# Stay One Step Ahead of Hackers With Visa Threat Intelligence

23 March 2016

Glen Jones, Sr. Director, VISA, Cyber Intelligence and Investigations
Kevin Thompson, Threat Analyst, FireEye

# Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

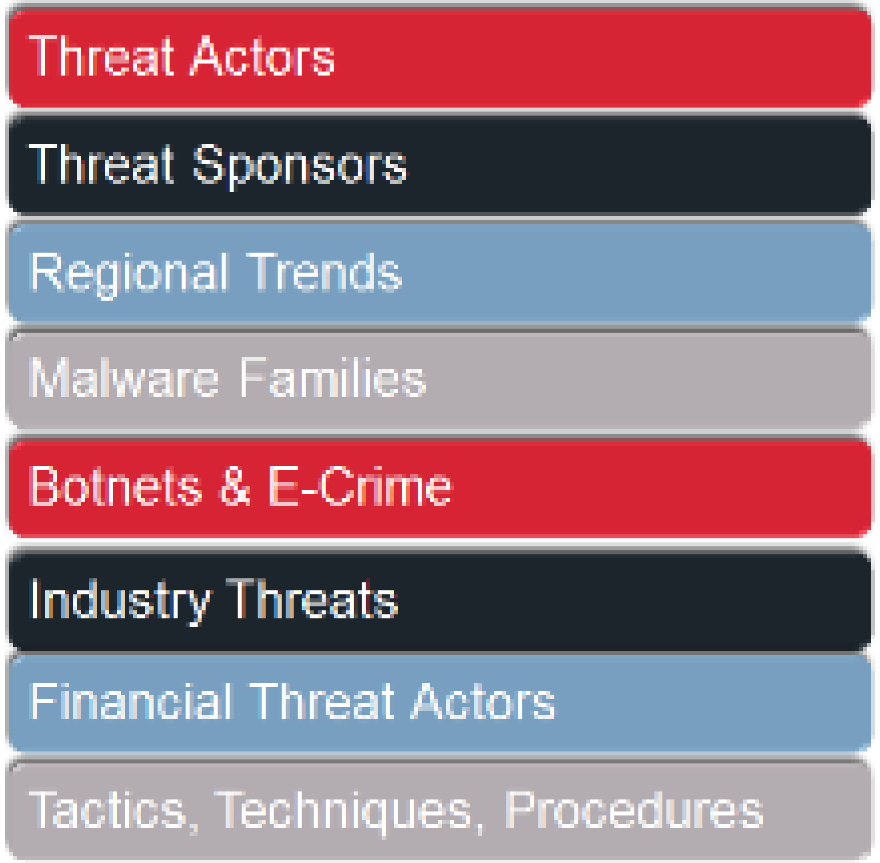
# Agenda

- Cyber Intelligence Trends
- Payment System Threat Intelligence
- Upcoming Events and Resources
- Q&A

# Cyber Intelligence Trends
# Making Intel Actionable

Kevin Thompson, Threat Analyst, FireEye

# What Is Threat Intelligence?



- Threat Actors
- Threat Sponsors
- Regional Trends
- Malware Families
- Botnets & E-Crime
- Industry Threats
- Financial Threat Actors
- Tactics, Techniques, Procedures

# Data vs. Threat Intelligence

## Commoditized Feeds:  Raw Data

- **Misses the threats that matter.** Commoditized threat intelligence is too broad and out-of-date to protect against surgical attacks.

- **Becomes part of the problem.** Typically leads to voluminous alerts that require additional personnel to identify the true threats from within the noise.

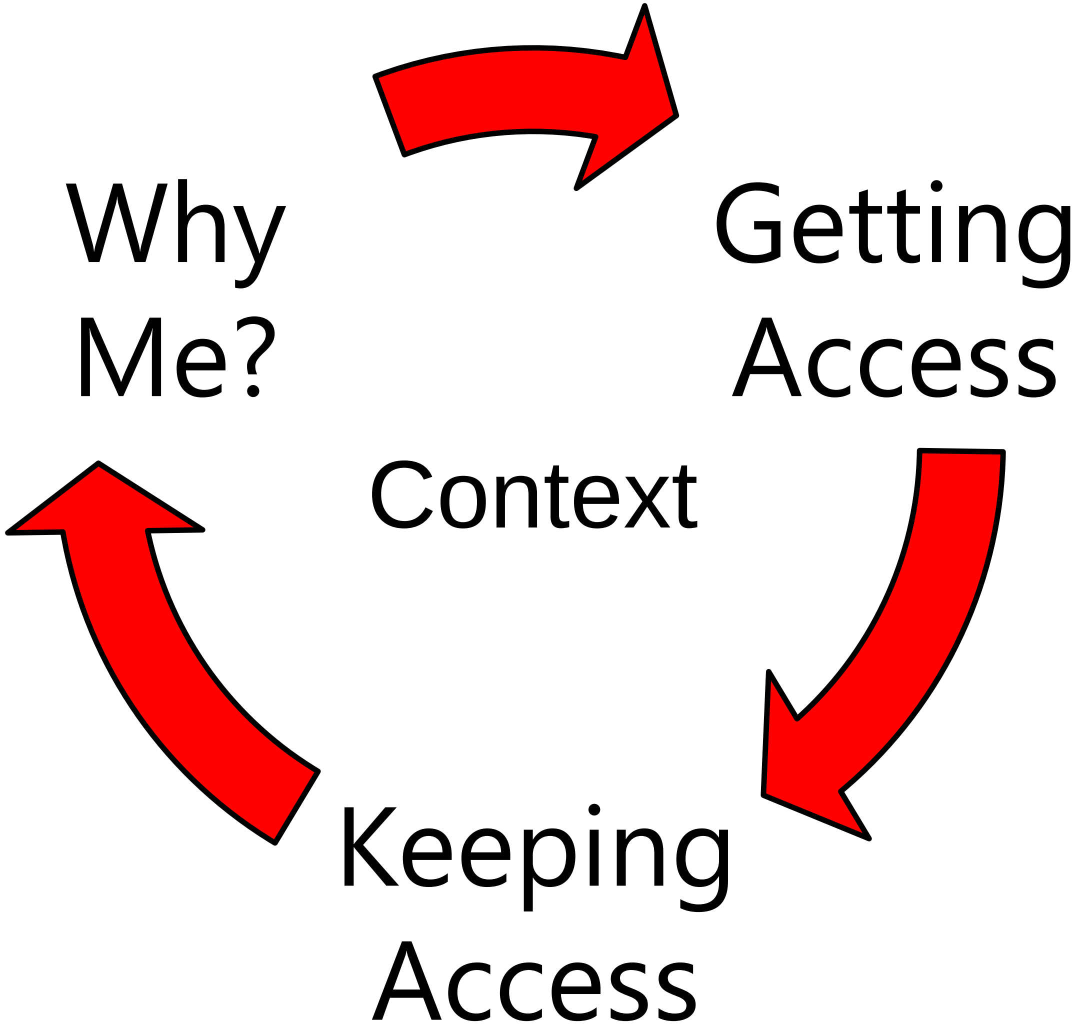
≠

## Threat Intelligence

- **Threat intelligence curates data sources to create high-fidelity, precise alerts** to surgically identify targeted attacks

