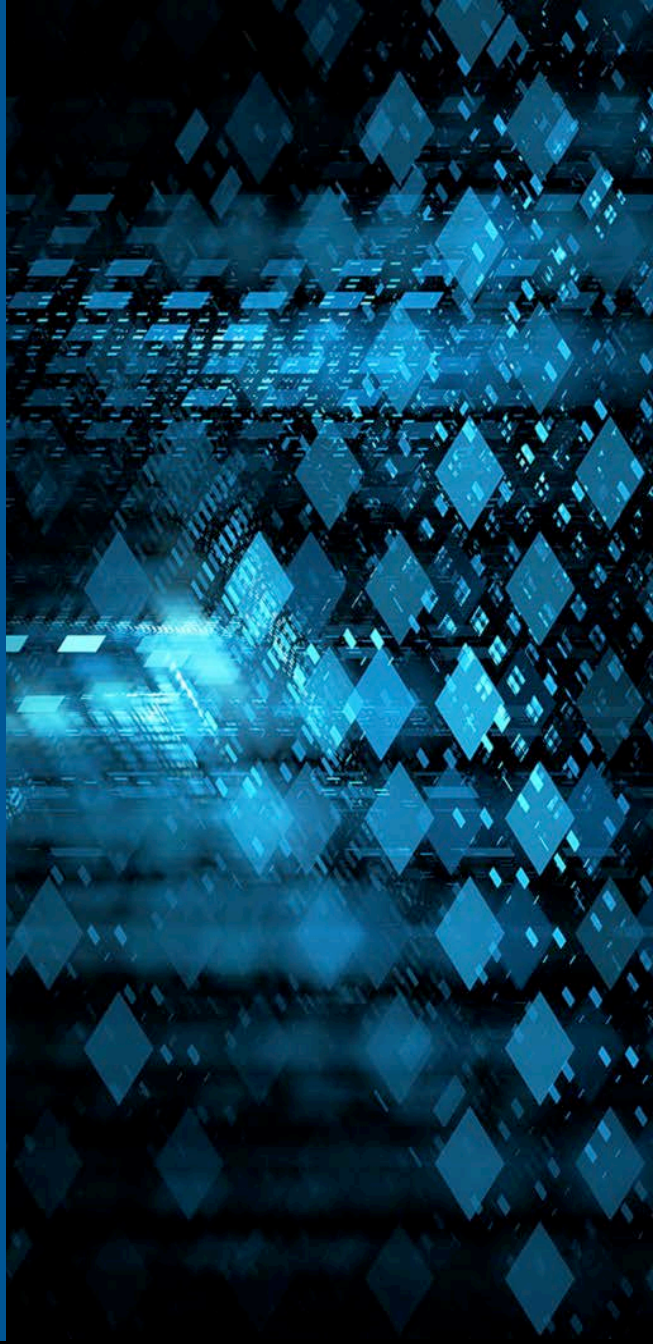
ACH Account Takeover Fraud

Alexander Volynkin, Ph.D.

