
**CIG Circular 72 – FASTCash ISO 8583-Specific Windows Malware Identified**

Date: 3/25/2019

TRAFFIC LIGHT PROTOCOL (TLP): WHITE – SUBJECT TO STANDARD COPYRIGHT RULES, TLP:WHITE INFORMATION MAY BE DISTRIBUTED WITHOUT RESTRICTION.

*Treasury is providing this Circular to inform the financial services sector about newly identified malware associated with FASTCash activity first described in* CIG Circular 66 – FASTCash ATM Cash Out Campaign*. This Circular includes an overview of the malware, file details, malware analysis, and detection and mitigation recommendations. Activity associated with FASTCash should be given the highest priority for enhanced mitigation and reported to the FBI or DHS National Cybersecurity and Communications Integration Center (NCCIC).*

**OVERVIEW**

Treasury has identified previously unknown malware that we have associated with FASTCash. In October 2018, we exposed FASTCash's capability to manipulate AIX servers running a bank's switch application to intercept financial request messages and reply with fraudulent but legitimate-looking affirmative response messages to enable extensive ATM cash outs. The newly identified malware provides FASTCash the additional capability to intercept and manipulate financial messages processed on a Windows server.

**FASTCash deployed financial message modification malware to a bank in Africa in July 2018.** The malware probably was in use as late as August 2018. Although the malware is Windows based and designed for the standardized ISO 8583 message format, it was not specific to the targeted bank suggesting FASTCash may attempt to use the same tool against other banks.

- We are not aware of any financial loss from ATM cash outs associated with this incident but the bank appears to have suffered significant and extended degradation in ATM services during purported response and recovery efforts.
- FASTCash used malware previously identified by Treasury in *CIG Circular 65 – APT-Connected RAT Associated with Financial Sector Intrusion Activity Related to Fraudulent Use of SWIFT* to deploy this newly identified malware on the victim bank's network, according to technical analysis.

**FASTCash continues to demonstrate sophisticated knowledge of standardized financial interchange messaging.** FASTCash also appears to have used modified publically available source code to write parts of the tool, probably to speed development.

- The malware contains code probably taken from open source repositories on the Internet to create hashmaps, hook functions, and parse ISO 8583 messages. FASTCash, however, appears to have modified the parsing code to support EBCIDC encoding. EBCDIC is a character encoding format like the more commonly used ASCII.
- The malware can inject itself into software running on a Windows platform. The malware then takes control of the software's network send and receive functions allowing FASTCash to manipulate ISO 8583 messages.

Want to learn more?

The malware described in this report appears to be functionally equivalent to the AIX inject applications and AIX ISO 8583 specific applications described in *CIG Circular 66 – FASTCash ATM Cash Out Campaign*. Additional information about these malicious AIX applications can be found at https://www.us-cert.gov/hiddencobra. Symantec has also analyzed samples of the AIX applications and named the AIX specific tool Trojan.Fastcash.

**FILE DETAILS**

Name: vspmvc.dll
MD5: A2B1A45A242CEE03FAB0BEDB2E460587
Compile Time: 3 July 2018 12:11:16 (unknown time zone)
File Size: 130560 bytes (127.5 KB)
Description: Windows malware designed to hook on the send and receive functions of ISO 8583 messages and parse and construct ISO 8583 messages.

**MALWARE ANALYSIS**

This file makes use of code from github to create hashmaps, hook functions, and parse ISO 8583 messages. The malware uses code from github.com/petewarden/c_hashmap for hashmaps, code from Microsoft's Detours Library at github.com/Microsoft/Detours to perform hooking, and code from github/sabit/Oscar-ISO8583 to parse ISO 8583 messages. The ISO 8583 code is slightly modified to facilitate the parsing of IBM037 (EBCDIC) formatted data.

The below table outlines files created or read from disk. Some files were encrypted using an unidentified block cipher.

| File Path | Encrypted? | Description |
|---|---|---|
| C:\intel\mvconf.ini | Yes | Configuration file that like contains Primary Account Numbers |

| File Path | Encrypted? | Description |
|---|---|---|
| C:\intel\mvblk.dat | Yes | Referred to as "blacklist" file in strings. If exists and contains the string "all", the blacklist is considered active |
| C:\intel_DMP_V\spvmdl.dat | No | Log file for success or failure of hook operation |
| C:\intel_DMP_V\spvmlog_%X.dat | No | Log file with status messages |
| C:\intel_DMP_V\spvmscap.dat | No | Log file with unknown purpose |
| C:\intel_DMP_V\spvmsuc.dat | Yes | Log file with unknown purpose |
| C:\intel_DMP_V\TMPL_%X.dat | No | Log file for metadata on send and receive calls |
| C:\intel_DMP_V\TMPR%X.TMP | No | Log file for received packets |
| C:\intel_DMP_V\TMPS%X.dat | No | Log file for sent packets |

