The Landscape of Finnancial & Banking Cyber Attacks

Roberto Kam

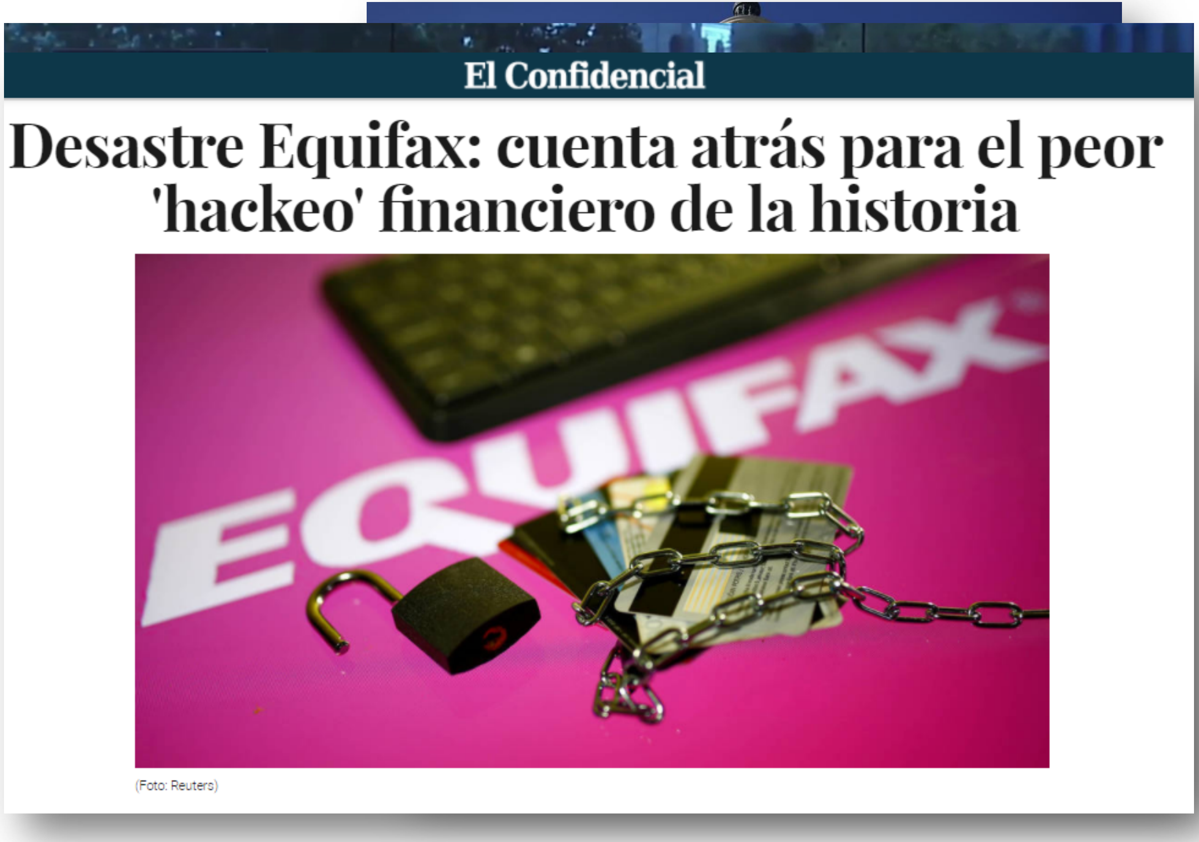
roberto_kam@trendmicro.com

https://www.youtube.com/watch?v=tyzQSk8TV9M

150 millones de afectados

Apache Struts CVE-2017-5638

Remote Code Execution Vulnerability



El Confidencial

Desastre Equifax: cuenta atrás para el peor 'hackeo' financiero de la historia

(Foto: Reuters)

How Cybercriminals get money from Banks & Financial Sector?

DIGITAL EXTORTION IN 2018

WHAT IT IS, HOW IT HAPPENS, AN… AGAINST IT

What assets are usually targeted?

Personal documents

What methods are used in the attack?

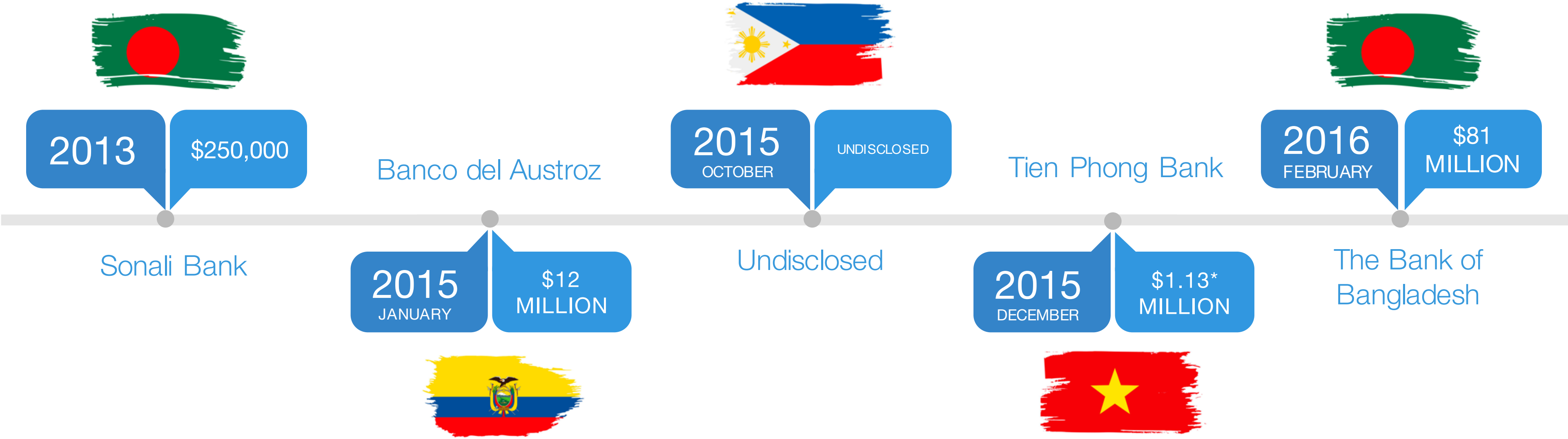
- Ransomware
- Online blackmail
- Online smear campaigns
- Equipment hijacking
- Negative review spamming
- Phishing

…ay secure?

- …ous behavior on social media.
- …go training and education to recognize digital extortion attempts.
- Install security solutions and secure all devices.
- Cooperate with social media administration staff to thwart harassment and smear campaigns.
- Never comply with cybercriminal demands.

Created by TrendLabs,
The Global Technical Support and R&D Center of TREND MICRO

FEDERAL RESERVE NOTE
HK 12955746 B
K11
HK 11218778 D
HA 05358189 B
THE UNITED STATES OF AMERICA
100
09290951 A
ONE HUNDRED DOLLARS
FK 55608223 A
HA 79852831 A



2013 | $250,000
Sonali Bank

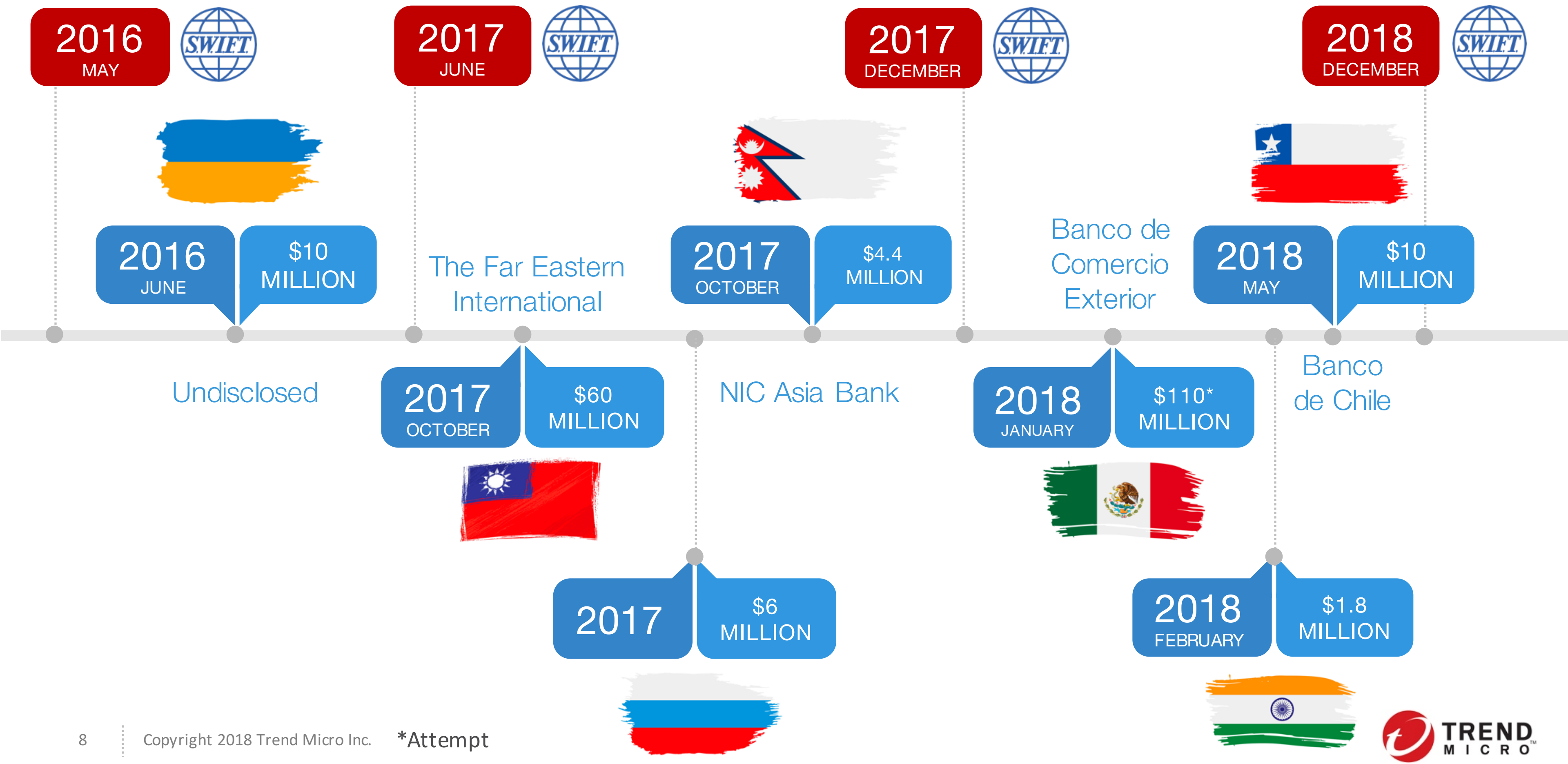
2015 JANUARY | $12 MILLION
Banco del Austroz

