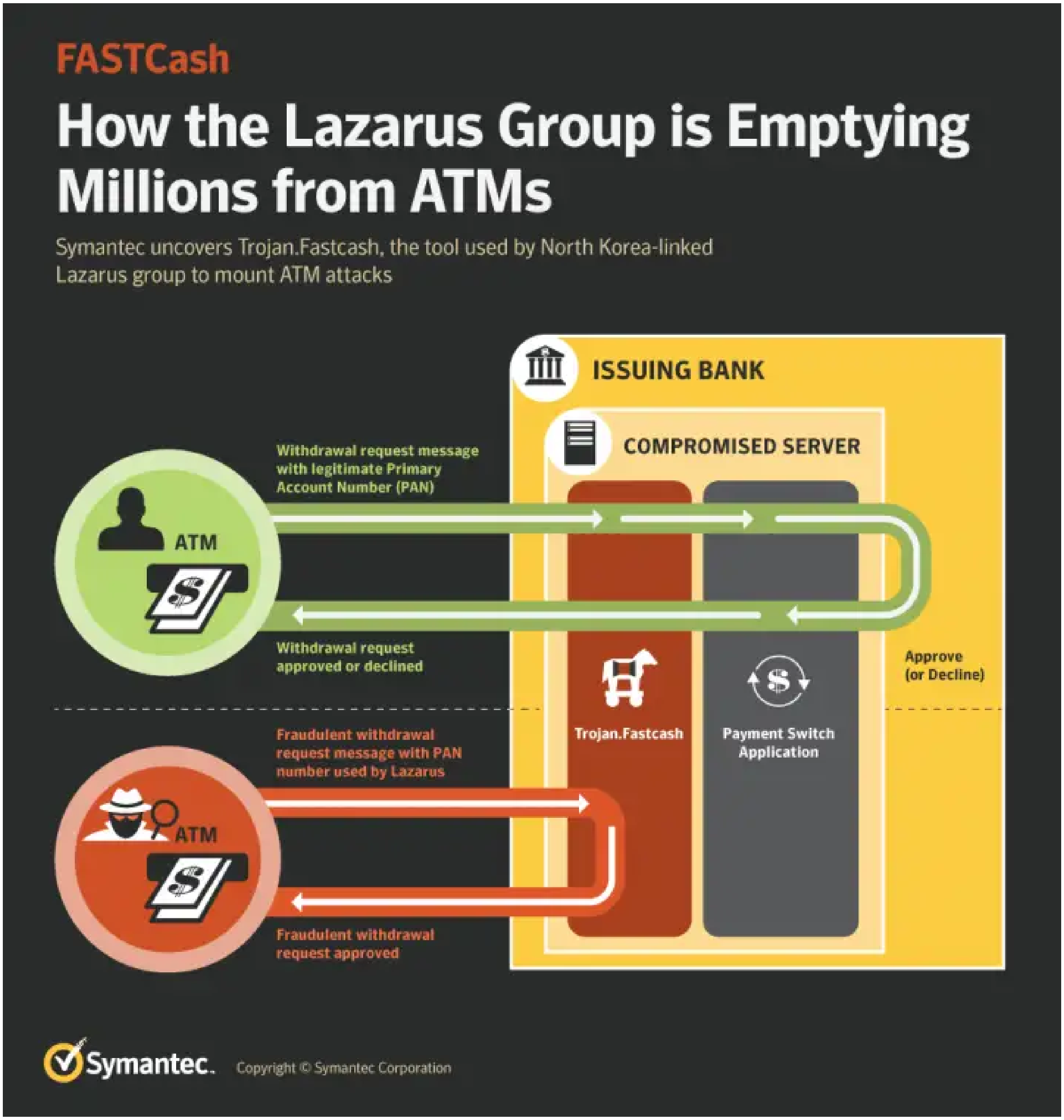
# FASTCash: How the Lazarus Group is Emptying Millions from ATMs

symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware



FASTCash

How the Lazarus Group is Emptying Millions from ATMs

Symantec uncovers Trojan.Fastcash, the tool used by North Korea-linked Lazarus group to mount ATM attacks

ISSUING BANK
COMPROMISED SERVER
Withdrawal request message with legitimate Primary Account Number (PAN)
ATM
Withdrawal request approved or declined
Approve (or Decline)
Trojan.Fastcash
Payment Switch Application
Fraudulent withdrawal request message with PAN number used by Lazarus
ATM
Fraudulent withdrawal request approved
Symantec.

Copyright © Symantec Corporation

## How FASTCash attacks work - Details

In order to permit their fraudulent withdrawals from ATMs, the attackers inject a malicious Advanced Interactive eXecutive (AIX) executable into a running, legitimate process on the switch application server of a financial transaction network, in this case a network handling ATM transactions. The malicious executable contains logic to construct fraudulent ISO 8583 messages. ISO 8583 is the standard for financial transaction messaging. The purpose of this executable has not been previously documented. It was previously believed that the attackers used scripts to manipulate legitimate software on the server into enabling the fraudulent activity.

