OFFICE OF PRIVATE SECTOR

DIRECTOR'S OFFICE

Liaison Information Report (LIR)

19 May 2016

(U) ATM Skimmers Target Standalone ATMs with Wiretap Devices

(U) Handling Notice: Recipients are reminded that DSAC LIRs contain sensitive information meant for use primarily within the corporate security community. Such messages shall not be released in either written or oral form to the media, the general public, or other personnel who do not have a valid need-to-know without prior approval from an authorized DSAC official.

(U) DSAC disseminates LIRs to convey timely, actionable information that has undergone some vetting but is not a completely refined product. The FBI and DHS prepare DSAC LIRs, which are intended for Chief Security Officers, Chief Information Security Officers, and their staff. This LIR was prepared by the Office of Private Sector in coordination with and based on information from the FBI's Criminal Investigative Division.

(U) The purpose of this DSAC LIR is to raise awareness. Recipients should immediately report any suspicious or criminal activities potentially related to these events to local law enforcement, their FBI Field Office or Fusion Center.

(U) Executive Summary

(U//FOUO) The purpose of this LIR is to inform DSAC and other relevant private sector partners about new methods ATM skimming[i] crews use to target standalone or kiosk-style ATM terminals such as those found at casinos, hotels, airports, shopping malls, gas stations, restaurants, and supermarkets. The skimming crews intercept customers' account data through the ATMs' external cables. The activity observed to date in the United States was discovered at convenience store locations in California, Delaware, and Pennsylvania. This LIR provides details on the methods used in these skimming attempts as well as previously reported use of internal wiretap skimming devices.

(U//FOUO) Internal and external wiretapping (or eavesdropping) skimmers allow criminals to capture card data while circumventing the most common anti-skimming measures, which generally focus on securing the ATM's card reader "mouth." Additionally, while many consumers have learned to look for devices attached to ATM card readers, they may not think to look at Ethernet or other cables in plain view and, if so, may not recognize they are out of place. The internal wiretapping method, if properly concealed or achieved through the non-destructive "top box" method, allows for further obfuscation of tampering (i.e., no plain-view wiring), while the external method likely permits easier device installation and retrieval.

[i] (U) For the purpose of this report, the FBI defines ATM skimming as the modification of ATM terminals to capture card data for further criminal exploitation. Skimming entails the use of either concealed card reading or data capture devices or malware, coupled with a pinhole camera or keypad overlay to record the victims' PIN entries.

OFFICE OF PRIVATE SECTOR

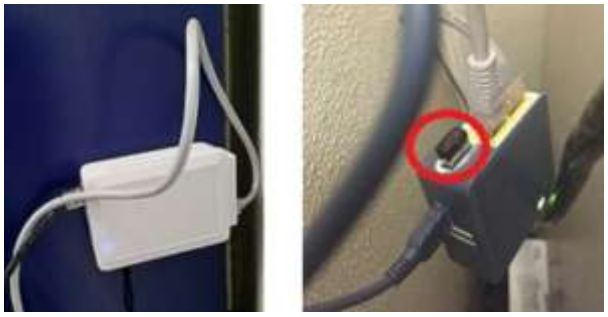
DIRECTOR'S OFFICE

(U) Overview

(U//FOUO) As of early 2016, card skimming crews targeted standalone ATM terminals in at least three US states and the Dominican Republic, with devices that intercept data in transit through the ATMs' external cables. This differs from previously observed wiretap devices which Romanian and other criminal groups placed inside ATM terminals in the United States, the United Arab Emirates (UAE), and the United Kingdom to capture data directly from the ATMs' card readers.

(U//FOUO) According to private sector reporting[1] in February 2016, external eavesdropping skimming devices were recovered from NCR and Diebold ATMs in California, Delaware, and Pennsylvania. The devices captured card data from the main ATM network communication cable during customer transactions but required additional devices to capture customers' personal identification numbers (PINs), which were encrypted upon entry on keypads. According to open source reporting[2], ATM manufacturer NCR issued a warning about these devices and reported a keyboard overlay was used to obtain PINs at a NCR ATM, while the Diebold ATM attacks used a concealed micro camera. External power sources resembling cell phone chargers were recovered.

(U//FOUO) No details were given about the US-based perpetrators, but FBI information indicates as of March 2016, Bulgarian skimmers in the Dominican Republic sought to identify standalone ATMs, as they could extract customer information using the wires behind the terminals.[3]



(U) To the right, an ATM compromised using this external "wiretapping" method, and to the left close-ups of the data-intercept device (left) and possible Bluetooth-enabled USB (right) linked to the ATM. PIN capture devices not pictured. Photos courtesy of KrebsonSecurity.com.

(U) This is not the first time skimmers have sought to exploit unencrypted ATM network communications with physical devices, though previous reports, dating to late 2014, noted the devices' placement inside the ATMs through various means, rather than on the ATMs' external wiring.