- **True threat intelligence "right-sizes" the problem** with the context and attribution required to prioritize and build response to the threats that represent the greatest risk

# Internal Intel



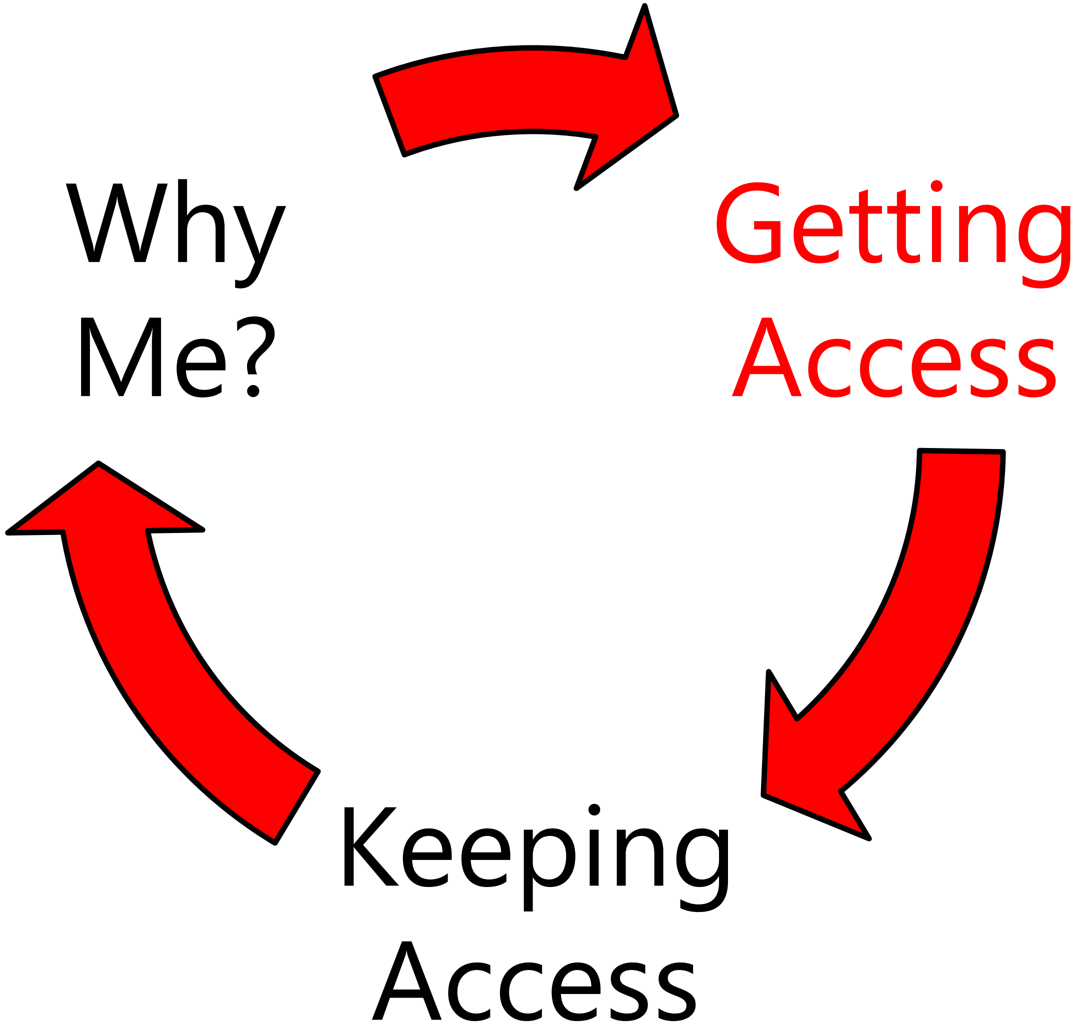
Why Me?

Getting Access

Context

Keeping Access

# Internal Intel



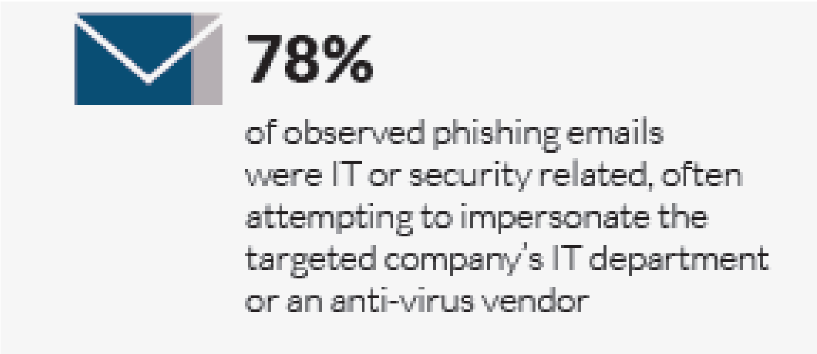
Why Me?

Getting Access

Keeping Access

# Email vs. Web

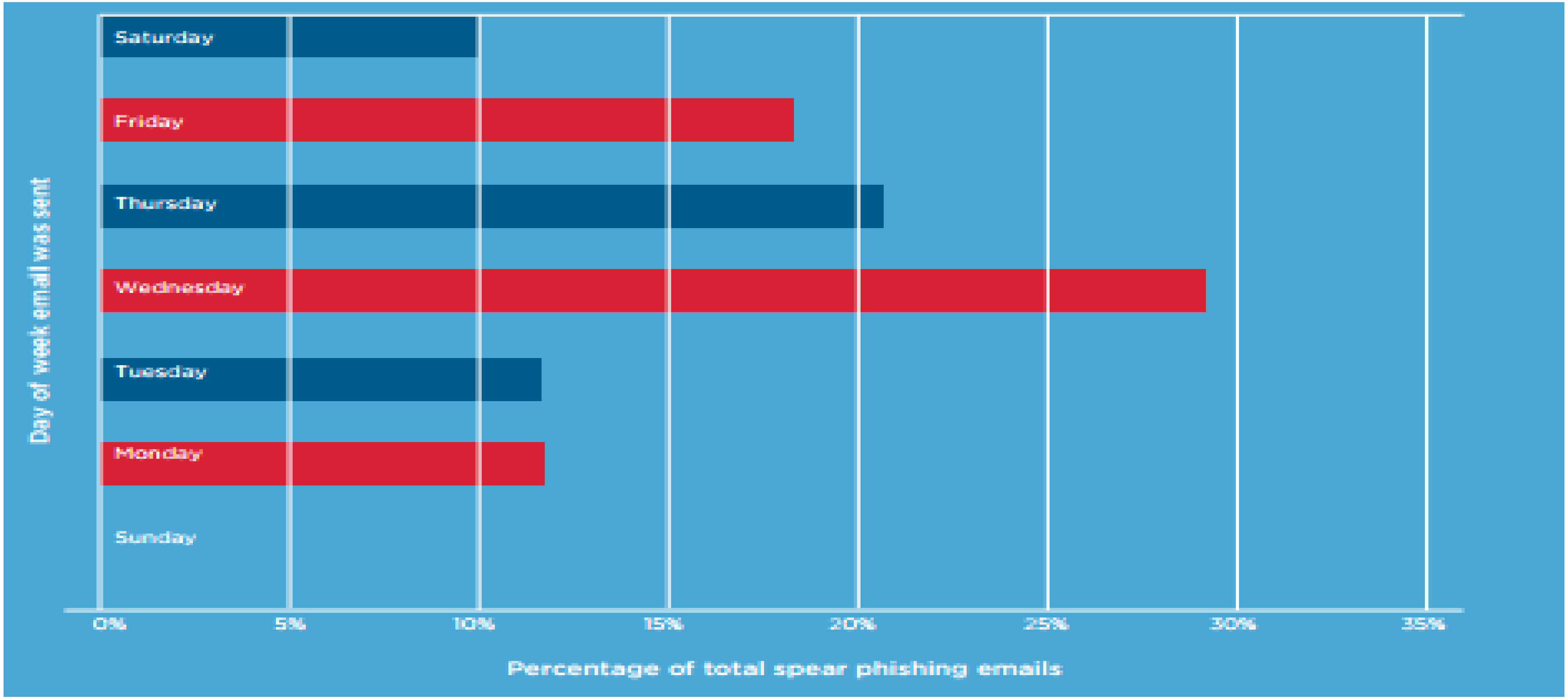
- 10 0-days discovered by the FireEye Labs:
  - 7 of them used via drive by download
  - 3 of them used email
- Macros are back
- Retail: ~97% had an email component
- Healthcare: ~97% had an email component
- Finance: ~98% had an email component



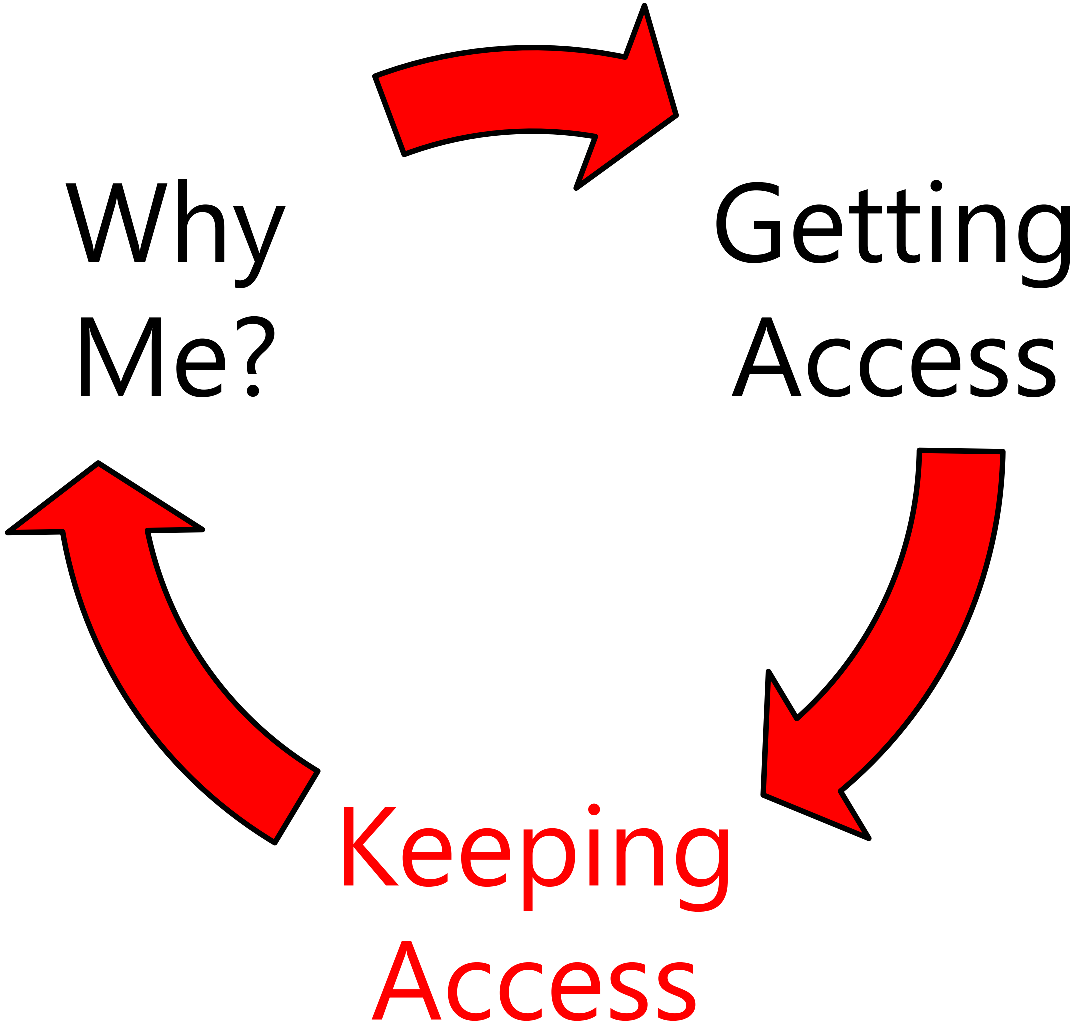
**78%**

of observed phishing emails were IT or security related, often attempting to impersonate the targeted company's IT department or an anti-virus vendor

# Email vs. Web


Saturday
Friday
Thursday
Wednesday
Tuesday
Monday
Sunday
Day of week email was sent
0%
5%
10%
15%
20%
25%
30%
35%
Percentage of total spear phishing emails