CERT - Carnegie Mellon University

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



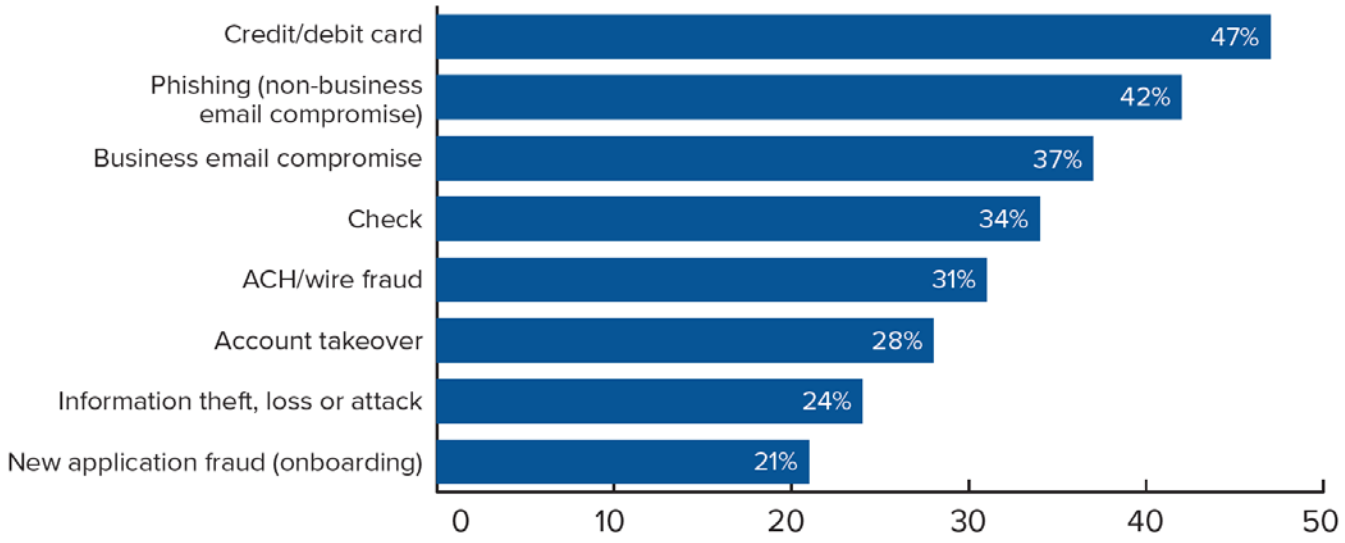
Legal

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0576

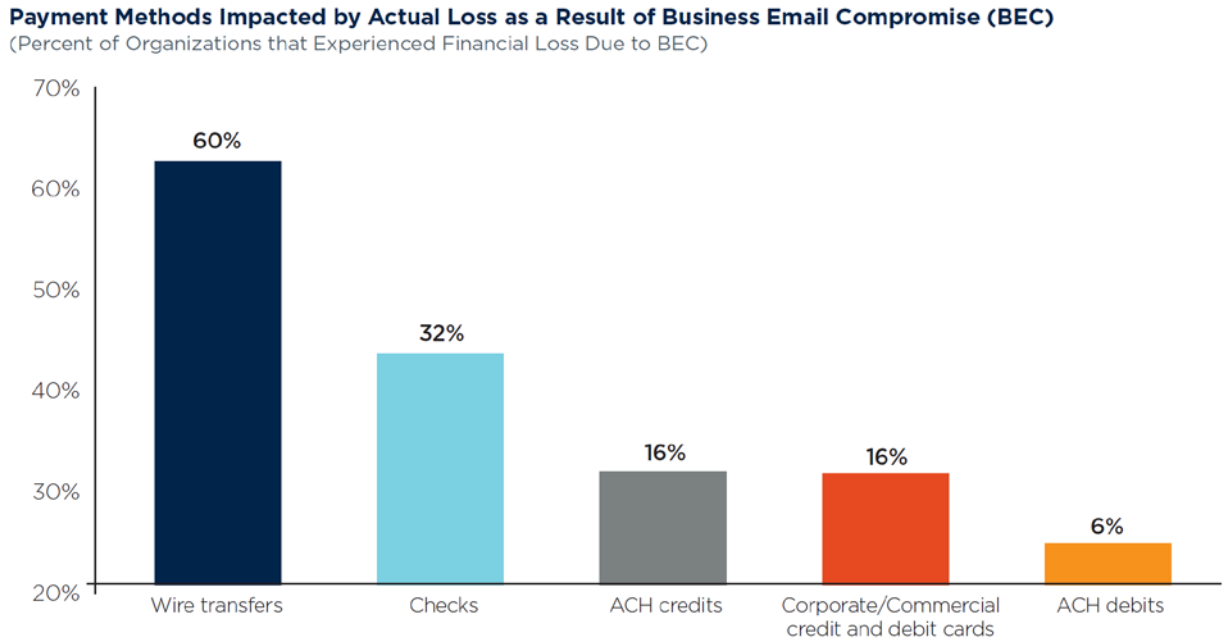
Common Corporate Fraud Types in 2017

Picture (optional)



