Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

9 August 2018

PIN Number
20180809-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP: AMBER** The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

“Unlimited Operation” Schemes Pose an Immediate Threat to Financial Institutions

Summary

The FBI has obtained unspecified reporting indicating cyber criminals are planning to conduct a global Automated Teller Machine (ATM) cash-out scheme in the coming days, likely associated with an unknown card issuer breach and commonly referred to as an ”unlimited operation.” Unlimited operations compromise a financial institution or payment card processor with malware to access bank customer card information and exploit network access, enabling large scale theft of funds from ATMs. Unlimited operations have resulted in the theft of at least $2.5 million since 2016 in the United States alone. Historic compromises have included small-to-medium size financial institutions, likely due to less robust implementation of cyber security controls, budgets, or third-party vendor vulnerabilities. The FBI expects the ubiquity of this activity to continue or possibly increase in the near future.

Threat

Unlimited operations require unauthorized network access to targeted financial institutions to acquire and/or access customer debit accounts for alteration and use during the ATM cash-out. To successfully complete this scheme, criminals need:

1. Unauthorized access to unencrypted bank card data. This may originate from bank customer information, a payment card processor, a point-of-sale vendor, or be purchased from another cyber criminal.
2. The expertise and ability to manipulate security and anti-fraud protocols pertaining to:
   a. Account balances (available funds)
   b. Withdrawal limit (amount which can be taken out from a single account)
   c. Bank, card, and ATM specific security measures (warnings identifying fraudulent behavior and block transactions)

The cyber criminals typically create fraudulent copies of legitimate cards by sending stolen card data to co-conspirators who imprint the data on reusable magnetic strip cards, such as gift cards purchased at retail stores. At a pre-determined time, the co-conspirators withdraw account funds from ATMs using these cards.

The cyber criminals also alter account balances and security measures to make an unlimited amount of money available at the time of the transactions, allowing for large amounts of cash to be quickly removed from the ATM. Criminals are more likely to initiate this scheme during low visibility times to minimize detection and prolong access to ATMs without interruptions.

The cyber criminals will often launder these funds by converting them into virtual currency, investing in local or regional criminal enterprises, or transferring them overseas. Of note, unlimited operations are distinct from a similar scheme known as ATM jackpotting since the software or mechanics of the ATM are not altered to enable the disbursement of funds.

Recommendations

Financial Institutions

- Implement separation of duties or dual authorization procedures for account balance or withdrawal increases above a specified threshold.
- Implement application whitelisting to block the execution of malware.
- Block execution of files from TEMP directories, from which most phishing malware attempts to execute.
- Monitor, audit, and limit administrator and business critical accounts with the required access and authority to modify the account attributes mentioned above.

- Monitor for remote network protocols and administrative tools used to pivot back into the network or conduct post-exploitation of a network, such as PowerShell, Cobalt Strike, and TeamViewer.
- Monitor for SSL or TLS traffic over non-standard ports.
- Monitor for network traffic to regions wherein you would not expect to see outbound connections from your financial institution.
- Scrutinize attachments and Web site hyperlinks contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Implement strong password requirements and two-factor authentication using a physical or digital token when possible for local administrators and business critical roles to inhibit lateral movement.
- Implement an update and patch management cycle.
- Install and regularly update anti-virus or anti-malware software on hosts.
- Implement an incident management system, and prepare an incident response plan for rapid deployment in case of a cyber intrusion.
- Update software for ATMs regularly and maintain awareness of security incidents associated with similar ATMs.
- Identify areas in systems that disarm alerts, and determine best practices when tampered with.
- Implement chip and PIN procedures for debit cards to restrict criminals from using store purchased gift cards as fake debit cards.
- Upgrade PowerShell to new versions with enhanced logging features, and centralize logs to detect usage of commonly used malware-related PowerShell commands.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers.

Card Owner

- Educate consumers on appropriate preventive and reactive actions to social engineering threats, including how employees from the financial institution should respond in their respective position and environment.
- Require multiple approval authorities for account alterations, and encourage two-factor authentication when available.
- Use discretion when posting to social media and company Web sites, especially job duties/descriptions, hierarchal information, and out-of-office details.
- See other published Privacy Industry Notifications, especially those related to Business Email Compromise.

This product is marked **TLP: AMBER**. Recipients may share **TLP: AMBER** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: AMBER** information may not be released outside of the community.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey