FBI Cyber Division

Private Industry Notification

DATE: 17 January 2014

PIN #: 140117 – 001

(U) Recent Cyber Intrusion Events Directed Toward Retail Firms

(U) Executive Summary

(U) Law enforcement officials and private security researchers have identified a rise in intrusions into point-of-sale (POS) systems. These attacks are perpetrated with the intent to obtain credit and debit card data as well as personally identifiable information. The Department of Homeland Security (DHS), in conjunction with iSIGHT Partners and the Secret Service, has released a TLP-Green report outlining the details surrounding the recent incidents affecting major US retailers. The United States Secret Service has the lead on those investigations. This report will outline high-level analytics involving POS-related malware to include incidents investigated by the FBI within the last year.

(U) Malware Targeting Point of Sale Systems

(U) There are several variations of malware that have been designed to exploit POS systems. This family of malware has also been identified by the names "Ram scraping" or "Memory Parsing." While POS malware varies in type, it is primarily designed to locate and extract specific financial transaction data. In a typical POS intrusion, there are two tracks of data targeted for exfiltration. Track 1 contains cardholder data (including names and account numbers) and Track 2 contains card data (including credit card numbers and expiration dates). This data is extracted from volatile memory by the malware and exfiltrated back to the individual committing the intrusion. Each time a customer's card is swiped at a POS terminal, Track 1 and Track 2 data is retrieved from the magnetic stripe and transferred electronically to the company's payment processing provider. It is during this process that the data is extracted from the system's RAM by the malware installed on the machine. This technique is designed to circumvent any encryption utilized during the electronic transfer of data to the payment processing provider, as the data remains in plaintext while in memory on the POS terminal. It is important to note, however, that POS malware is rarely designed to be an all inclusive and automated malware package. Malicious actors are usually required to conduct reconnaissance to ascertain where the POS systems reside within a corporate architecture and then design several pieces of malware to conduct further reconnaissance to locate the appropriate systems, extract the information, and then surreptitiously exfiltrate it back to the actor. The networks that need to be accessed by the actor are typically not flat and may require bypassing several networks with various levels of administrative access. Point-of-Sale systems are connected via a LAN, but are not internet addressable. POS malware samples are typically stand alone tools that are dropped by other types of malware. Many of the POS systems that large retailers deploy utilize lightweight, embedded operating systems distributed via a centralized server. The actors

may have to compromise one or many of these servers in the hierarchy in order to deploy the POS malware to the terminals.

(U) Current FBI Investigations Relating to POS Malware

(U) The FBI has discovered approximately twenty incidents related to POS malware within the last year. The malware identified in open source (known as KAPTOXA) in the recent intrusions, has previously been seen by the FBI and has appeared in reporting since at least 2011. Due to customization of the KAPTOXA malware, the most recent variant analyzed by the FBI did not match by MD5; however, the underlying codebase utilized in the recent attacks is within the same malware family. Additional POS malware identified in the most recent FBI cases include Cardstealer, Dexter, and vSkimmer.

(U) The Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) has determined the following POS malware as of particular interest:

- (U) **BlackPOS** infects computers running Windows that are part of POS systems and have card readers attached to them. Once installed on a POS system, the malware identifies the running process associated with the credit card reader and steals payment card Track 1 and Track 2 data from its memory. BlackPOS does not have an offline data extraction method; rather, the captured information is uploaded to a remote server via FTP.

- (U) **Dexter** is a Windows-based malware with several variants. Security researchers noted that in one instance of infection, the low number of victim machines suggested the actors may have been testing the software between mid-October and mid-November 2013.

- (U) **Trojan.POSRAM** monitors information in payment application programs. When the malware determines unencrypted track data is in RAM, the information is stolen.

- (U) **VSkimmer**, which may be a successor to Dexter, also targets Windows machines. Researchers have determined that if a VSkimmer-infected machine is not connected to the internet, the program will wait until a USB drive with the volume name KARTOXA007 is inserted into the computer, and download stolen information to the USB drive.

(U) In addition to the above, malware known as “Alina” malware illustrates the evolving nature of POS malware in that the author(s) introduced an option to update the malware remotely. This highlights the persistent nature of the malware in commercial or retail settings.

(U) Initial Infection Vectors

(U) The POS malware is typically introduced into a system after the system has already been compromised. In other words, the POS malware serves as the payload as a result of the initial intrusion. The attack can take various forms, such as phishing e-mails, compromised Web sites, and other common infection vectors.

(U) Analytical Findings

(U) At least one version of POS malware has been observed for sale for up to $6,000 in a well-known criminal forum. Of the current ongoing FBI cases of POS related malware intrusions, most were primarily infections of small-to-medium sized local or regional businesses. The estimated losses to affected

companies related to these intrusions range from in the tens of thousands to millions of dollars. Open source information reported from CTO Daniel Ingevaldson of Easy Solutions cited a recent massive flow of stolen credit card data in December, as well as a second round of stolen credit card numbers discovered on Jan 4th. The second group of cards contained an inordinate amount of premier, high-limit credit accounts. The dollar value of these types of intrusions can have a significant impact on both individuals and corporations. Variations of cyber POS attacks can be exceedingly sophisticated. The high dollar value gained from some of these compromises can encourage intruders to develop high sophistication methodologies, as well as incorporate mechanisms for the actors to remain undetected.

(U) As the NCCIC report suggests, the growing popularity of this type of malware, the accessibility of the malware on underground forums, the affordability of the software and the huge potential profits to be made from retail POS systems in the United States make this type of financially-motivated cyber crime attractive to a wide range of actors. We believe POS malware crime will continue to grow over the near term despite law enforcement and security firms' actions to mitigate it.

(U) Administrative Notes

No portion of this report should be released to the media, the general public, or over non-secure Internet servers. Release of this material could adversely affect or jeopardize investigative activities.