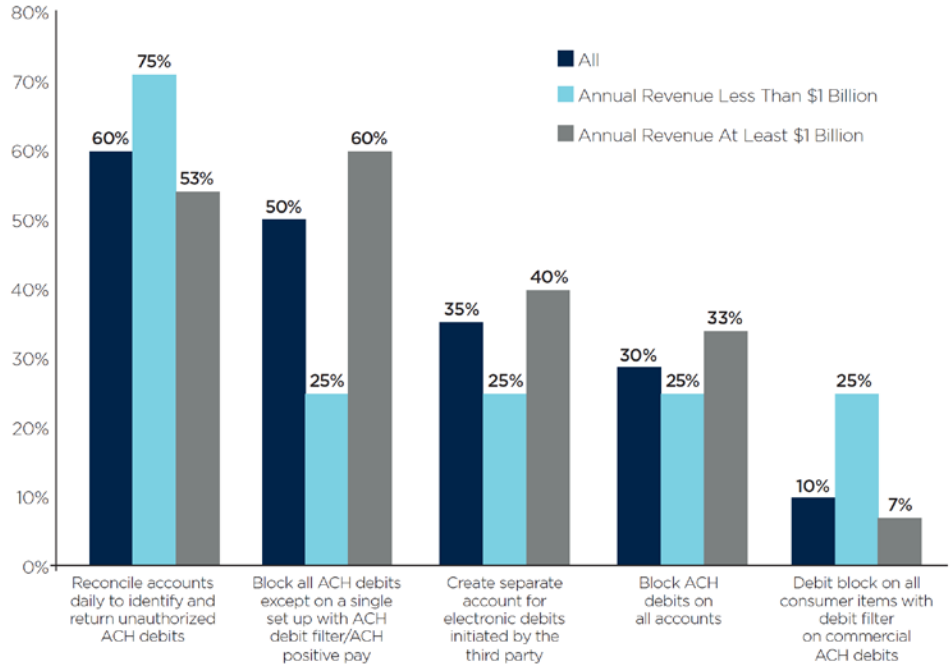
Payment Methods Impacted by BEC

Picture (optional)



Fraud Control Procedures Used to Prevent ACH Fraud

Picture (optional)



ACH Account Takeover at a Glance

Picture (optional)

Malware such as Black Hole Exploit, Zeus, Citadel, is built.

Malware sent via attachments or phish attempts through spam.

User opens attachment or follows link.

Executes malicious code on PC and/or Network.

Hacker monitors compromised PC and waits for user to access accounts.

Staff member signs into Online Banking.

Hacker hijacks Online Banking session when user enters credentials/token.

Hacker creates fraudulent ACH or Wire Transfer.

Fraudulent transaction sent to bank for processing.

Bank receives what appears to be a legitimate request.

NACHA's Most Common Phishing Titles

The Federal Deposit Insurance Corporation (FDIC) regarding your business's ACH activity

NACHA indicating that your business's ACH membership has expired

ADP, a payroll service company

The bank, related to a rejected wire transfer

Law enforcement agencies issuing traffic violations in New York City

Adobe Software regarding an upgrade for Adobe Acrobat Reader and Adobe X Suite Advanced

A credit card company regarding an overdue payment

The Better Business Bureau

Booking.com, a hotel booking website, regarding a reservation

Shipping companies, such as FedEx, UPS or DHL, regarding a parcel that was not properly delivered

PayPal regarding changes to your email address, an account review notification or your account availability

Typical Attack Scenario

Choose a company

- Small/Medium size preferred: more likely to not have additional security policies in place

Introduce malware

- Email/Phishing most common
- Network infrastructure compromise

Additional attack measures

- Social engineering
- Personal/business account compromise

Access bank account

Typical Attack Scenario (Cont)

Execute supplemental attacks

Commence Wire Transfer

- Same day ACH anyone?

Minimize early detection

- Keep IT busy
- Admin/management personal

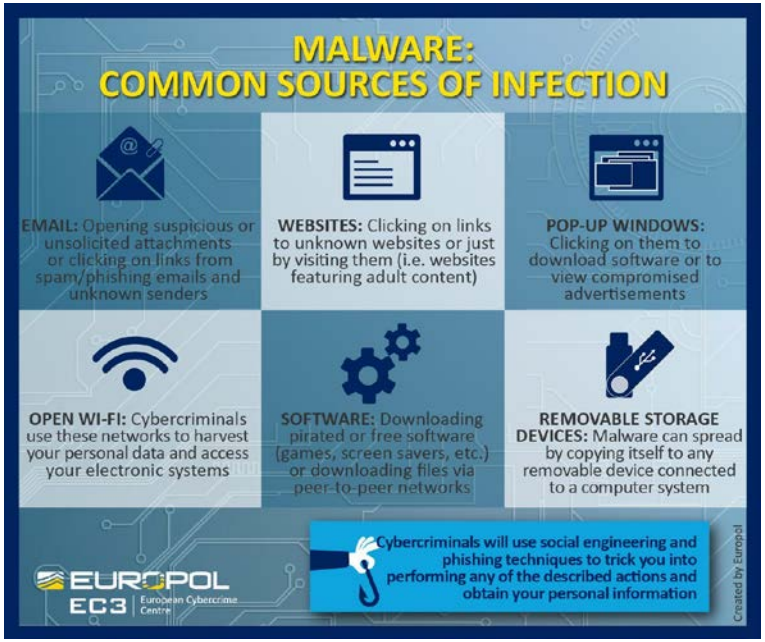
Collect Money

Example: Inject malware

Picture (optional)