2015 OCTOBER | UNDISCLOSED
Undisclosed

2015 DECEMBER | $1.13* MILLION
Tien Phong Bank

2016 FEBRUARY | $81 MILLION
The Bank of Bangladesh

*Attempt



Customer Security Program (CSP) Introduced

2016 MAY

2016 JUNE $10 MILLION

Undisclosed

Customer Security Program (CSP) Becomes Mandatory

2017 JUNE

2017 OCTOBER $60 MILLION

The Far Eastern International

2017 $6 MILLION

2017 OCTOBER $4.4 MILLION

NIC Asia Bank

First self-attestation to be summited

2017 DECEMBER

2018 JANUARY $110* MILLION

Banco de Comercio Exterior

2018 FEBRUARY $1.8 MILLION

2018 MAY $10 MILLION

Banco de Chile

All users need to re-attest and confirm full compliance with the mandatory security controls

2018 DECEMBER

*Attempt

Important Dates for SWIFT CSP

- **By 31 December 2018:** All SWIFT users must re-attest and confirm full compliance with the mandatory security controls V1 (2018), dependent on the expiry date of the attestation.
- **From 1 January 2019**: SWIFT reserves the right to report users who have failed to self-attest full compliance with all mandatory security controls (or who connect through a non-compliant service provider) to their local supervisors.

Source: https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/our-kyc-solutions/the-kyc-security-attestation-application/features

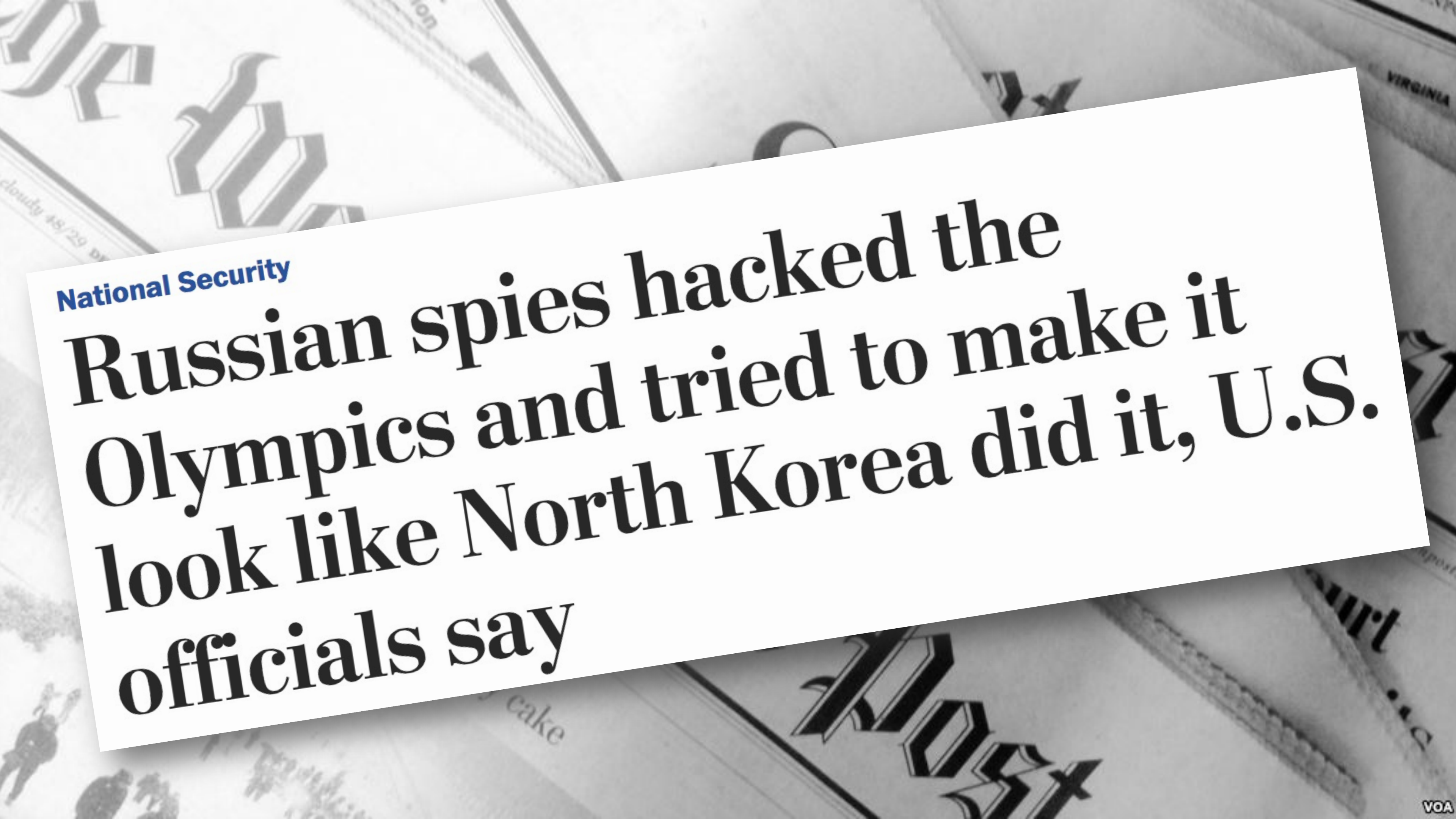
Important Dates for SWIFT CSP

- **By 31 December 2018:** All SWIFT users must re-attest and confirm full compliance with the mandatory security controls V1 (2018), dependent on the expiry date of the attestation.
- **From 1 January 2019**: SWIFT reserves the right to report users who have failed to self-attest full compliance with all mandatory security controls (or who connect through a non-compliant service provider) to their local supervisors.

Source: https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/our-kyc-solutions/the-kyc-security-attestation-application/features

Who? (Attribution)

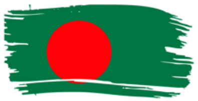
CYBERCRIMINALS
HACKTIVISTS
COMPANIES
MALICIOUS INDIVIDUALS
STATE ACTORS
TERRORISTS



National Security

Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say

VOA



2016
FEBRUARY

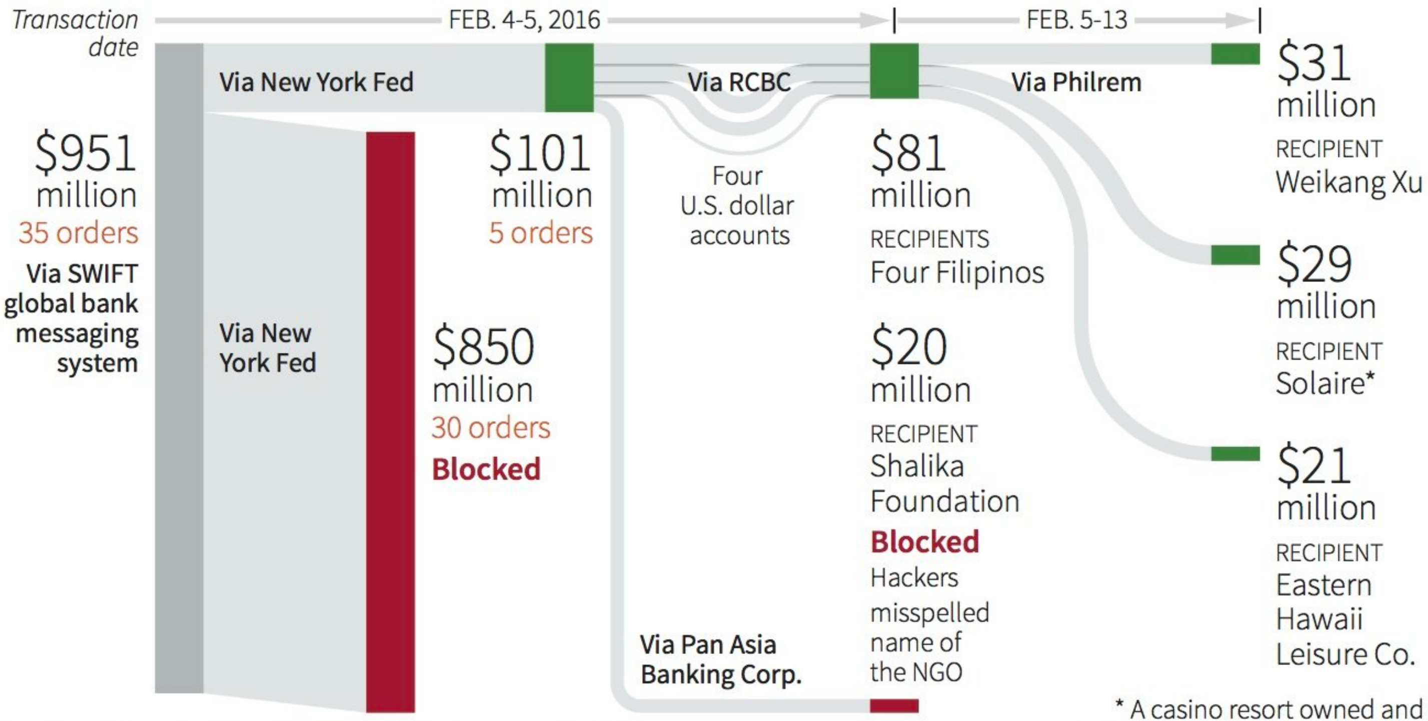
$81
MILLION

The Bank of Bangladesh

Bangladesh Bank heist

In one of the largest cyber heists in history, hackers ordered the Federal Reserve Bank of New York to transfer $81 million from Bangladesh Bank to accounts in the Philippines.