However, analysis by Symantec has found that this executable is in fact malware, which we have named Trojan.Fastcash. Trojan.Fastcash has two primary functions:

1. It monitors incoming messages and intercepts attacker-generated fraudulent transaction requests to prevent them from reaching the switch application that processes transactions.
2. It contains logic that generates one of three fraudulent responses to fraudulent transaction requests.

Once installed on the server, Trojan.Fastcash will read all incoming network traffic, scanning for incoming ISO 8583 request messages. It will read the Primary Account Number (PAN) on all messages and, if it finds any containing a PAN number used by the attackers, the malware will attempt to modify these messages. How the messages are modified depends on each victim organization. It will then transmit a fake response message approving fraudulent withdrawal requests. The result is that attempts to withdraw money via an ATM by the Lazarus attackers will be approved.

Here is one example of the response logic that Trojan.Fastcash uses to generate fake responses. This particular sample has logic to construct one of three fake responses based on the incoming attacker request:

```
For Message Type Indicator == 200 (ATM Transaction) and Point of Service Entry
Mode starts with 90 (Magnetic Strip only):

  If Processing Code starts with 3 (Balance Inquiry):

        Response Code = 00 (Approved)

  Otherwise, if the Primary Account Number is Blacklisted by Attackers:

        Response Code = 55  (Invalid PIN)

  All other Processing Codes (with non-blacklisted PANs):

         Response Code = 00 (Approved)
```

In this case, the attackers appear to have built in a capability to selectively deny transactions based on their own blacklist of account numbers. However, the capability was not implemented in this sample, and the check for blacklisting always returns “False”.

Symantec has found several different variants of Trojan.Fastcash, each of which uses different response logic. We believe that each variant is tailored for a particular transaction processing network and thus has its own tailored response logic.

The PAN numbers used to carry out the FASTCash attacks relate to real accounts. According to the US-CERT report, most accounts used to initiate the transactions had minimal account activity or zero balances. How the attackers gain control of these accounts remains unclear. It is possible the attackers are opening the accounts themselves and making withdrawal requests with cards issued to those accounts. Another possibility is the attackers are using stolen cards to perform the attacks.

In all reported FASTCash attacks to date, the attackers have compromised banking application servers running unsupported versions of the AIX operating system, beyond the end of their service pack support dates.

## Who is Lazarus?

Lazarus is a very active group involved in both cyber crime and espionage. Lazarus was initially known for its involvement in espionage operations and a number of high-profile disruptive attacks, including the 2014 attack on Sony Pictures that saw large amounts of information being stolen and computers wiped by malware.

In recent years, Lazarus has also become involved in financially motivated attacks. The group was linked to the $81 million theft from the Bangladesh central bank in 2016, along with a number of other bank heists.

Lazarus was also linked to the WannaCry ransomware outbreak in May 2017. WannaCry incorporated the leaked “EternalBlue” exploit that used two known vulnerabilities in Windows (CVE-2017-0144 and CVE-2017-0145) to turn the ransomware into a worm, capable of spreading itself to any unpatched computers on the victim’s network and also to other vulnerable computers connected to the internet. Within hours of its release, WannaCry had infected hundreds of thousands of computers worldwide.

## Ongoing threat to the financial sector

The recent wave of FASTCash attacks demonstrates that financially motivated attacks are not simply a passing interest for the Lazarus group and can now be considered one of its core activities.

As with the 2016 series of virtual bank heists, including the Bangladesh Bank heist, FASTCash illustrates that Lazarus possesses an in-depth knowledge of banking systems and transaction processing protocols and has the expertise to leverage that knowledge in order to steal large sums from vulnerable banks.

In short, Lazarus continues to pose a serious threat to the financial sector and organizations should take all necessary steps to ensure that their payment systems are fully up to date and secured.

## Protection

Symantec has the following detections in place to protect customers against Lazarus FASTCash attacks:

- Trojan.Fastcash

## Mitigation

Organizations should ensure that operating systems and all other software are up to date. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by attackers. In all reported FASTCash attacks to date, the attackers have compromised banking application servers running unsupported versions of the AIX operating system, beyond the end of their service pack support dates.

## Indicators of Compromise

D465637518024262C063F4A82D799A4E40FF3381014972F24EA18BC23C3B27EE
(Trojan.Fastcash Injector)

CA9AB48D293CC84092E8DB8F0CA99CB155B30C61D32A1DA7CD3687DE454FE86C
(Trojan.Fastcash DLL)

10AC312C8DD02E417DD24D53C99525C29D74DCBC84730351AD7A4E0A4B1A0EBA
(Trojan.Fastcash DLL)

3A5BA44F140821849DE2D82D5A137C3BB5A736130DDDB86B296D94E6B421594C
(Trojan.Fastcash DLL)