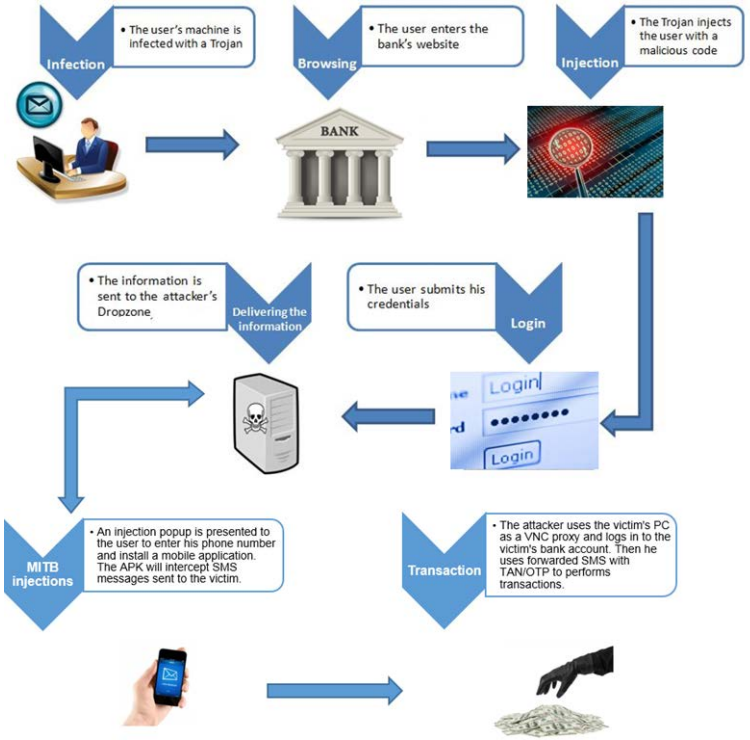
CEO's computer infected with Neverquest malware

- Attack vector unknown, email/phishing is likely suspect



Example: Neverquest

Picture (optional)



Example: Attack Commences

Picture (optional)

Neverquest captures CEO's bank account login credentials

Neverquest opens backdoor to CEO's computer

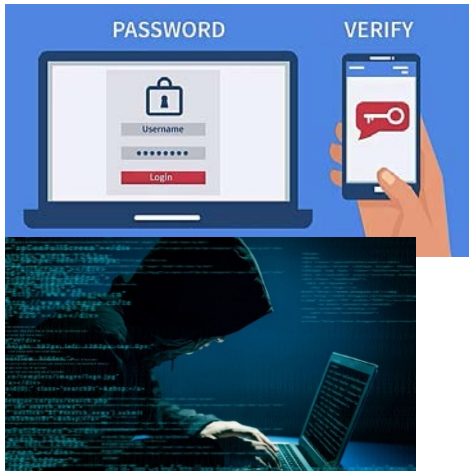
Attacker uses compromised computer and credentials to gain access to bank account

- No security alerts regarding unknown IP address

CEO uses two-factor authentication via his phone, but….

- Attacker already compromised his cell phone online account
- All messages and phone call redirected to attacker

One time security code intercepted by attacker



Example: Bank Account Hacked

Picture (optional)

Attacker gains access to bank account, but…

- Wire transfer requires second user approval (wait for it…)

CEO's user account has full admin privileges

- Attacker creates second user
- New user approves wire transfer

Wire transfer sent to bank

Example: Game not over yet

Picture (optional)

Wire transfer not yet cleared and can be cancelled

- Bank security team
- At ACH level
- Company accounting and security

Let’s distract company employees just long enough for the transfer to go through

- Send massive spam tsunami
- Tens of thousands of emails sent to accounting, security and CEO’s mailboxes

Example: Bank Gets Involved

Bank fraud prevention flags wire transfer transaction

- Large amount
- Out of pattern for this company

Calls customer's phone number of file

- CEO's cell number
- Already hijacked by attacker

Attacker picks up the phone and talks to the bank

- Stresses urgency of transaction
- Appears to be nervous

Bank puts transaction on hold

CEO eventually calls off the transfer

Corporate Account Takeover can be APT

Attackers research victims' schedule

- CFO travelling – perfect time to spoof email assistant to transfer funds

Attackers compromise personal and other business accounts

- Phone accounts let attackers redirect text messages and calls
- Email accounts for confirmation messages and early warnings
- Additional account credentials revealed through these means as well
- Cloud storage reveals accounting data, available funds, schedule of management team, etc.