THE MONEY TRAIL



Transaction date

FEB. 4-5, 2016

FEB. 5-13

$951 million
35 orders
Via SWIFT global bank messaging system

Via New York Fed

Via New York Fed

$850 million
30 orders
Blocked

$101 million
5 orders

Via RCBC

Four U.S. dollar accounts

Via Pan Asia Banking Corp.

$81 million
RECIPIENTS
Four Filipinos

$20 million
RECIPIENT
Shalika Foundation
Blocked
Hackers misspelled name of the NGO

Via Philrem

$31 million
RECIPIENT
Weikang Xu

$29 million
RECIPIENT
Solaire*

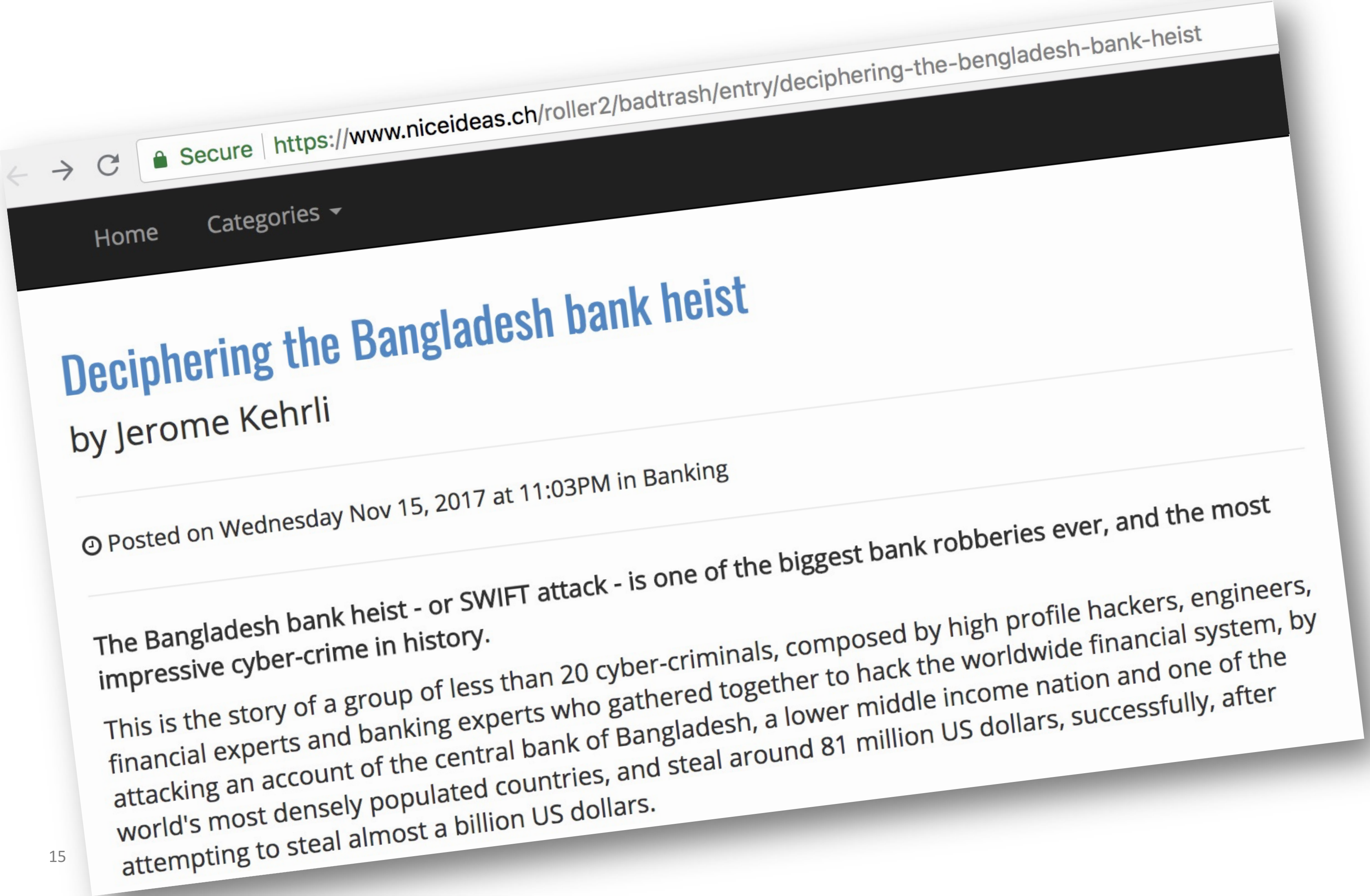
$21 million
RECIPIENT
Eastern Hawaii Leisure Co.

Sources: Philippines Court of Appeals documents; Reuters

* A casino resort owned and operated by Bloomberry Resorts

W. Foo, 31/03/2016

REUTERS



https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist

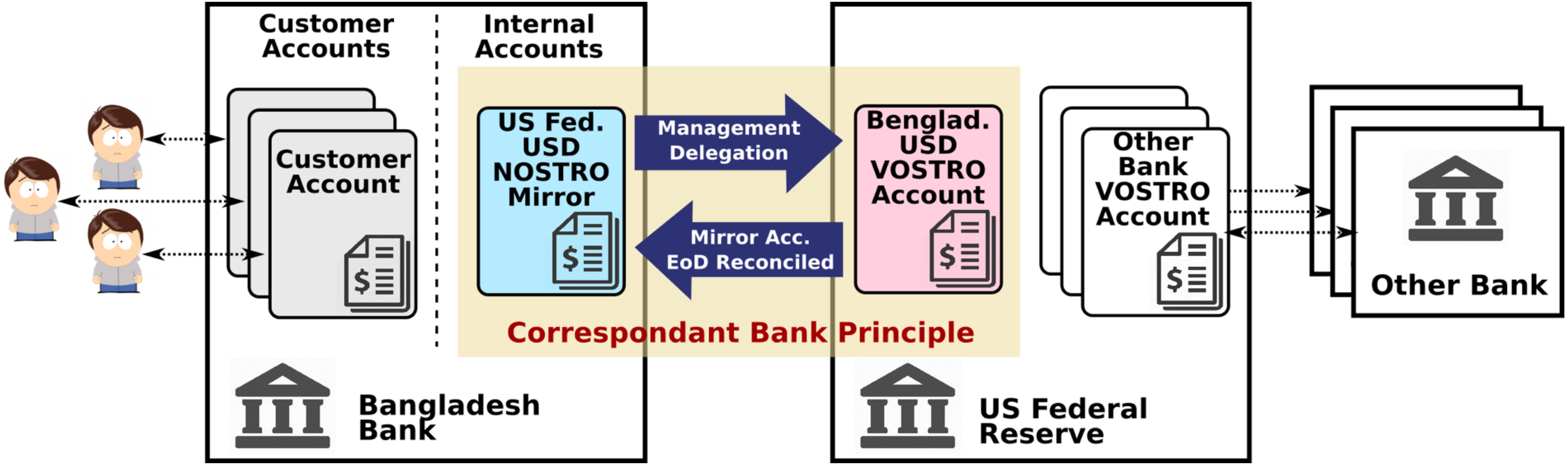
Deciphering the Bangladesh bank heist

by Jerome Kehrli

Posted on Wednesday Nov 15, 2017 at 11:03PM in Banking

The Bangladesh bank heist - or SWIFT attack - is one of the biggest bank robberies ever, and the most impressive cyber-crime in history.

This is the story of a group of less than 20 cyber-criminals, composed by high profile hackers, engineers, financial experts and banking experts who gathered together to hack the worldwide financial system, by attacking an account of the central bank of Bangladesh, a lower middle income nation and one of the world's most densely populated countries, and steal around 81 million US dollars, successfully, after attempting to steal almost a billion US dollars.