The malware first parses the contents of mvconf.ini and populates a hashmap probably with expected illicit primary account numbers (PAN). Then it hooks on the receive and send functions of the process it was injected into. The send hook simply logs what data is sent on port 7029. The receive hook:

1) Parses the following ISO 8583 fields out of the incoming datagram: MESSAGE_TYPE_INDICATOR, PRIMARY_ACCOUNT_NUMBER, PROCESSING_CODE, RESERVED_NATIONAL_3.
2) Checks the hashmap for a match of the PAN from the inbound message. If the PAN is in the hashmap the malware continues processing, otherwise, the malware stops and presumably allows the legitimate software to normally process the message.
3) Checks if the blacklist file exists and that it contains the string "all" and sets the blacklist variable accordingly. This flag presumably determines if the malware fully runs or operates in a test mode where it does not generate actual response messages.
4) Determines processing path based on the MESSAGE_TYPE_INDICATOR and PROCESSING_CODE.
    a. If the message is a 0100, then the message is assumed to have come from a POS system according to the string: "Message comes from POS" and the code calls the GenerateResponsePOS function.
    b. If the message is a 0200 and the PROCESSING_CODE is 0x100000, then the message is assumed to be a transaction request from an ATM and the code calls the GenerateResponseTransaction1 function.
    c. If the message is a 0200 and the PROCESSING_CODE is 0x300000, then the message is assumed to be a balance inquiry request from an ATM and the code calls the GenerateResponseInquiry1 function.

To construct fraudulent but otherwise legitimate-looking response messages:

1) The malware uses the PRIMARY_ACCOUNT_NUMBER and ICC_DATA fields to construct what appears to be an EMV-specific message based on the parsing of the EMV tags from the ICC_DATA field and the use of a hard-coded value "KQ".
2) The suspected EMV-specific message also contains the hard-coded string "U8BFE0AE12F9000C1480B297BE43CAC97".
3) The malware sends the EMV-specific message to the localhost on port 9990 and then receives and parses the response.
4) The malware then reconstructs an ISO 8583 message filled with the following values:

| ISO 8583 Field | ISO 8583 Field Name | Value |
|---|---|---|
| 0 | MESSAGE_TYPE_INDICATOR | 0110 or 0210 |
| 2 | PRIMARY_ACCOUNT_NUMBER | Copied from request |
| 3 | PROCESSING_CODE | Copied from request |
| 4 | AMOUNT_TRANSACTION | Copied from request |
| 7 | TRANSMISSION_DATE_TIME | Copied from request |
| 11 | SYSTEM_TRACE_AUDIT_NUMBER | Copied from request |
| 15 | SETTLEMENT_DATE | Copied from request |
| 19 | ACQUIRING_INSTITUTION_CC | Copied from request |
| 23 | APPLICATION_PAN_SEQUENCE_NUMBER | Copied from request |
| 25 | POS_CONDITION_CODE | Copied from request |
| 32 | ACQUIRING_INSTITUTION_INDENTIFICATION_CODE | Copied from request |
| 37 | RETRIEVAL_REFERENCE_NUMBER | Copied from request |
| 38 | AUTHORIZATION_IDENTIFICATION_RESPSONSE | Randomly generated |
| 39 | RESPONSE_CODE | 00 (success) if blacklist is not set<br>51 (insufficient funds) if blacklist is set |
| 41 | CARD_ACCEPTOR_TERMINAL_INDENTIFICATION | Copied from request |
| 42 | CARD_ACCEPTOR_IDENTIFICATION_CODE | Copied from request |
| 44 | ADDITIONAL_RESPONSE_DATA | Copied from request if present |
| 49 | CURRENCY_CODE_TRANSACTION | Copied from request |
| 55 | ICC_DATA | Possibly written from response to EMV-specific message |
| 63 | RESERVED_PRIVATE_3 | Copied from request |