Global Fraud Index Report

Key Findings Include:

45 percent: Increase in account takeovers in Q2 2017

$3.3 billion: Amount lost by merchants to account takeovers in Q2 2017

$57.8 billion: Value of potential fraud in the eight industries studied by the Index

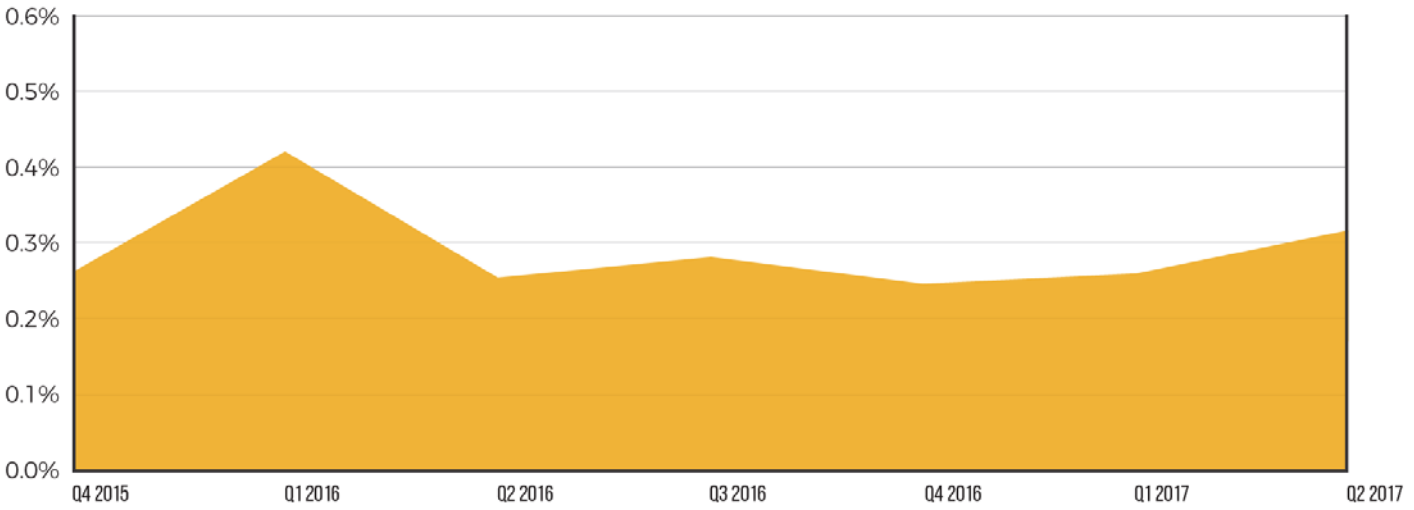
5.5 percent: Increase in total fraud from Q2 2016 to Q2 2017

11.64 percent: Fraud rate of transactions over $500, 22 times higher than the fraud rate for transactions worth less than $100

Picture (optional)

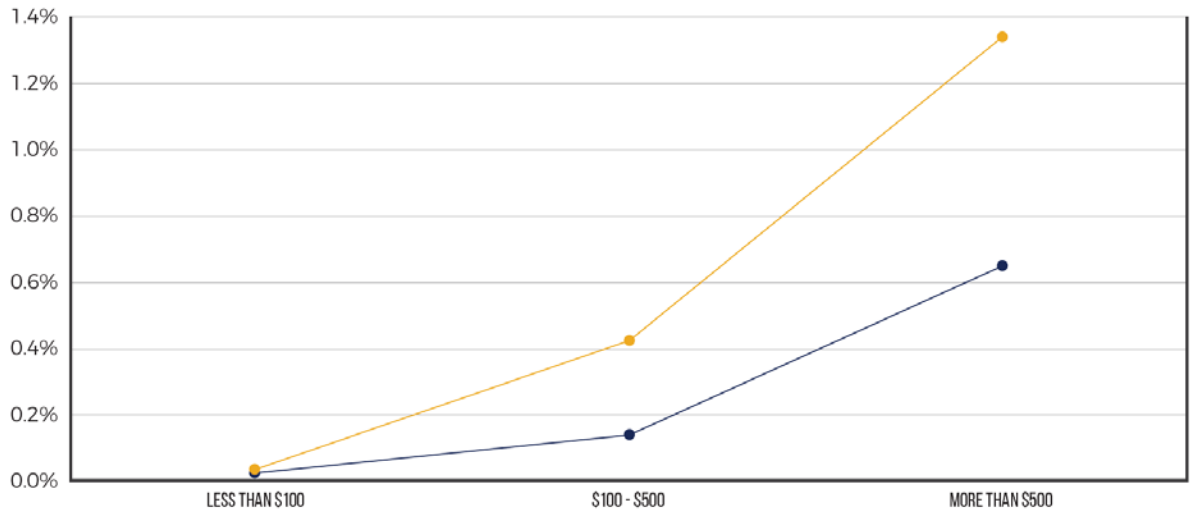
Likely due to recent data breaches (Equifax2)