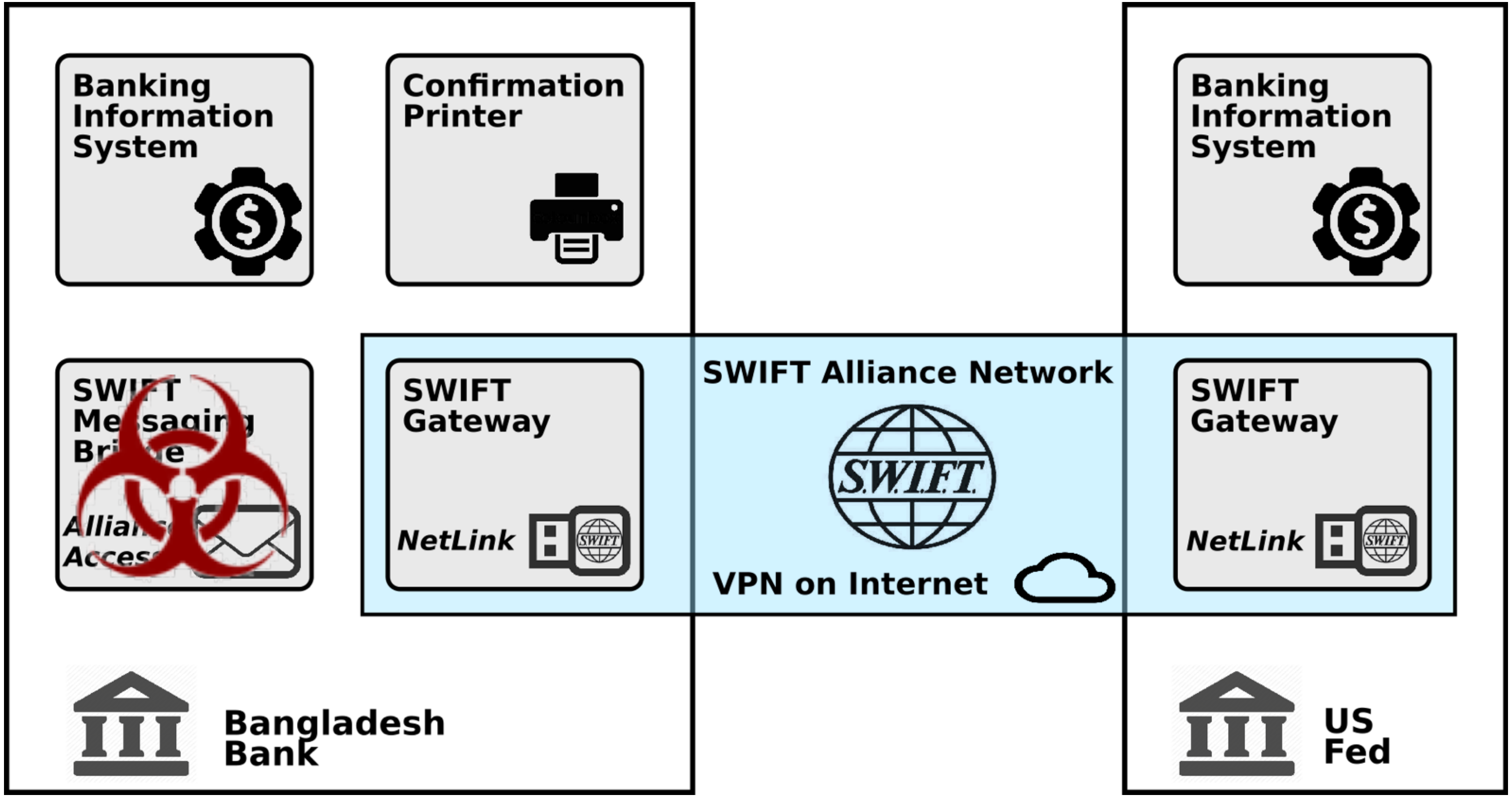

Customer Accounts
Internal Accounts
Customer Account
US Fed. USD NOSTRO Mirror
Management Delegation
Mirror Acc. EoD Reconciled
Benglad. USD VOSTRO Account
Other Bank VOSTRO Account
Other Bank
Correspondant Bank Principle
Bangladesh Bank
US Federal Reserve

Source: https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist

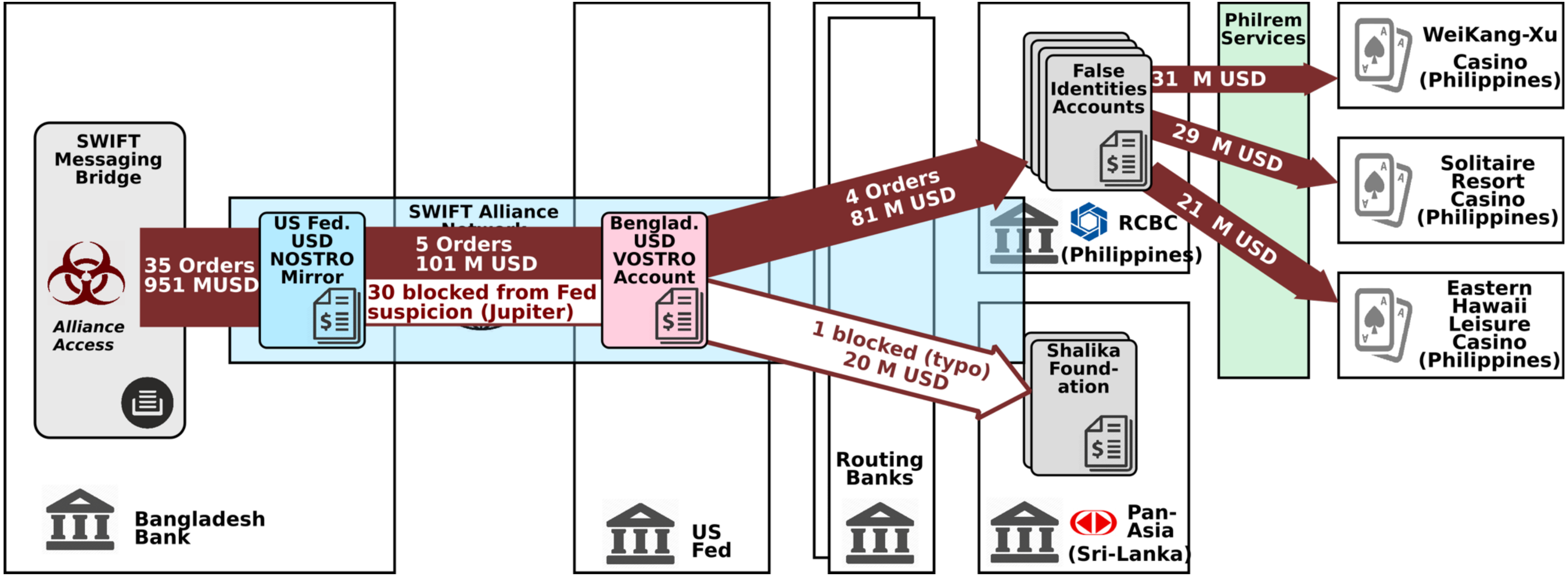
2016
FEBRUARY

$81
MILLION

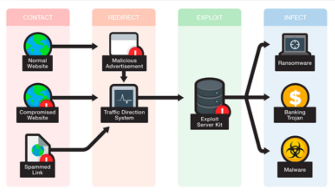
The Bank of Bangladesh



Source: https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist



Source: https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist



May 15 2015

Three dollar bank accounts RCBC were opened with an initial deposit of $500 each. These accounts, which were later found to be fake, remained idle until February 4, 2016.

2015 - Jan 2016

preparation
- Access gaining
- Worm development
- Social Engineering
- etc.

Thu, Feb 4 2016

ackers ordered 5 transfers worth 951 million to be ansferred to CBC Jupiter branch.

The Federal Reserve Bank did not execute 30 of the 35 transfers due to "lack of details."

Fri, Feb 5 2016

After blocking these 30 transactions, the Fed tried to reach the bangladesh bank but **Fri, Feb 5**, is a **banking holiday in bangladesh.** Nobody answered.

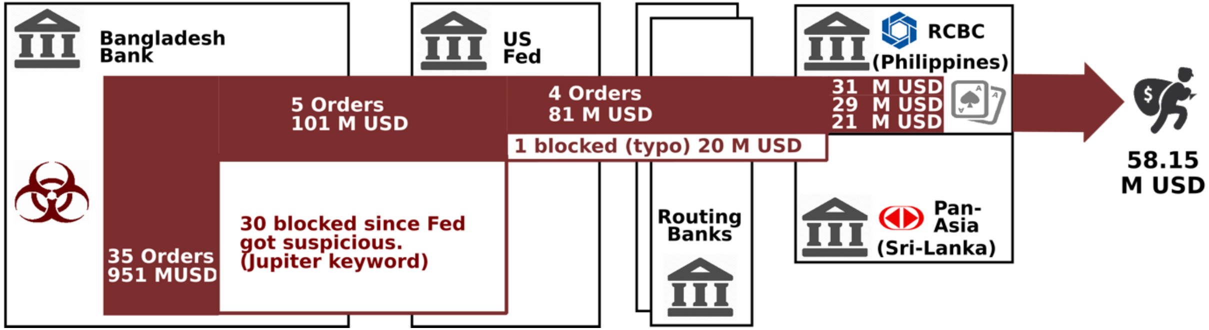
During the course of the Week-End the 4 transactions passed succesfully and the money left the fed to routing banks.

Mon, Feb 8 2016

When the bangladesh bank finally reached the Fed back, it was too late Tracking the orders, the bangladesh bank could trace them to RCBC and send RCBC stop payments orders. But **Mon, Feb 8 is a banking holiday in Philippines** (Chinese New-Year)

Feb 9 2016

Despite the "stop payment" order, RCBC Jupiter branch still allowed withdrawals from the accounts. The stolen funds were transferred to money transfer company Philrem Services Corporation. Philrem converted into pesos the $81 million and delivered the money in cash tranches. From there the money was laundered in Philippine's Casinos (fairly easy at Chinese New-Year)



Bangladesh Bank

US Fed

Routing Banks

RCBC (Philippines)

Pan-Asia (Sri-Lanka)

35 Orders 951 MUSD

5 Orders 101 M USD

30 blocked since Fed got suspicious. (Jupiter keyword)

4 Orders 81 M USD

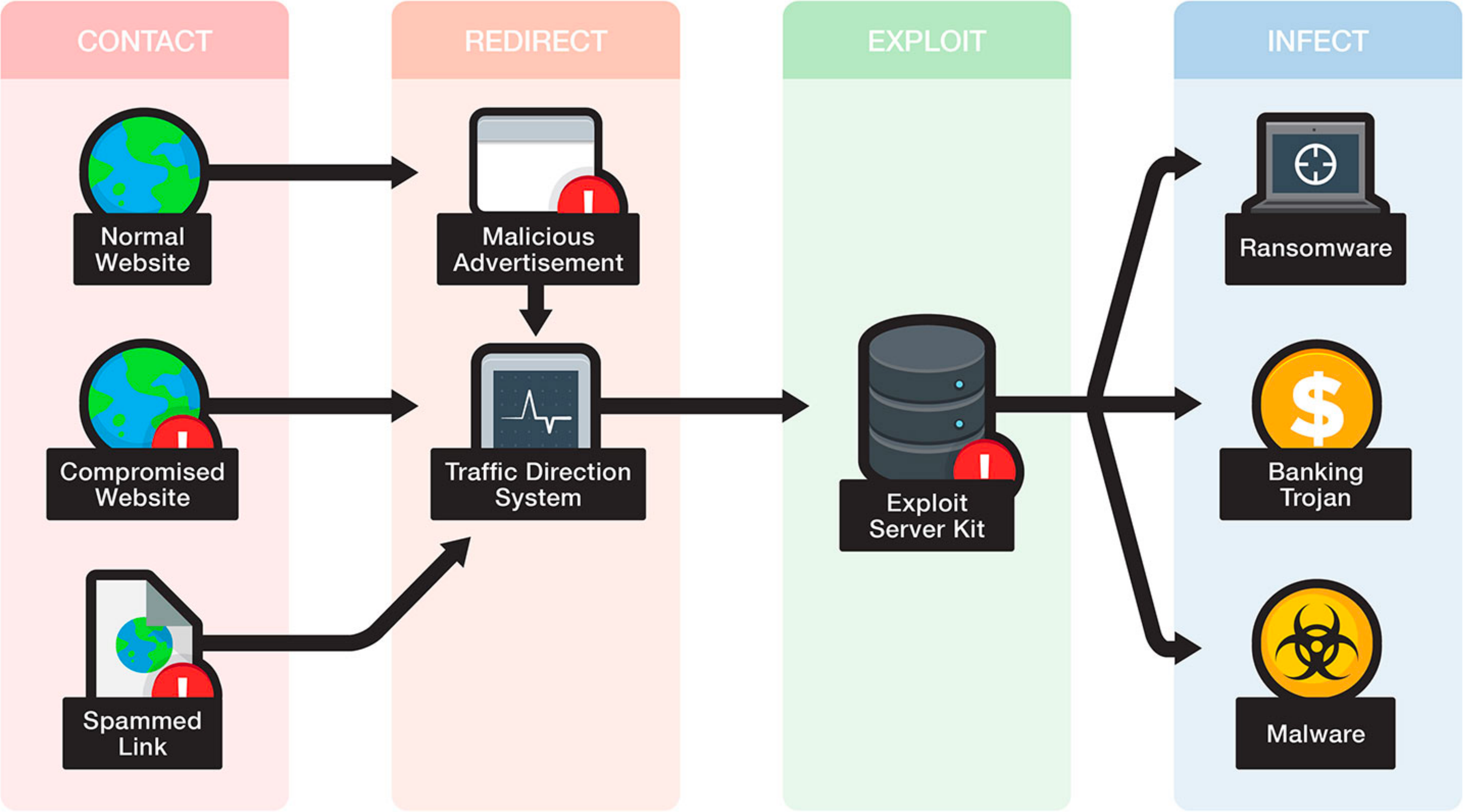
1 blocked (typo) 20 M USD

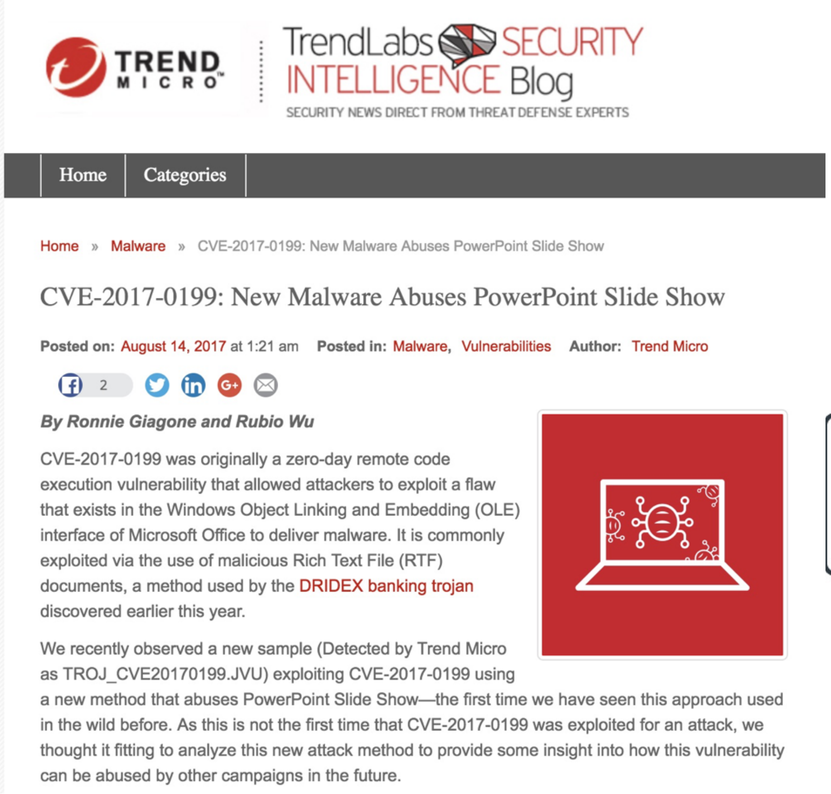
31 M USD
29 M USD
21 M USD

58.15 M USD

Source: https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist

TREND MICRO


CONTACT
REDIRECT
EXPLOIT
INFECT
Normal Website
Malicious Advertisement
Ransomware
Compromised Website
Traffic Direction System
Exploit Server Kit
Banking Trojan
Spammed Link
Malware



TrendLabs SECURITY INTELLIGENCE Blog

SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Home » Malware » CVE-2017-0199: New Malware Abuses PowerPoint Slide Show

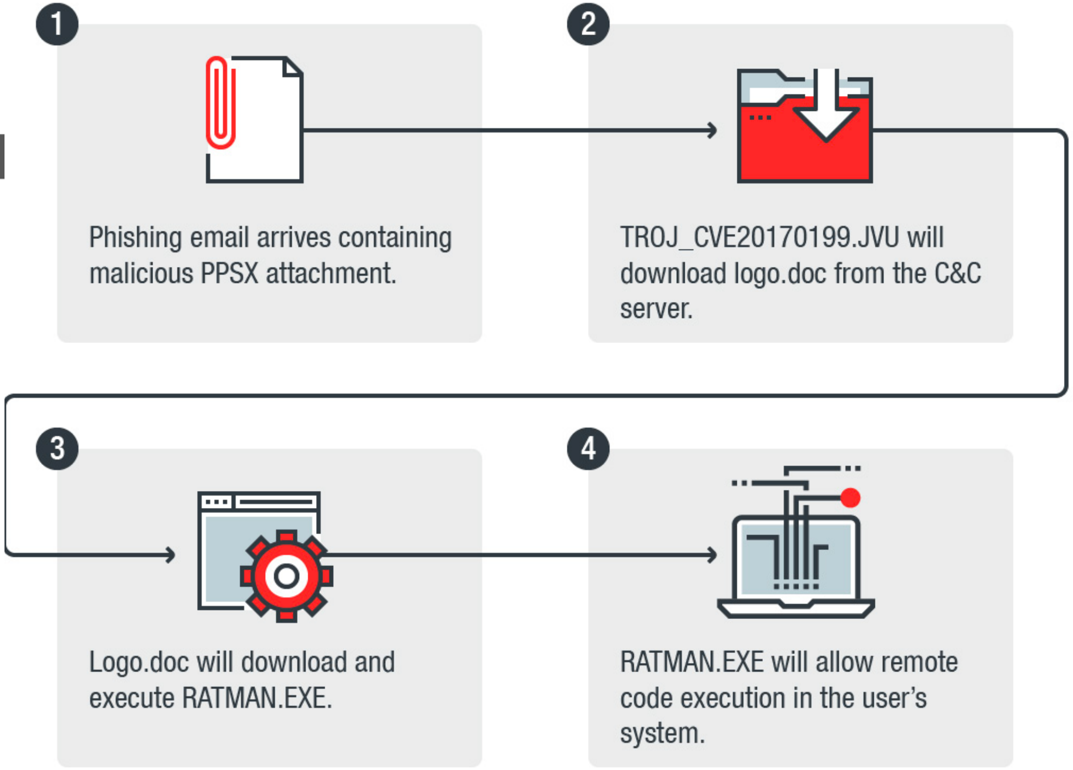
CVE-2017-0199: New Malware Abuses PowerPoint Slide Show

Posted on: August 14, 2017 at 1:21 am **Posted in:** Malware, Vulnerabilities **Author:** Trend Micro

By Ronnie Giagone and Rubio Wu

CVE-2017-0199 was originally a zero-day remote code execution vulnerability that allowed attackers to exploit a flaw that exists in the Windows Object Linking and Embedding (OLE) interface of Microsoft Office to deliver malware. It is commonly exploited via the use of malicious Rich Text File (RTF) documents, a method used by the DRIDEX banking trojan discovered earlier this year.

We recently observed a new sample (Detected by Trend Micro as TROJ_CVE20170199.JVU) exploiting CVE-2017-0199 using a new method that abuses PowerPoint Slide Show—the first time we have seen this approach used in the wild before. As this is not the first time that CVE-2017-0199 was exploited for an attack, we thought it fitting to analyze this new attack method to provide some insight into how this vulnerability can be abused by other campaigns in the future.