# Internal Intel

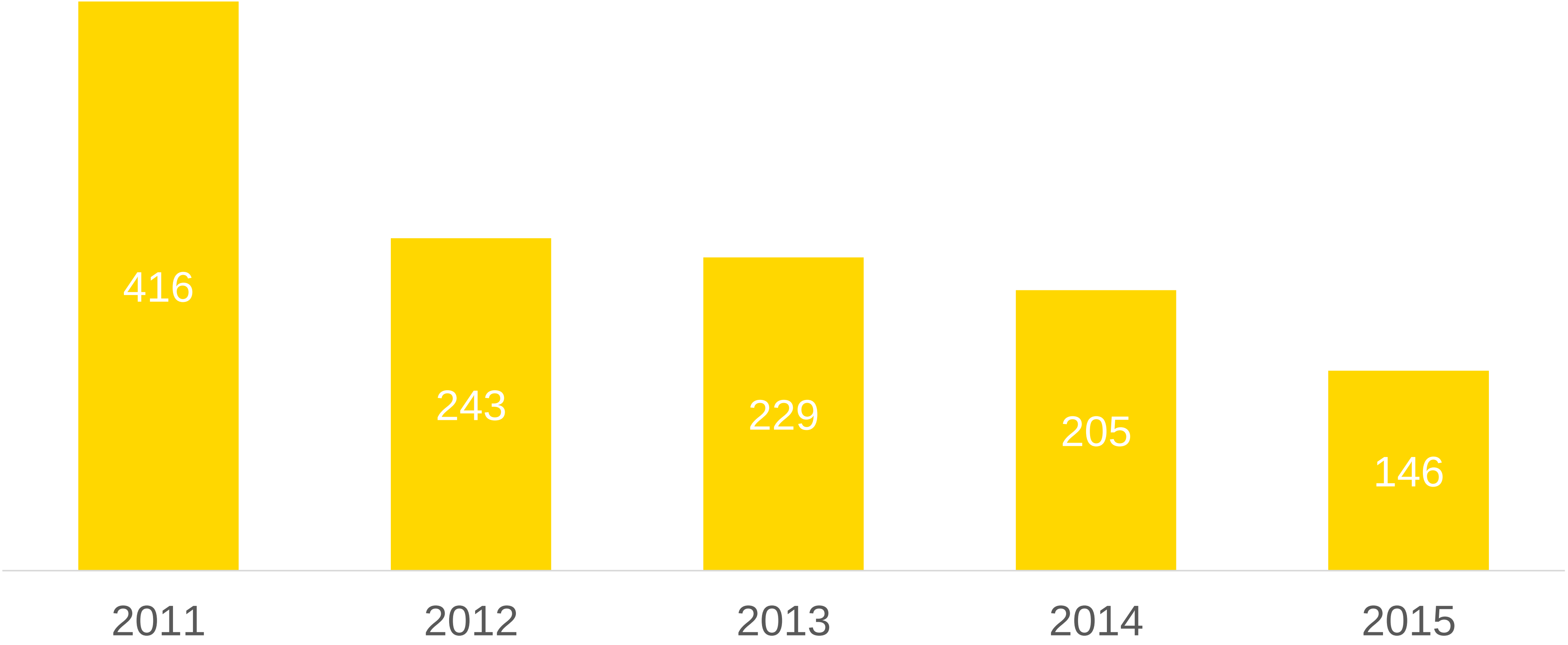


Why Me?

Getting Access

Keeping Access

# Median Days Before Discovery



# How Compromises Are Detected

**47%** Internal

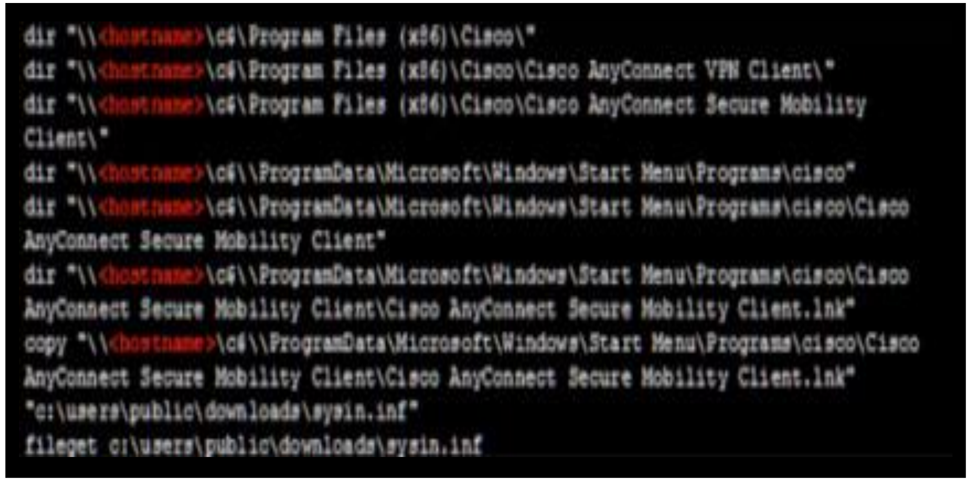
**53%** External

# Lateral Movement ≠ Malware

***Of all of the compromised machines Mandiant identified in the last two years, only ~50% had malware on them.***

# New persistence mechanisms

- Hijacking the VPN
  - Attackers targeting VPN immediately after compromise and abandon traditional malware
  - Theft of client-side certificates
  - Exploiting single-factor authentication

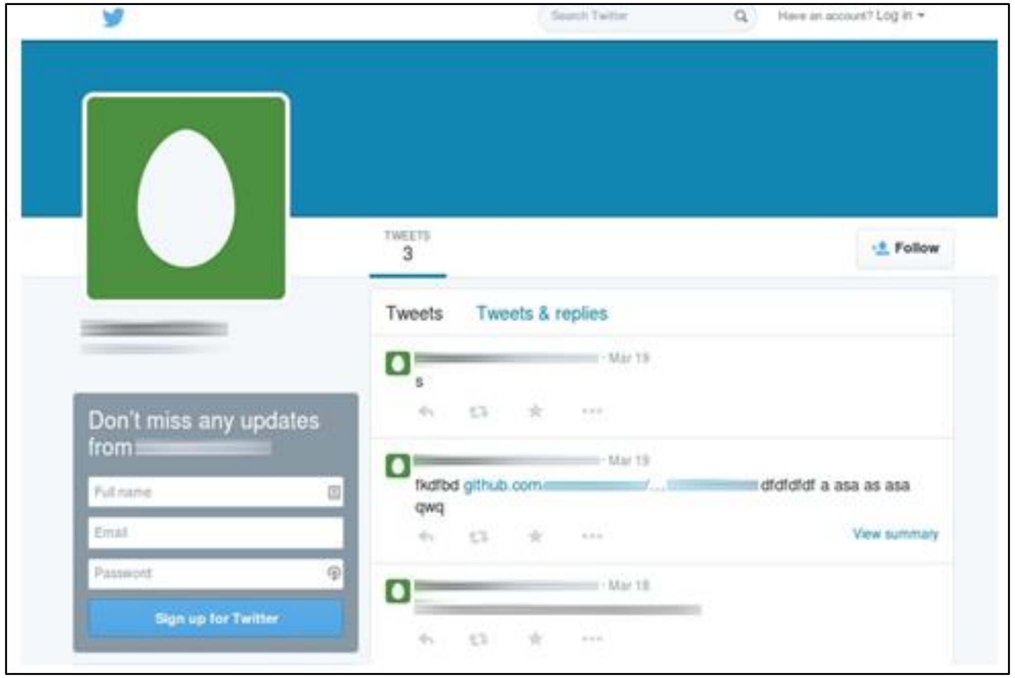


```
dir "\\<hostname>\c$\Program Files (x86)\Cisco\"
dir "\\<hostname>\c$\Program Files (x86)\Cisco\Cisco AnyConnect VPN Client\"
dir "\\<hostname>\c$\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility
Client\"
dir "\\<hostname>\c$\\ProgramData\Microsoft\Windows\Start Menu\Programs\cisco"
dir "\\<hostname>\c$\\ProgramData\Microsoft\Windows\Start Menu\Programs\cisco\Cisco
AnyConnect Secure Mobility Client"
dir "\\<hostname>\c$\\ProgramData\Microsoft\Windows\Start Menu\Programs\cisco\Cisco
AnyConnect Secure Mobility Client\Cisco AnyConnect Secure Mobility Client.lnk"
copy "\\<hostname>\c$\\ProgramData\Microsoft\Windows\Start Menu\Programs\cisco\Cisco
AnyConnect Secure Mobility Client\Cisco AnyConnect Secure Mobility Client.lnk"
"c:\users\public\downloads\sysin.inf"
fileget c:\users\public\downloads\sysin.inf
```

# Attackers in the cloud

## Attackers use Twitter to send instructions to their malicious tools

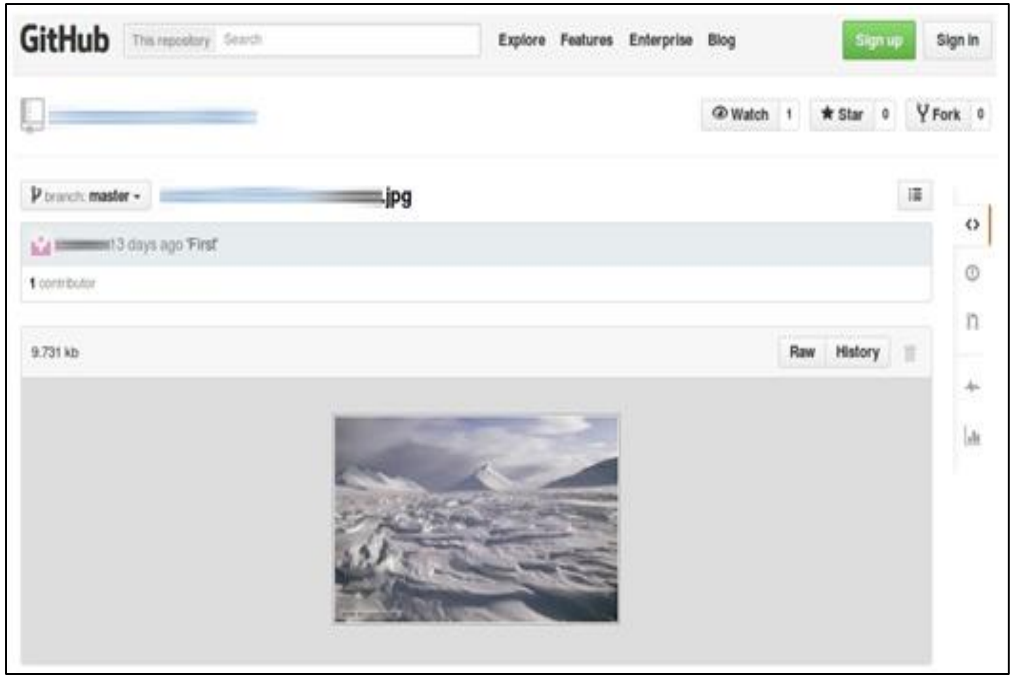
- Twitter accounts include encoded instructions on where to go next
- Network monitoring shows an end user visiting a twitter account, NOT malware receiving instructions



[redacted] · Mar 19
s

[redacted] · Mar 19
fkdfbd github.com[redacted]/…[redacted]dfdfdfdf a asa as asa qwq

[redacted] · Mar 18
[redacted]



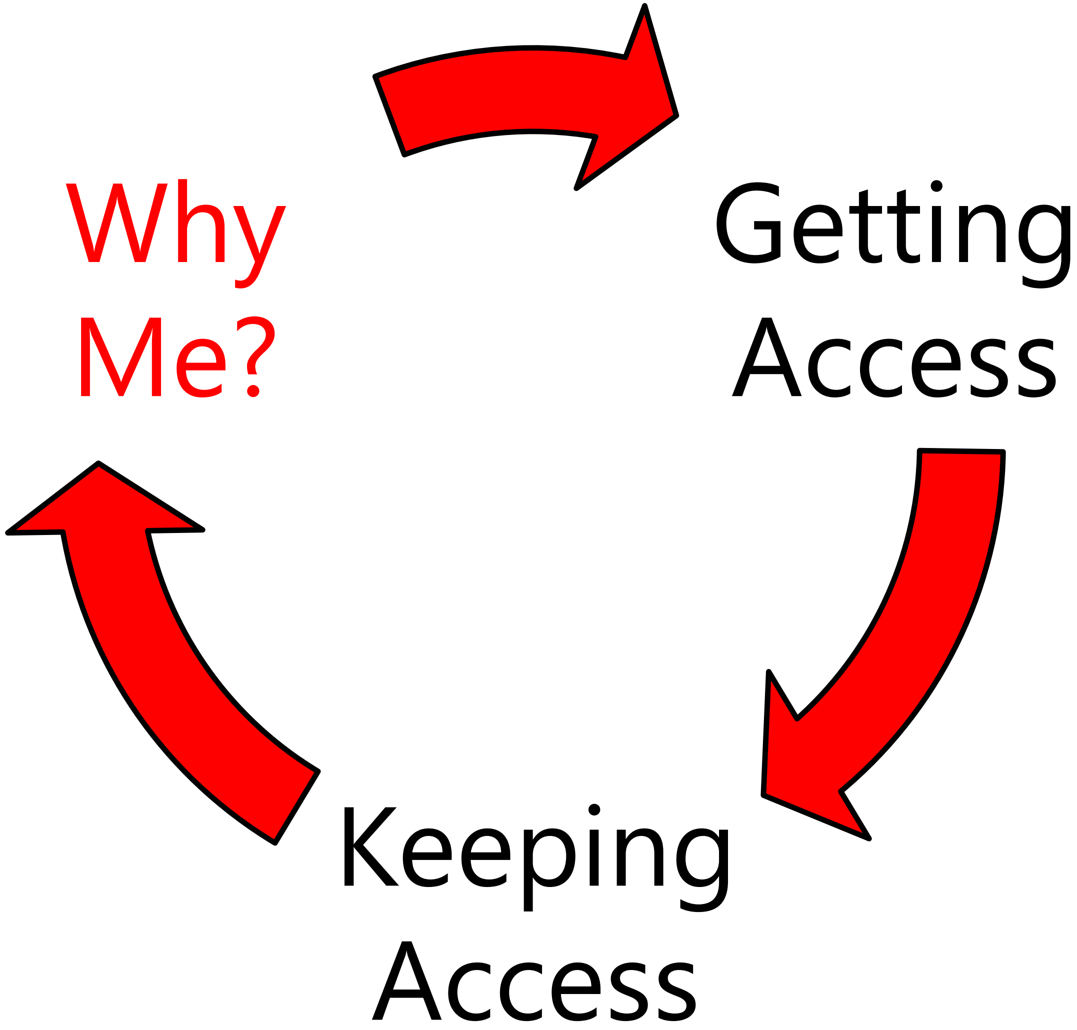
[redacted].jpg

[redacted]13 days ago 'First'

1 contributor

9.731 kb

# Internal Intel



Why Me?

Getting Access

Keeping Access

# Isn't all cyber crime stealing CC #'s?

VISA / FireEye

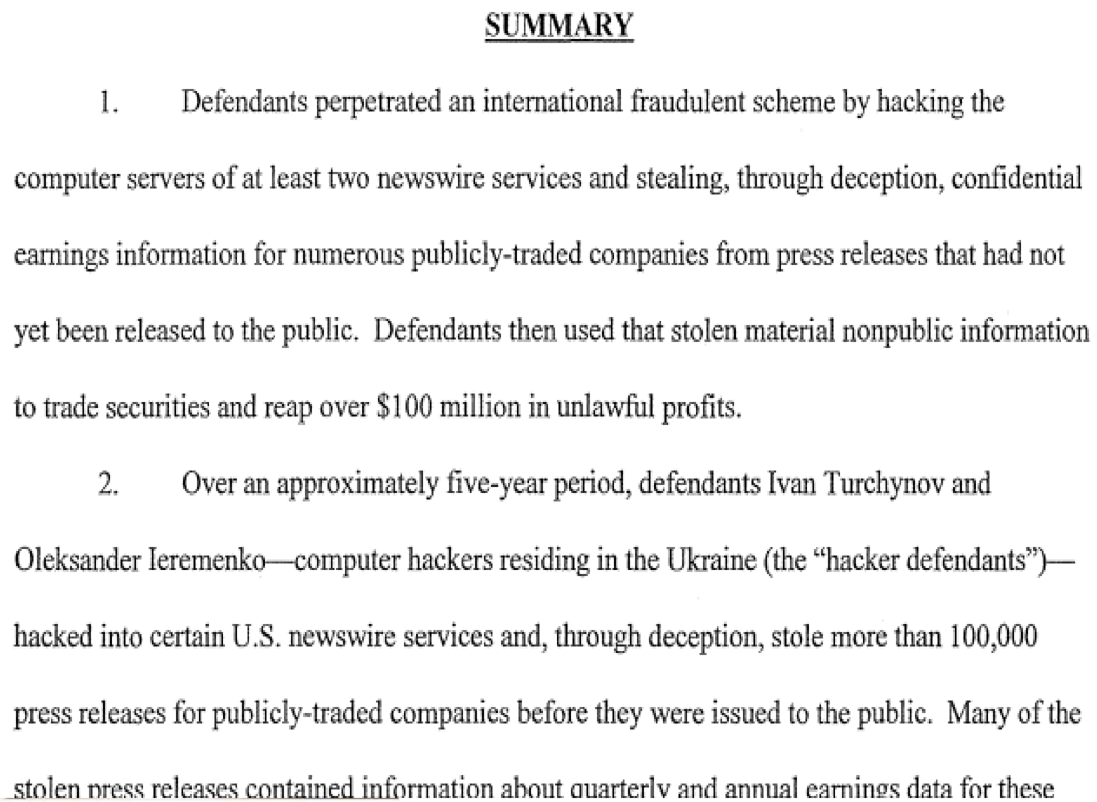
## SEC takes $30m pound of flesh in newswire-hacking scandal

Biz will forfeit its ill-gotten gains frc

HESFARMER 28.13 16500 WESTFIELD 14.07 22100 WOOLWORTHS 11.09 17200
5:24PM
MELBOURNE
3283.0 +16.8
4:2PM
TOKYO

14 Sep 2015 at 20:20, Shaun Nichols

72 7 23



SUMMARY

1. Defendants perpetrated an international fraudulent scheme by hacking the computer servers of at least two newswire services and stealing, through deception, confidential earnings information for numerous publicly-traded companies from press releases that had not yet been released to the public. Defendants then used that stolen material nonpublic information to trade securities and reap over $100 million in unlawful profits.