Account Takeovers Jump 45% in Q2, 2017



Retail Account Takeovers

Particularly intensified with fraudulent transactions over $100



Corporate Account Takeover Losses

Mattel - $3mln in one reported instance in 2016

- Money transferred to China. May Day saved the money: Bank holiday in China; Transfer stopped in time by Chinese authorities.

Ubiquiti - $46mln aggregate

- Hong Cong subsidiary got hit; initiated multiple transactions to various countries
- $8mln was eventually recovered

The Scoular Co. - $17mln

- CEO wired funds in multiple transactions to China

Vendor Impersonation Fraud

Attacker contacts business pretending to be legitimate vendor or contractor

Requests to update account information including account number and routing

Next time vendor is paid, money go into attacker's account

Public sector is a particularly attractive target for this

- Vendor list is publicly available
- Fraud prevention policies lacking

Details of Business Email Compromise

Picture (optional)

Seller's email compromised (phishing, malware, etc.)

Attacker searches email for high valued transactions in preorder phase (i.e. request for a quote)

Attacker sets up redirects for future emails from selected buyers

Buyer sends purchase order to seller; Attacker intercepts PO

Attacker copies buyers' email content, uses slightly different email address

Seller responds to spoofed email address with invoice and payment instructions

Attacker modifies bank account details on the invoice and forwards to buyer

Buyer wires money to attackers' controlled bank account

Business email compromise (Cont)

In cases in which additional approval or paperwork was needed, the attackers found and filled out appropriate forms and spoofed supervisor emails to get required approvals

Malware not necessarily used in all cases

- Malware-based detection methods less effective

SWIFT Attacks

Bangladesh Bank attack

- Bank system infected with malware
- Malware allows attacker to inject fraudulent messages into SWIFT stream
- Malware hides these messages from being included in logs and printed ledgers

Odinaff

- Same concept, but different targets
- SWIFT software targeted specifically
- Log records removed
- Disk images affected

SWIFT Attacks

Far Eastern International Bank in Taiwan

- Malware planted to gain access to SWIFT terminals
- Keylogger/screen capture to get SWIFT terminal credentials
- Credentials were then used to transfer over $60m oversees
- All except $500,000 were recovered

Lazarus APT Targeting Banking

Central Bank of Bangladesh

150+ malware different samples used for different targets

Step 1. Web server compromise

- Either financial institution own web server
- Or a .GOV server used by financial institution
- Once compromised, only serves exploits to targets on whitelist
- Someone within financial institution visits website and gets compromised

Step 2. Backdoor installed

- Access to compromised system
- Start migrating to other systems within organization

Lazarus APT Example (Cont.)

Step 3. SWIFT terminals and messaging servers identified

- Enumerate backup servers
- IT admin systems
- Security measures identified

Step 4. Custom malware deployed to SWIFT software

- SWIFT credentials captured
- Disable security checks
- SWIFT message servers don’t report malicious transactions

Step 5. Start money transfers

South East Asia Bank SWIFT Attack

Picture (optional)

Happened shortly after Bangladesh Bank attack

Attackers were present within the company's infrastructure for over 7 months

Targeted attack. Malware compiled within hours of attack

Malware designed to avoid AV detection

Attacks happened outside of regular office hours

Disable internal integrity checks of SWIFT Alliance software to prep for infection

Keylogger was used to capture login credentials

SWIFT Software patched by malware

Passive and Active backdoors used

Bank's public web server was on the same network segment as their SWIFT server. Likely where the attack started

Questions?

avolynkin@cert.org