Finally, the malware populates a buffer with the following fields presumably to tee up the response message for sending:

| ISO 8583 Field | ISO 8583 Field Name |
|---|---|
| 0 | MESSAGE_TYPE_INDICATOR |
| 2 | PRIMARY_ACCOUNT_NUMBER |
| 3 | PROCESSING_CODE |
| 4 | AMOUNT_TRANSACTION |
| 7 | TRANSMISSION_DATE_TIME |
| 35 | TRACK_2_DATA |
| 38 | AUTHORIZATION_IDENTIFICATION_RESPSONSE |
| 39 | RESPONSE_CODE |
| 41 | CARD_ACCEPTOR_TERMINAL_INDENTIFICATION |
| 43 | CARD_ACCEPTOR_NAME_LOCATION |
| 49 | CURRENCY_CODE_TRANSACTION |
| 54 | ADDITIONAL_AMOUNTS |
| 60 | RESERVED_NATIONAL_3 |

## DETECTION AND MITIGATION RECOMMENDATIONS

1. Contact law enforcement immediately regarding any identified activity related to FASTCash. Please see contact information for FBI and DHS NCCIC at the end of this report.
2. Incorporate the indicators of compromise identified in DHS's Malware Analysis Report MAR-10201537 on https://www.us-cert.gov/hiddencobra and from *CIG Circular 65 – APT-Connected RAT Associated with Financial Sector Intrusion Activity Related to Fraudulent Use of SWIFT* into intrusion detection systems and security alert systems to enable active blocking or reporting of suspected malicious activity.

### Recommendations for Institutions with Retail Payment Systems

Require Chip and PIN Cryptogram Validation

- Implement Chip and PIN requirements for debit cards.
- Validate card-generated authorization request cryptograms.
- Use issuer-generated authorization response cryptograms for response messages.
- Require card-generated authorization response cryptogram validation to verify legitimate response messages.

Isolate Payment System Infrastructure

- Require two factor authentication for any user to access the switch application server.
- Confirm perimeter security controls prevent Internet hosts from accessing the private network infrastructure servicing your payment switch application server.
- Confirm perimeter security controls prevent all hosts outside of authorized endpoints from accessing your system, especially if your payment switch application server must be Internet accessible.

Logically Segregate your Operating Environment

- Use firewalls to divide your operating environment into enclaves.
- Use access control lists to permit/deny specific traffic from flowing between those enclaves.
- Give special considerations to segregating enclaves holding sensitive information (e.g., card management systems) from enclaves requiring Internet connectivity (e.g., email).

Encrypt Data in Transit

- Secure all links to payment system engines with a certificate based mechanism, such as MTLS, for all traffic external or internal to your organization.
- Limit the number of certificates that can be used on the production server and restrict access to those certificates.

Monitor for Anomalous Behavior as Part of Layered Security

- Configure the switch application server to log transactions and routinely audit transaction and system logs.

- Develop a baseline of expected software, users, and logons and monitor switch application servers for unusual software installations, updates, account changes, or other activities outside of expected behavior.
- Develop a baseline of expected transaction participants, amounts, frequency, and timing. Monitor and flag anomalous transactions for suspected fraudulent activity.

**Recommendations for Organizations with ATM or POS Devices**

Validate Issuer Responses to Financial Request messages

- Implement Chip and PIN requirements for debit cards.
- Require and verify message authentication codes on issuer financial request response messages.
- Perform authorization response cryptogram validation for CHIP and PIN transactions.

**Recommendations for All Organizations**

Treasury reminds users and administrators to use the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and require regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, and configure it to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the Internet before executing.
- Maintain situational awareness of the latest threats.
- Implement appropriate access control lists.

Additional information on malware incident prevention and handling can be found in NIST's Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops:

https://www.nist.gov/publications/guide-malware-incident-prevention-and-handling-desktops-and-laptops

**REPORTING FASTCash ACTIVITY**

To report an intrusion and request resources for incident response or technical assistance, contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), FBI through a local field office (https://www.fbi.gov/contact-us/field-offices) or FBI Cyber Division (CyWatch@fbi.gov or 855-292-3937).

The Financial Sector Cyber Information Group (CIG) was established within the Department of the Treasury, Office of Critical Infrastructure Protection and Compliance Policy in 2013. The CIG monitors and analyzes all-source information on cyber threats and vulnerabilities to the financial sector; provides timely, actionable cyber threat information to the sector; and solicits feedback and information requirements from the sector. Please take a moment to let us know:

Does this CIG Circular provide information that is not available to you elsewhere?
Is the information provided actionable?
Is the level of context appropriate?

Please direct any comments or questions to CIG@Treasury.gov.

CIG Circulars and Indicator Lists are being provided "as-is" for informational purposes only. The Treasury Department does not provide any warranties of any kind regarding any information contained within. Eligible stakeholders can download CIG Circulars and other relevant government information from the DHS Homeland Security Information Network (HSIN) Financial Services Portal. For information on membership, download the quick guide from: http://go.usa.gov/3YH45