2. Over an approximately five-year period, defendants Ivan Turchynov and Oleksander Ieremenko—computer hackers residing in the Ukraine (the "hacker defendants")—hacked into certain U.S. newswire services and, through deception, stole more than 100,000 press releases for publicly-traded companies before they were issued to the public. Many of the stolen press releases contained information about quarterly and annual earnings data for these

SPECIAL REPORT

FireEye

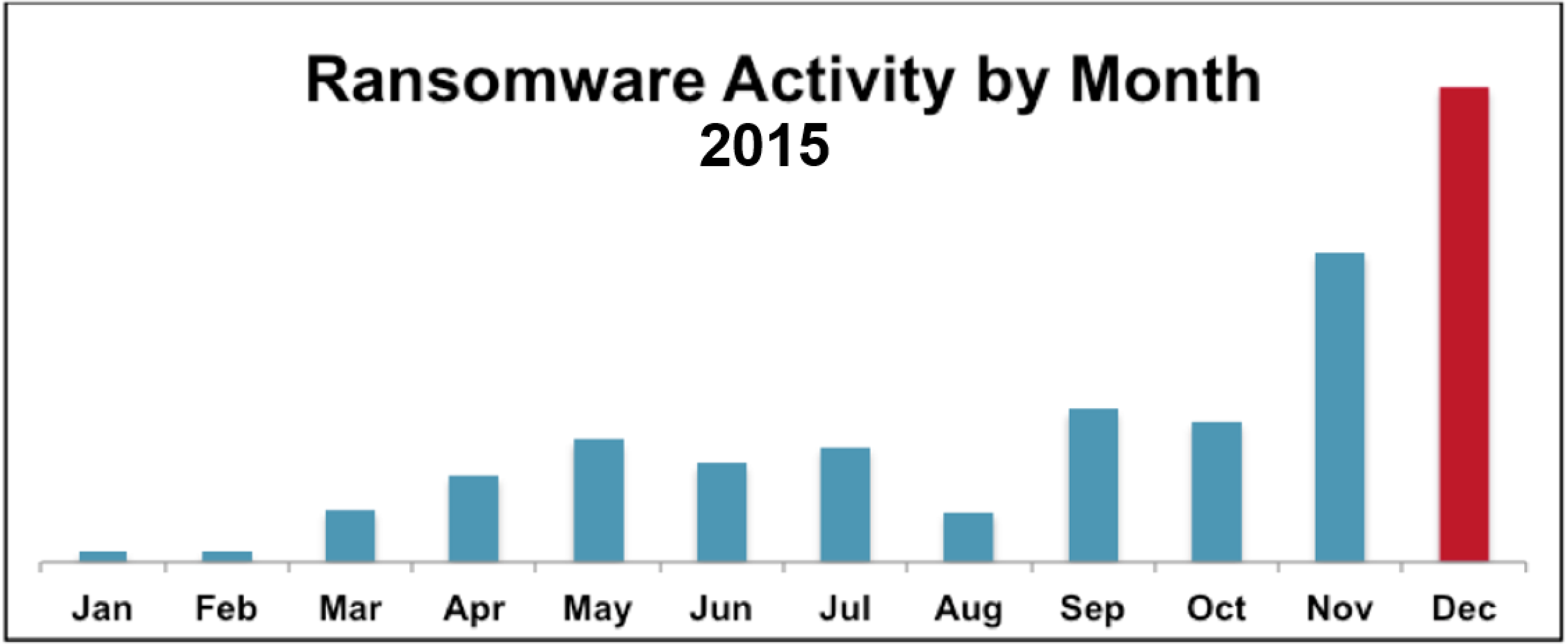
HACKING THE STREET?

FIN4 LIKELY PLAYING THE MARKET

WRITTEN BY:
BARRY VENGERIK
KRISTEN DENNESEN
JORDAN BERRY
JONATHAN WROLSTAD

SECURITY REIMAGINED

# Ransomware


Ransomware Activity by Month
2015
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec

# How to Use Strategic Intel

- Going from reactive to proactive
- Building a business case
- Prioritize response
- Anticipate attacker TTP
- Going from threats based to risk based
- What do we need to defend against first?

# Payment System Threat Intelligence

Glen Jones, Sr. Director, VISA, Cyber Intelligence and Investigations

# Merchant Data Compromises

## Entry

- Hackers targeting internet-exposed remote access systems as initial intrusion points
- Once in, reconnaissance
- Custom attack scripts and tools to further extend access

