data. In some cases, intentional systematic development of such tactics exists within a campaign over time. Even if mistakes are made on some networks, attackers learn from those mistakes, make improvements to the code and reap profits in each attack regardless. POS terminals may be configured within some networks as a separate segment with no Internet capabilities (LAN only). This may impact how and when audits and management of such systems take place and/or the security postures adopted compared with those of higher risk machines within a network such as an executive's laptop or common users' desktops.

WHAT IS THE FUTURE OF POS MALWARE?

Original POS malware fraud was simple in most cases, starting with opportunistic scanning of all processes looking for possible credit card data. However, memory monitoring and scraping is becoming more refined and efficient, even targeted in some cases, so that only specific processes and/or strings are collected as part of such operations. Track 1 and Track 2 data are common targets of credit card fraud, but PINs open up the options for monetization, making them an obvious target for more advanced POS fraud operations going forth.

Installation and updates of POS malware will also become increasingly refined and specific. For example, Punkey [8] installs either a 32-bit or 64-bit version of itself on POS terminals and can download and update other files as needed for fraud operations. Another example of innovation and development is seen in the LogPOS [9] malware, which does not write stolen data to disk but instead uses a mailslot for rapid exfiltration of data.

All forms of netflow, including data transfer of files, programs and stolen data, are moving towards obfuscation and encryption. This helps all such operations stay under the radar and hinders investigative efforts. This can, in some cases, buy more time for fraudsters seeking to rapidly monetize stolen credit card data prior to law enforcement or security operations identifying such stolen or exfiltrated data. Respondents' use of whack-a-mole counter actions are clearly utilized by e-crime actors who now use sophisticated schemes for C&C communications that are constantly changing and on the move. This is combined with innocuous-looking HTTP traffic and data that is not easy to spot amongst a massive amount of Internet flow on a daily basis in and out of a network.

POS fraud operations will continue to escalate globally due to financial incentives indicative of various geopolitical regions. For example, in Brazil a single individual was able to steal more than 22,000 unique credit cards in over a month using vnLoader and FighterPOS [10]. These types of financial incentives are massive, encouraging fraud operations in countries where jobs are hard to come by and pay is low, and where law enforcement against global fraudsters is unlikely. In this anecdotal example, FighterPOS is a tool that can be purchased [11] for 18 bitcoins, or about US$5,250 – an amount that can easily be recouped within the first hour of a successful POS network compromise.

To make matters worse, a convergence of e-crime and espionage means and motives is currently taking place globally. No longer do we have one-off e-crime attacks, but more sophisticated, systematic, long-term campaigns that involve everything from opportunistic to highly targeted attacks for maximum profits. A highly skilled marketplace of fraudsters now exists for performing very sophisticated intrusions into networks. Criminals are more than happy to spend weeks or months subverting a system when the payout can be huge, like that of multiple POS breaches identified in the past 18 months.

WILL CHIP AND PIN (EMV) AND NEW INDUSTRY COLLABORATION EFFORTS MAKE A DIFFERENCE?

Chip and PIN, or EMV, is a different technology solution to make it harder for fraudsters to monetize stolen credit card data. It was originally developed by three companies after which the 'EMV' standard was named: *Europay*, *MasterCard* and *Visa*. Because much of Europe and related time zones already use such technology in their credit cards, the Americas are the low-hanging fruit, as they are the easiest to monetize overall.

Introduction of Chip-and-PIN technology in the US will drive up merchant and POS risk management operations but will not stop POS fraud. Rather, it will simply change the game, bringing the Americas up to the global playing field of counter-actions for credit card fraud. In short, it will change the global risk posture and assumed liabilities related to ongoing e-crime credit card fraud.

As adoption of EMV in the Americas takes place, changes in how stolen credit card data is monetized will follow [12]. Take note that EMV adoption in the Americas will likely start with signature authentication only instead of PIN, due to merchant expense in retooling for the newer cards; this will delay the hardening of such solutions, maintaining a low-hanging fruit status globally until full adoption is completed. Additionally, it will take a very long time for adoption to be complete, as was seen in Canada which started in 2003, only reaching 85 per cent adoption ten years later [13]. Further, EMV standards in Europe and the surrounding area have not stopped credit card fraud.