1. Phishing email arrives containing malicious PPSX attachment.
2. TROJ_CVE20170199.JVU will download logo.doc from the C&C server.
3. Logo.doc will download and execute RATMAN.EXE.
4. RATMAN.EXE will allow remote code execution in the user's system.

2018
MAY

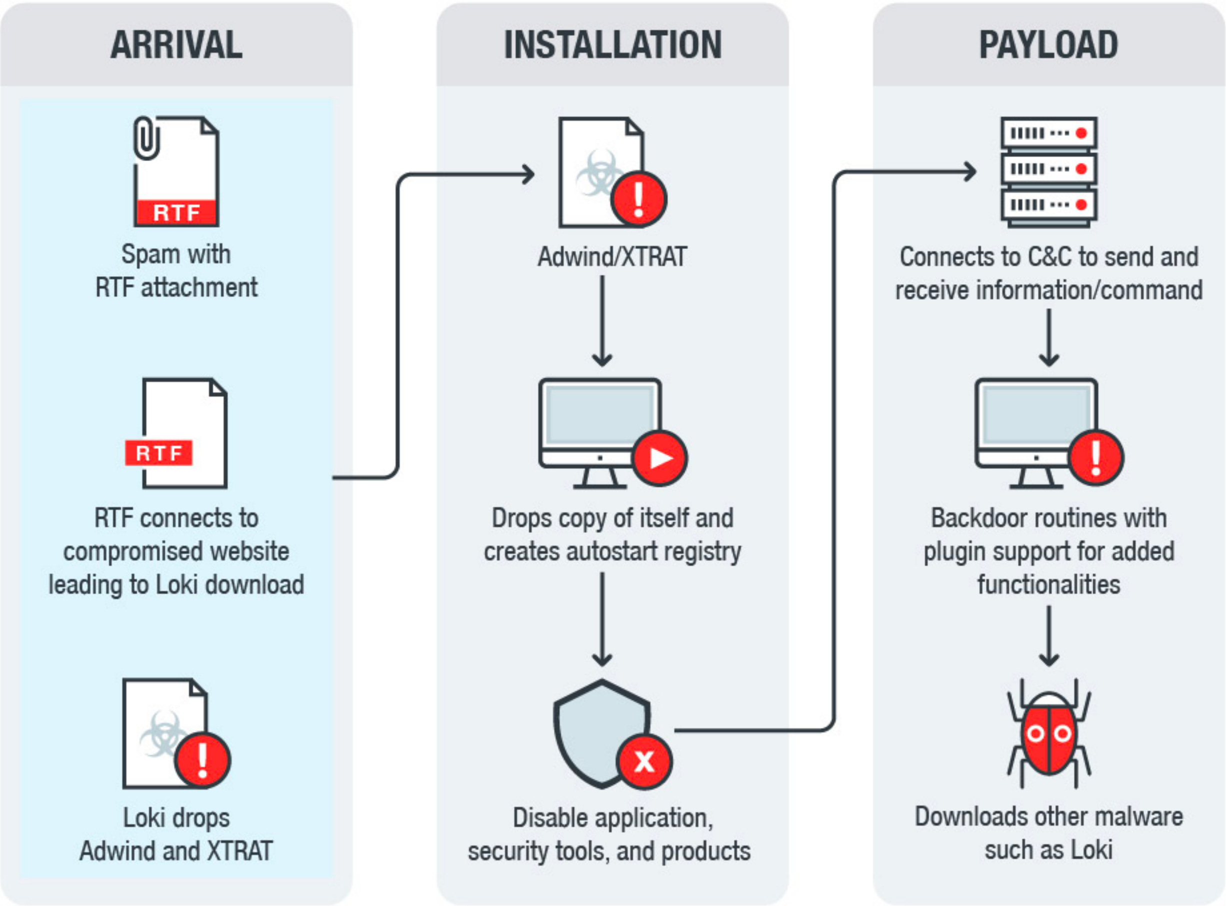
$10
MILLION

KILLMBR

DRIDEX
FALLCHILL

2018
JANUARY

$110*
MILLION



ARRIVAL

Spam with RTF attachment

RTF connects to compromised website leading to Loki download

Loki drops Adwind and XTRAT

INSTALLATION

Adwind/XTRAT

Drops copy of itself and creates autostart registry

Disable application, security tools, and products

PAYLOAD

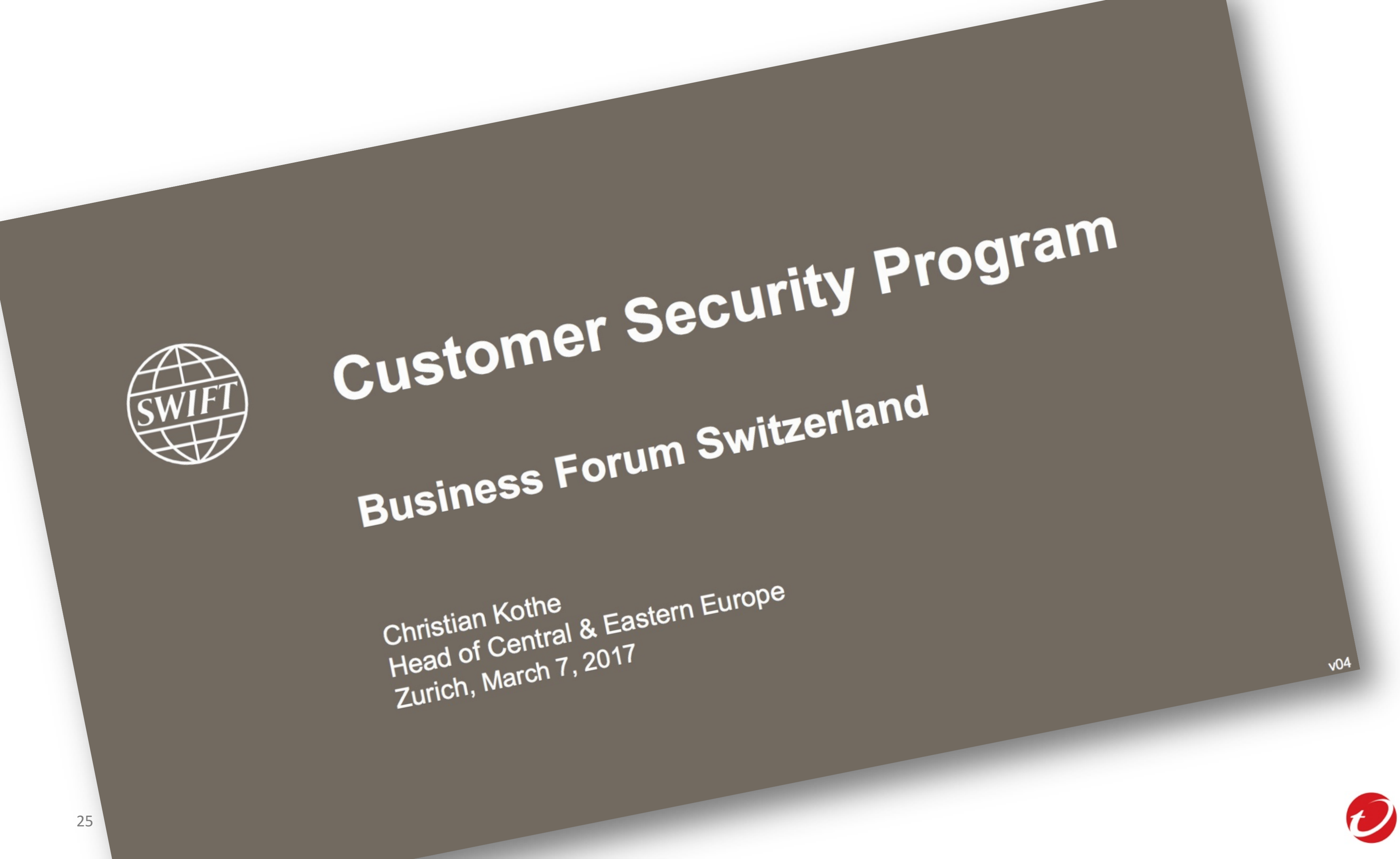
Connects to C&C to send and receive information/command

Backdoor routines with plugin support for added functionalities

Downloads other malware such as Loki

- Information theft
- File and registry management
- Remote desktop
- Remote shell
- Process management
- Uploading, downloading, and executing files
- Screen capture desktop
- Recording via webcam or microphone
- Upload and download files
- Registry manipulation (read, write and manipulate)
- Process manipulation (execute and terminate)
- Service manipulation (stop, start, create and modify)
- Perform remote shell and control victim’s system

SWIFT CSP
(Customer Security Program)



Customer Security Program

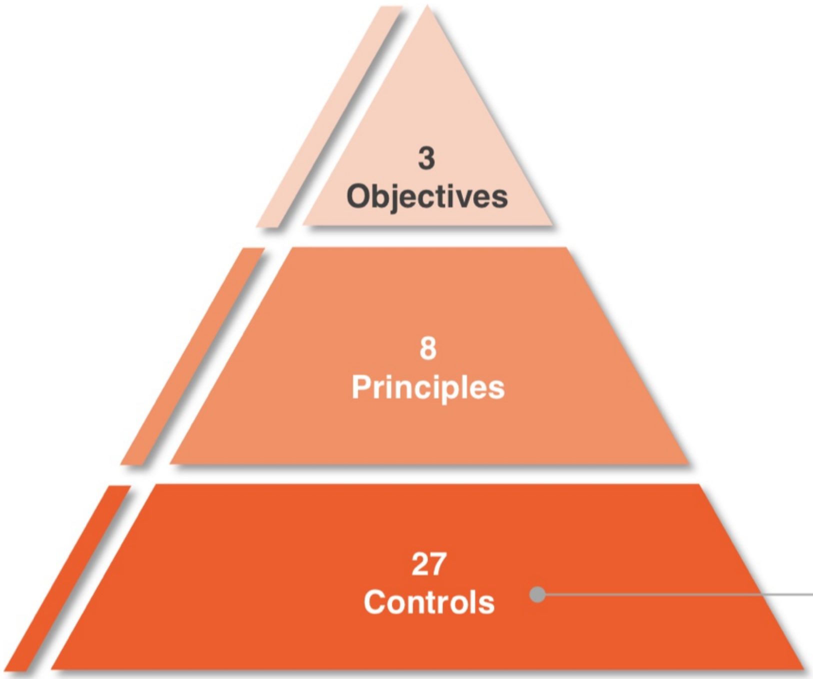
Business Forum Switzerland

Christian Kothe
Head of Central & Eastern Europe
Zurich, March 7, 2017

v04

CSP | You > Security Guidelines and Assurance

Security Controls



CSP Security Controls Framework

Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

- Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure
- Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002
- 16 controls are mandatory and 11 are advisory

How Trend Micro can help?