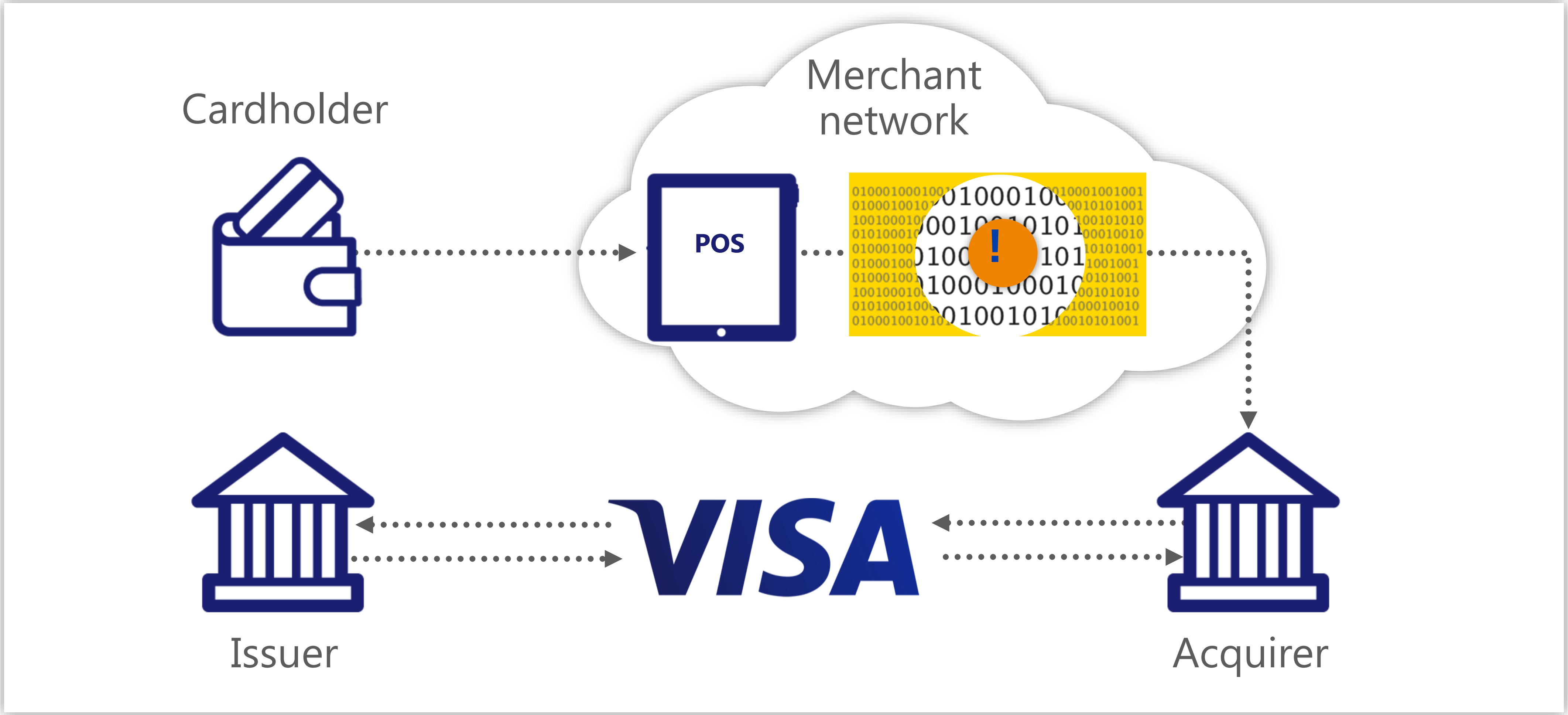
## Card data theft

- Payment card data is extracted with specialized, difficult to detect malware
- Malware is named to appear as legitimate security software in some cases
- Stolen card data is encrypted to avoid detection

## Monetization

- Payment data is used to commit fraud, often across countries via coordinated criminal activity
- Cards carry a typical value of between US$20–US$60

# Point of Sale RAM scraping



# Rise of POS Malware

## Privatized malware

- Kaptoxa (BlackPOS), BlackPOSv2, Alina, Dexter, BrutPOS, Backoff, FindPOS, RawPOS, Poseidon
- Nearly undetectable malware sold on underground markets
- Malware development, customization, deployment

## POS malware functionality

- RAM-scraping
- Keystroke logging
- Command-and-control communication
- Data exfiltration
- Download additional data (tools, scripts)
- Malware kill switch

# Transactional Threat Intelligence

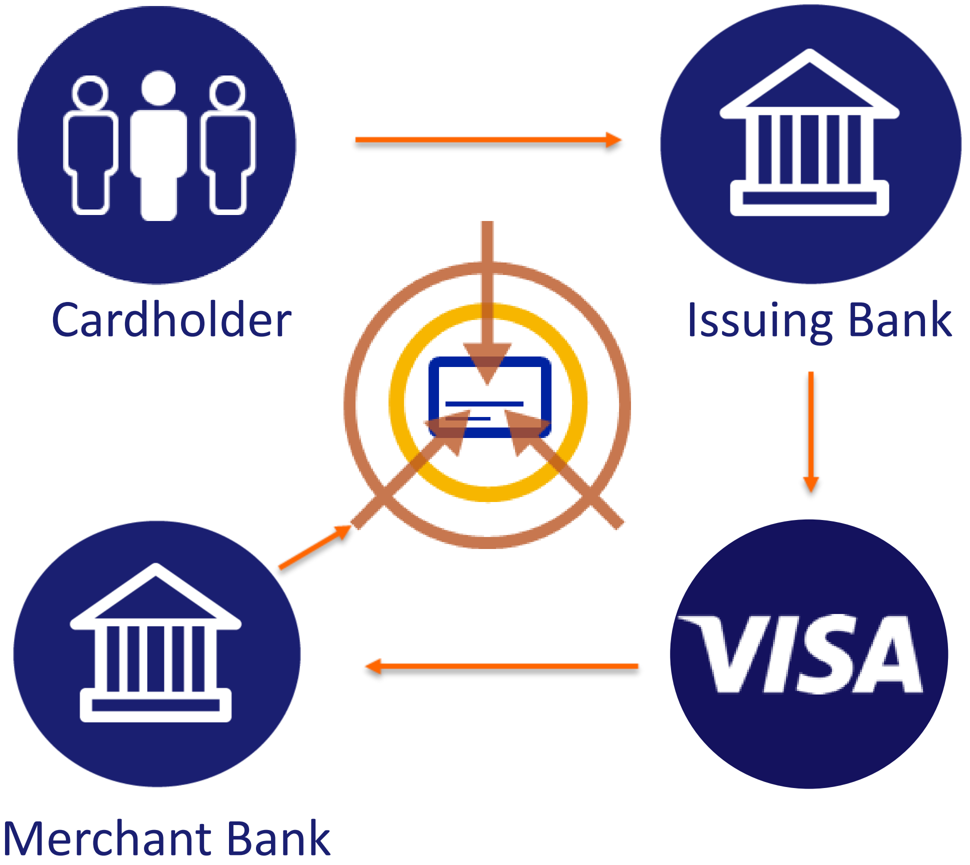
Intelligence comes from recognizing fraud patterns, predicting fraud activity

- Cardholders report fraud to their bank
- Banks report fraud to Visa (CPP)
- Visa reports fraud to other banks
- Breach found, stopped

One major limitation:

**What if there's no fraud?**

Breach Detection Cycle



# A new approach to Intel: Visa Threat Intelligence

**Intelligence briefings**

Detailed, curated, current, and expert intelligence to keep your business informed of key payment and cyber threats, what they mean for your business, and how to take action

**Indicator feeds**

Up-to-date and comprehensive intelligence that can easily be integrated into your security infrastructure to enable immediate identification and remediation of attacks

**Community circles**

A community-controlled, invite-only platform for company alliances and partnerships to share knowledge on today's threats and collaborate with peers to better defend against attackers

# Visa Threat Intelligence in Action: Case Study

1

- Visa or FireEye staff are involved in an investigation in the field*
- Malware that was used in the data compromise is discovered and analyzed

2

- Visa or FireEye inputs the Indicators of Compromise (IOC's) and other information into the Visa Threat Intelligence portal
- The IOC's highlight suspicious IP addresses, and characteristics of the malware that clients should look for in their own systems

3

- Visa Threat Intelligence clients read the bulletin, and download the IOC's so they can be loaded into their own threat detection systems
- IOC's can be downloaded manually through the portal, or programmatically via an optional API

4

- The clients' systems are poised to respond to this latest threat
- The turnaround time between step 2 through 4 could occur in minutes

** Visa Cyber Intelligence and Investigations*

# Upcoming Events and Resources

## Upcoming Webinars – Training tab on www.visa.com/cisp

Visa Threat Intelligence Webinar Series

- Retail Threats: April 13, 2016
- Hospitality Industry Threats: April 27, 2016
- Financial Intuition Threats: May 11, 2016
- Point of Sale Threats: May 25, 2016

Data Security

- Identifying, Mitigating and Preventing Skimming Attacks
  - 13 April 2016, 10 am PST

## FireEye – FireEye Threat Intelligence Website

## Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Past Webinar Presentations

## PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…