- (U//FOUO) As of July 2015, FBI information indicated identified Romanian ATM fraudsters had the faceplate key for an NCR brand kiosk ATM and planned to install a "wiretap" skimmer on the interior wiring to capture card numbers directly from the ATM's card reader rather than by reading the cards' magnetic stripes. The subjects used a camera wired directly into the ATM to capture customer PINs and

transmit them via Bluetooth to the subjects.[4] Previous reporting in December 2014 indicated skimming crews were installing "wiretapping" skimming devices by drilling or burning a hole in the ATM faceplate below the card reader slot and attaching the device directly to the magnetic card reader head.[5]

- (U) In June 2015, NCR issued an alert that thieves installed "card reader eavesdropping" devices by opening the "top box" of freestanding ATM terminals in the UAE. No holes were drilled into the ATM's fascia to gain access.[6] Open source reporting indicated access was gained by picking the locks, though the underlying source for this detail was not provided.[7]

(U) At right, a "top box" eavesdropping skimmer, photo courtesy of NCR Security Alert 2015-15.

- (U) In late 2014 open source reporting indicated the discovery of "wiretapping" skimmer devices installed through holes cut in the front of ATMs close to the card readers and concealed with plastic decals. This scheme was first observed targeting NCR ATMs in the United Kingdom in September of that year.[8,9]

(U) To the left, the hole cut in an ATM face to obtain access to place an internal wiretap device, and a decal used to conceal it. Photos courtesy of KrebsonSecurity.com.

(U//FOUO) These internal and external devices exploit a vulnerability in account data transmission between the ATM's card reader and its financial network. While PINs are required to be encrypted at the point of interaction by industry-standard encrypting PIN pads, account numbers may be transmitted "in the clear" (unencrypted), depending on each bank's practices, allowing interception for use in conjunction with other PIN capture methods, such as a concealed micro camera or keypad overlay.

(U//FOUO) Kiosk (or standalone) ATMs are particularly susceptible to skimming due to the general lack of anti-skimming technology or video surveillance in place at these terminals.

(U) Outlook

(U//FOUO) This represents one of numerous technological developments observed in the realm of ATM skimming. Although there is no information available about the criminals responsible for the external devices reported in the private sector, technical advancements in skimming have in the past been pioneered in large part by groups based out of Eastern Europe, especially Romania and Bulgaria.

(U//FOUO) It is neither suggested nor addressed in the noted reporting, but while drilling a hole in an ATM faceplate would obviously draw suspicion, skimming subjects could disguise themselves as service technicians to install and remove devices through non-destructive top box access or on external cables.

(U) DSAC would like to highlight the tactics ATM skimming crews may use to obtain customers' transaction information from standalone ATM machines. DSAC encourages financial institutions, casinos, and other companies with standalone ATMs on premises to take the information provided by this LIR into account and to review their internal procedures related to the maintenance and inspection of standalone ATMs as well as the verification of any ATM service technicians' authorization. Businesses with standalone ATMs should ensure personnel are familiar with the appearance of their ATM terminals, both external and internal if they have that access. Businesses are encouraged to contact the ATM owner or service provider if they have questions or notice anomalies regarding the appearance, operation, or maintenance of standalone ATMs.

(U) If you believe this activity may be taking place at standalone ATMs in your business's facilities, contact your local FBI Field Office.

OFFICE OF PRIVATE SECTOR

DIRECTOR'S OFFICE

(U) Endnotes

[1] (U) A private sector contact requesting non-attribution, reporting on 5 February 2016.
[2] (U) Blog post; KrebsonSecurity; "Skimmers Hijack ATM Network Cables"; 9 February 2016; https://krebsonsecurity.com/2016/02/skimmers-hijack-atm-network-cables/; accessed 9 February 2016; Source is a reputable cybersecurity expert and investigative reporter, citing an NCR security alert with limited distribution.
[3] (U) FBI case information dated 15 March 2016.
[4] (U) FBI case information dated 28 July 2015.
[5] (U) FBI case information dated 5 December 2014.
[6] (U) Industry report; NCR; 22 June 2015; "NCR Security Update – Card Skimming Advisory – New Variation of Card Reader Eavesdropping Attacks"; http://668781195408a83df63a-e48385e382d2e5d17821a5e1d8e4c86b.r51.cf1.rackcdn.com/external/NCR-Security-Alert-2015-05-Card-Reader-Evesdropping.pdf; NCR is a leading US and global manufacturer of ATMs and consumer transaction technologies.
[7] (U) Online article; Softpedia; Ionut Ilascu; "New Method for Reading Card Info at ATMs Discovered"; 25 June 2015; https://news.softpedia.com/news/ncr-alerts-of-new-method-used-for-reading-card-info-485253.shtml; accessed on 11 February 2016; Softpedia, owned by Romanian company SoftNews NET SRL, primarily provides software downloads and information but also reports news covering a variety of technology topics.
[8] (U) Blog post; KrebsonSecurity; "Skimmer Innovation: 'Wiretapping' ATMs"; 26 November 2015; http://krebsonsecurity.com/2014/11/skimmer-innovation-wiretapping-atms/; accessed 9 February 2016; Source is a reputable cybersecurity expert and investigative reporter.
[9] (U) Blog post; KrebsonSecurity; "More on Wiretapping ATM Skimmers"; 9 December 2014; http://krebsonsecurity.com/2014/12/more-on-wiretapping-atm-skimmers/; accessed 9 February 2016; Source is a reputable cybersecurity expert and investigative reporter.