Mandatory CSP Security Controls – 1.1

1.1 SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.
How Trend Micro help to achieve compliance	Deep Security Firewall for Microsegmentation

Mandatory CSP Security Controls – 2.2

2.2 Security Updates	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.
How Trend Micro help to achieve compliance	Deep Security Virtual Patching for Vulnerability Inventory and Automatic Remediation without Impacting Business Continuity

Mandatory CSP Security Controls – 2.3

2.3 System Hardening	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.
How Trend Micro help to achieve compliance	Deep Security Application Control for White Listing systems and prevent Uwanted Modifications

Mandatory CSP Security Controls – 6.1

6.1 Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.
How Trend Micro help to achieve compliance	Deep Security Anti-Malware to detect emerging threats using Predictive Machine Learning

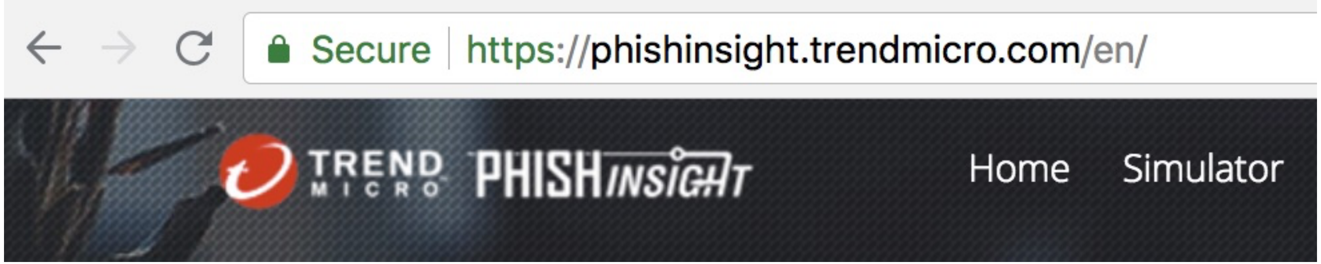
Mandatory CSP Security Controls – 6.2

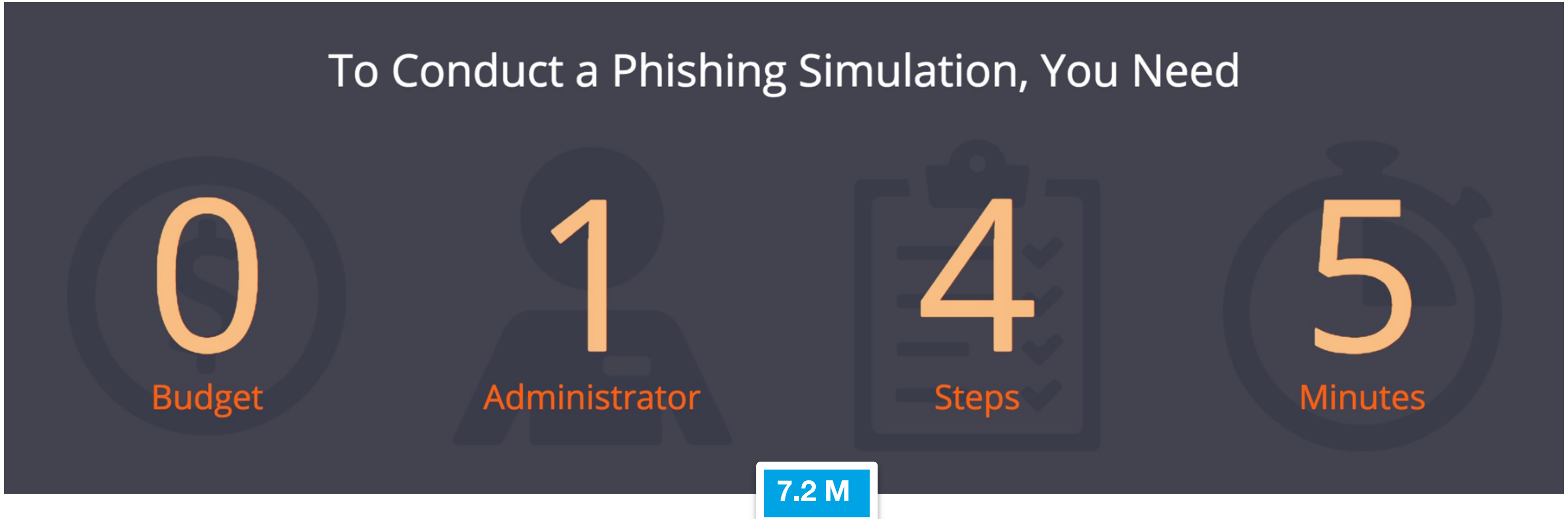
6.2 Software Integrity	Ensure the software integrity of the SWIFT-related applications.
How Trend Micro help to achieve compliance	Deep Security File Integrity Monitoring to detect unauthorized modifications to the system

Mandatory CSP Security Controls – 7.2

7.2 Security Training and Awareness	Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.
How Trend Micro help to achieve compliance	Trend Micro Phish Insight is an awareness service to help your organization resist online scams. Phish Insight lets you test and educate your employees on how to spot phishing and avoid attacks.