Consumers in the Americas will be wondering if EMV will make things more secure, but we are highly likely to see ongoing fraud and identity theft cases emerge despite adoption of EMV. Nevertheless, due to how liability for such e-crime fraud is assumed in the Americas (little to none for the consumer), this is not likely to erode confidence in or use of EMV solutions compared with other forms of payment such as cash.

Changes in security products will also take place to counter known and expected e-crime fraud operations. Specifically, the battle against memory management, encryption and scraping is well under way. Expect obfuscation and encryption strategies to move into memory management of sensitive data as part of payment processing risk management.

The increased sophistication of e-crime attacks greatly hinders threat identification and mitigation. Multiple compromised POS environments when informed of a possible breach by federal authorities were unable to identify fraud within their own networks for weeks if not months. Meanwhile, exploitation and exfiltration of sensitive POS systems continues concurrent to the lengthy incident response cycle seen in such incidents. E-crime fraudsters are able to create innovative new codes and use encryption and similar solutions to their maximum advantage to make it next to impossible for organizations to identify what is being stolen, how it is being done and what might have been breached or compromised. In multi-layered defence plans, e-crime actors are able to subvert on *every level*, greatly increasing the need for highly skilled security technicians alongside mature policies and plans for dealing with such events, which largely don't exist today in most merchant networks. The industry needs to move from panic and awareness mode into operational risk management to manage ongoing POS e-crime fraud operations.

REFERENCES

[1] 10 Years of Trends and Predictions. Capgemini. https://www.worldpaymentsreport.com/10-Years-of-Trends-and-Predictions.

[2] Nilson Repot. http://www.nilsonreport.com/publication_chart_and_graphs_archive.php?1=1&year=2015.

[3] Chen, T. Credit Card and Debit Card Transaction Volume Statistics. NerdWallet. https://www.nerdwallet.com/blog/credit-card-data/credit-card-transaction-volume-statistics/.

[4] 2015 Data Breach Investigations Report (DBIR). Verizon. http://www.verizonenterprise.com/DBIR/.

[5] Wisniewski, C. Targeted attacks steal credit cards from hospitality and educational institutions. Naked Security. https://nakedsecurity.sophos.com/2011/11/30/targeted-attacks-steal-credit-cards-from-hospitality-and-educational-institutions/.

[6] Visa data security alert. Retail Merchants Targeted by Memory-Parsing Malware – UPDATE. http://usa.visa.com/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf.

[7] Fisher, D. Neverquest Trojan Adds New Targets, Capabilities. Threatpost. https://threatpost.com/neverquest-Trojan-adds-new-targets-capabilities/108076.

[8] Constantin, L. New malware program Punkey targets point-of-sale system. PCWorld. http://www.pcworld.com/article/2910912/new-malware-program-punkey-targets-pointofsale-systems.html.

[9] LogPOS – New Point of Sale Malware Using Mailslots. Morphick. http://morphick.com/blog/2015/2/27/mailslot-pos.

[10] One-Man PoS Malware Operation Captures 22,000 Credit Card Details in Brazil. TrendLabs Security Intelligence Blog. http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-fighting-a-new-pos-malware-family/.

[11] Walker, D. FighterPOS malware strikes over 100 terminals in Brazil, captures info for 22K cards. SC Magazine. http://www.scmagazine.com/recent-pos-malware-attacks-in-brazil-may-be-work-of-sole-perpetrator/article/408795/.

[12] Mecia, T. Online fraud may surge after EMV chip card rollout. CreditCards.com. http://www.creditcards.com/credit-card-news/online-fraud-surge-emv-1273.php.

[13] Guy Birken, E. Will New Chip-and-PIN Credit Cards Stop Identity Theft? Wise Bread. http://www.wisebread.com/will-new-chip-and-pin-credit-cards-stop-identity-theft.