SWIFT CSP




To Conduct a Phishing Simulation, You Need

0 Budget

1 Administrator

4 Steps

5 Minutes

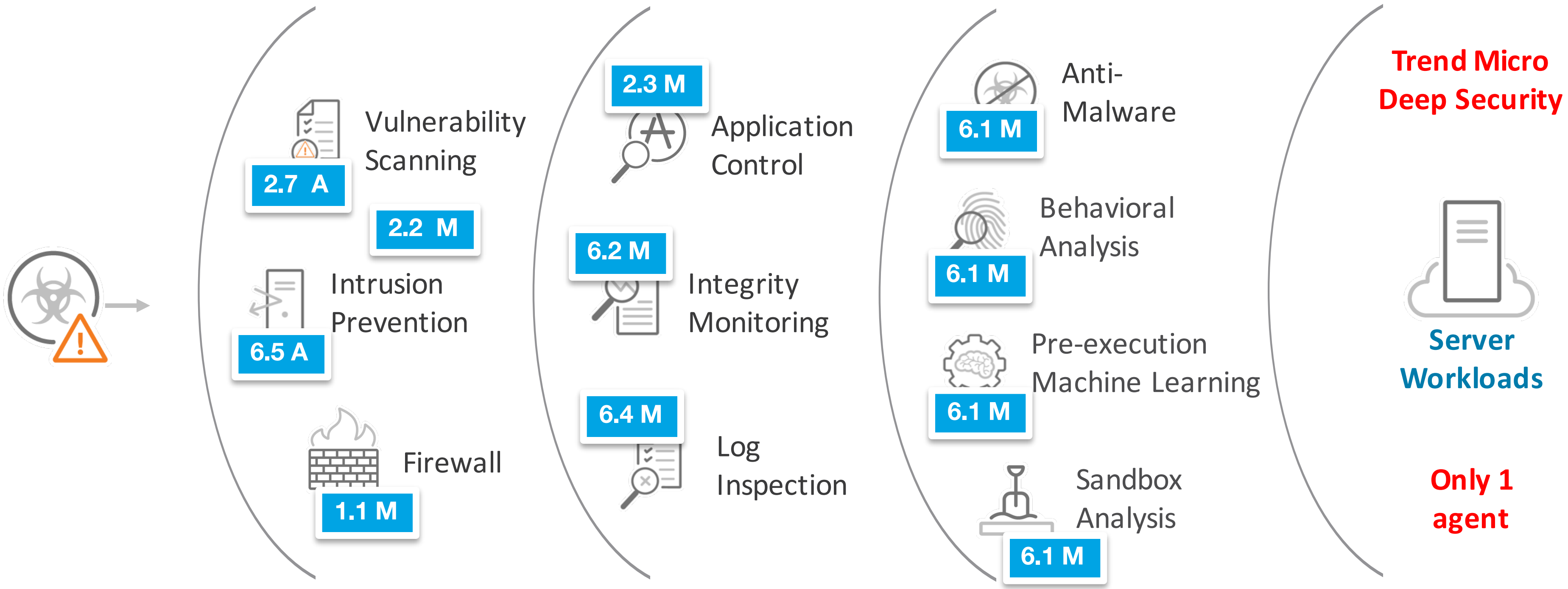
7.2 M

SWIFT CSP

Network Security

System Security

Malware Prevention



Vulnerability Scanning 2.7 A 2.2 M

Intrusion Prevention 6.5 A

Firewall 1.1 M

Application Control 2.3 M

Integrity Monitoring 6.2 M

Log Inspection 6.4 M

Anti-Malware 6.1 M

Behavioral Analysis 6.1 M

Pre-execution Machine Learning 6.1 M

Sandbox Analysis 6.1 M

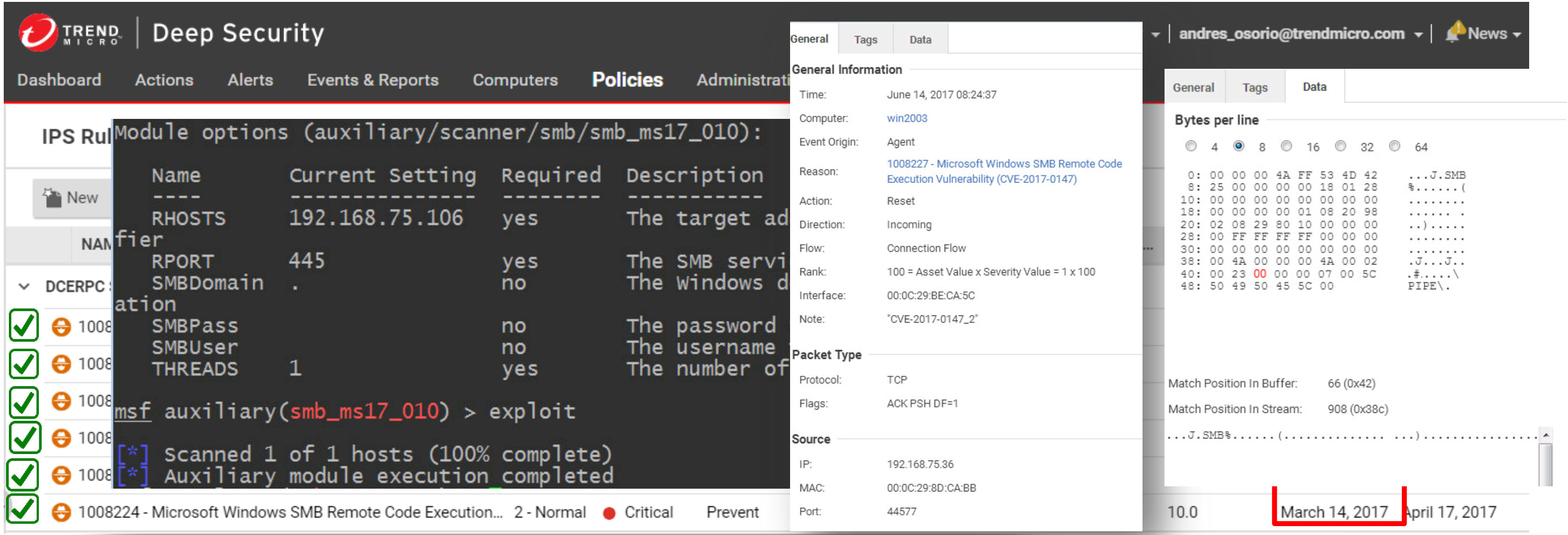
Trend Micro Deep Security

Server Workloads

Only 1 agent

vmware aws VMware Cloud on AWS AWS GovCloud (US) Google Cloud Platform Microsoft Azure docker TREND MICRO

Ciclo de Parches Vuln: Microsoft MS17-010



```
Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   RHOSTS       192.168.75.106   yes       The target ad
fier
   RPORT        445              yes       The SMB servi
   SMBDomain    .                no        The Windows d
ation
   SMBPass                       no        The password
   SMBUser                       no        The username
   THREADS      1                yes       The number of

msf auxiliary(smb_ms17_010) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

General | Tags | Data

General Information

Time: June 14, 2017 08:24:37
Computer: win2003
Event Origin: Agent
Reason: 1008227 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-0147)
Action: Reset
Direction: Incoming
Flow: Connection Flow
Rank: 100 = Asset Value x Severity Value = 1 x 100
Interface: 00:0C:29:BE:CA:5C
Note: "CVE-2017-0147_2"

Packet Type

Protocol: TCP
Flags: ACK PSH DF=1

Source

IP: 192.168.75.36
MAC: 00:0C:29:8D:CA:BB
Port: 44577

General | Tags | Data

Bytes per line

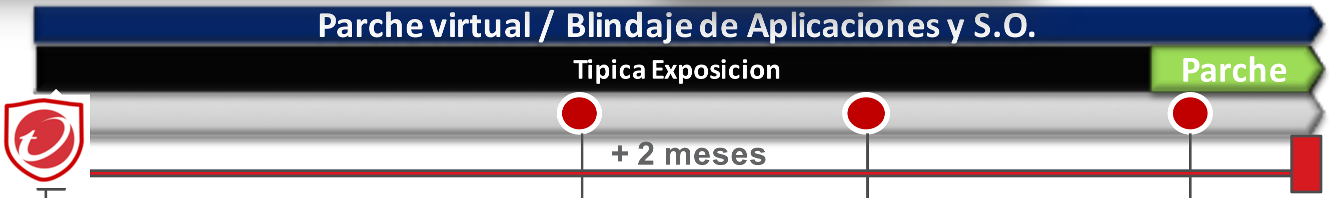
○ 4 ● 8 ○ 16 ○ 32 ○ 64

```
 0: 00 00 00 4A FF 53 4D 42     ...J.SMB
 8: 25 00 00 00 00 18 01 28     %......(
10: 00 00 00 00 00 00 00 00     ........
18: 00 00 00 00 01 08 20 98     ...... .
20: 02 08 29 80 10 00 00 00     ..).....
28: 00 FF FF FF FF 00 00 00     ........
30: 00 00 00 00 00 00 00 00     ........
38: 00 4A 00 00 00 4A 00 02     .J...J..
40: 00 23 00 00 00 07 00 5C     .#.....\
48: 50 49 50 45 5C 00           PIPE\.
```

Match Position In Buffer: 66 (0x42)
Match Position In Stream: 908 (0x38c)

```
...J.SMB%......(.............. ...)...............
```

✓	1008224 - Microsoft Windows SMB Remote Code Execution...	2 - Normal	● Critical	Prevent	10.0	March 14, 2017	April 17, 2017



Parche virtual / Blindaje de Aplicaciones y S.O.

Tipica Exposicion

Parche

+ 2 meses

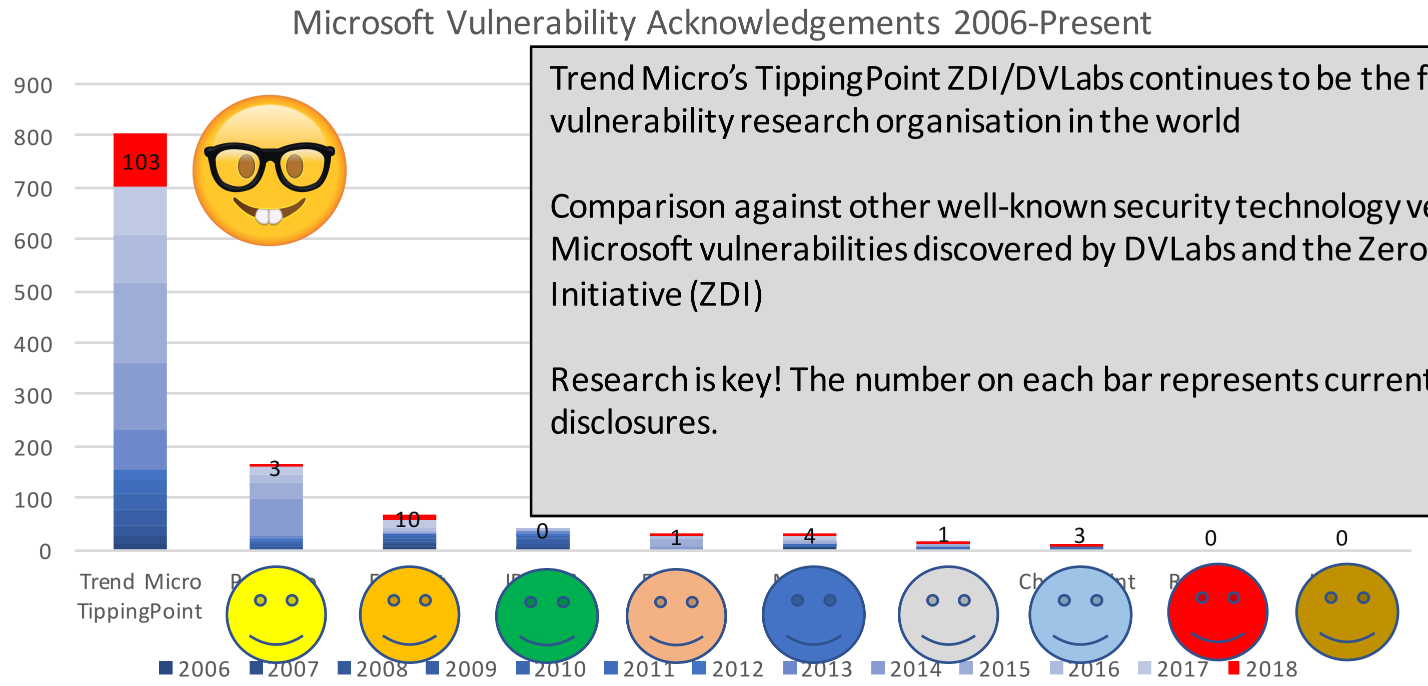
14 de Marzo
Parche Disponible

17 de Abril
Exploit Publico

Pruebas de
Implementacion

12 de Mayo
WannaCry
Instalación parche

Microsoft Vulnerability Acknowledgments Since 2006*



Trend Micro’s TippingPoint ZDI/DVLabs continues to be the foremost vulnerability research organisation in the world

Comparison against other well-known security technology vendors of Microsoft vulnerabilities discovered by DVLabs and the Zero-Day Initiative (ZDI)

Research is key! The number on each bar represents current year disclosures.

*From publicly available data at https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments as of October 1, 2018

Muchas Gracias !