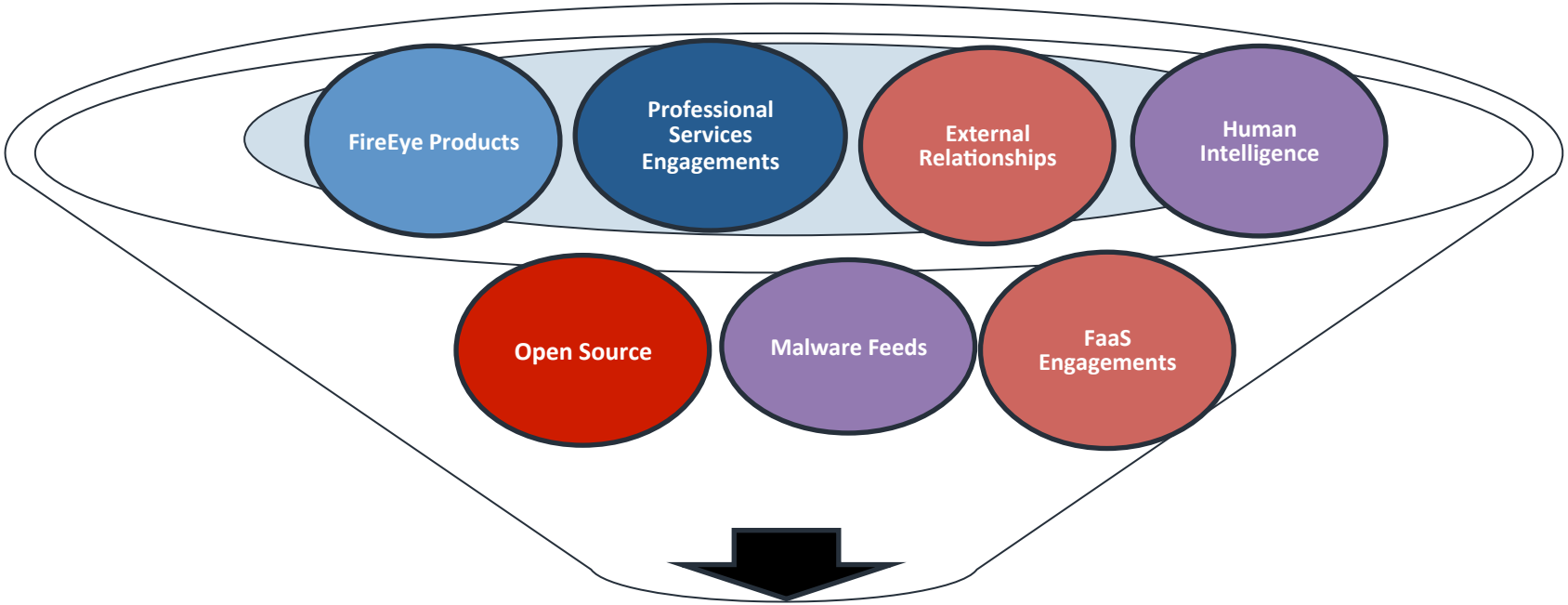
THREAT LANDSCAPE

Whoami

- FireEye Strategic Partners

- Cyber Analyst for CIA
  - Educated US Govt on cyber threats
  - Wrote for President's Daily Briefing
  - Presented at workshops and cyber conferences

Data is our Differentiator



Knowledge Base

DATA VS. THREAT INTELLIGENCE

Commoditized Feeds: Raw Data

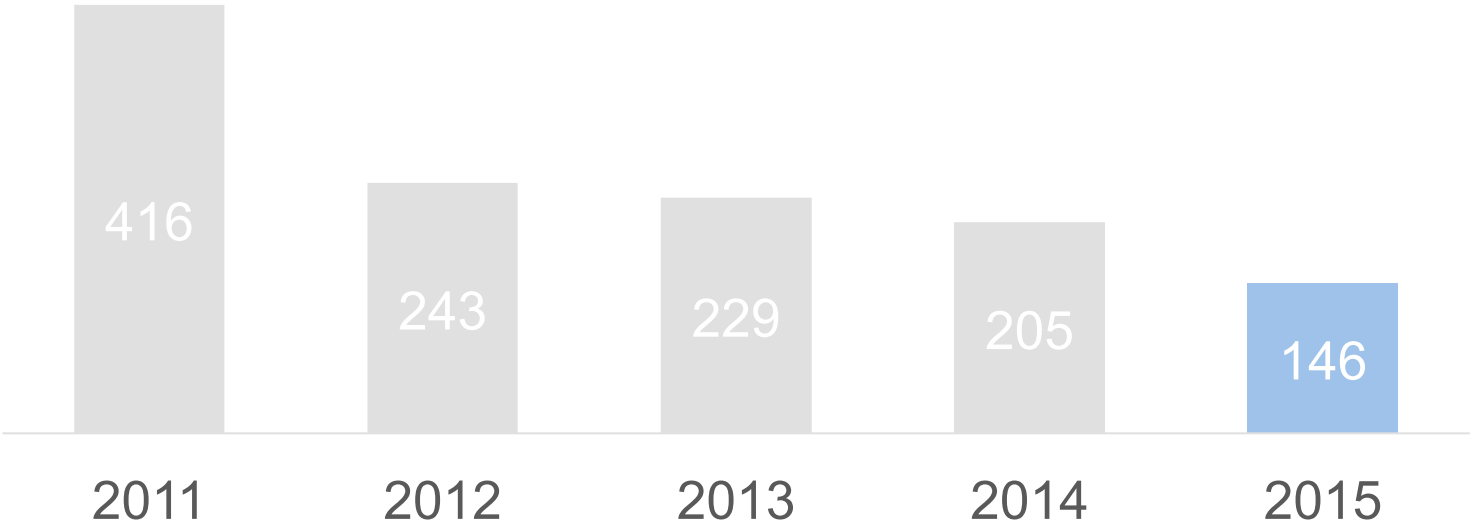
- **Misses the threats that matter.** Commoditized threat intelligence is too broad and out-of-date to protect against surgical attacks.
- **Becomes part of the problem.** Typically leads to voluminous alerts that require additional personnel to identify the true threats from within the noise.

≠

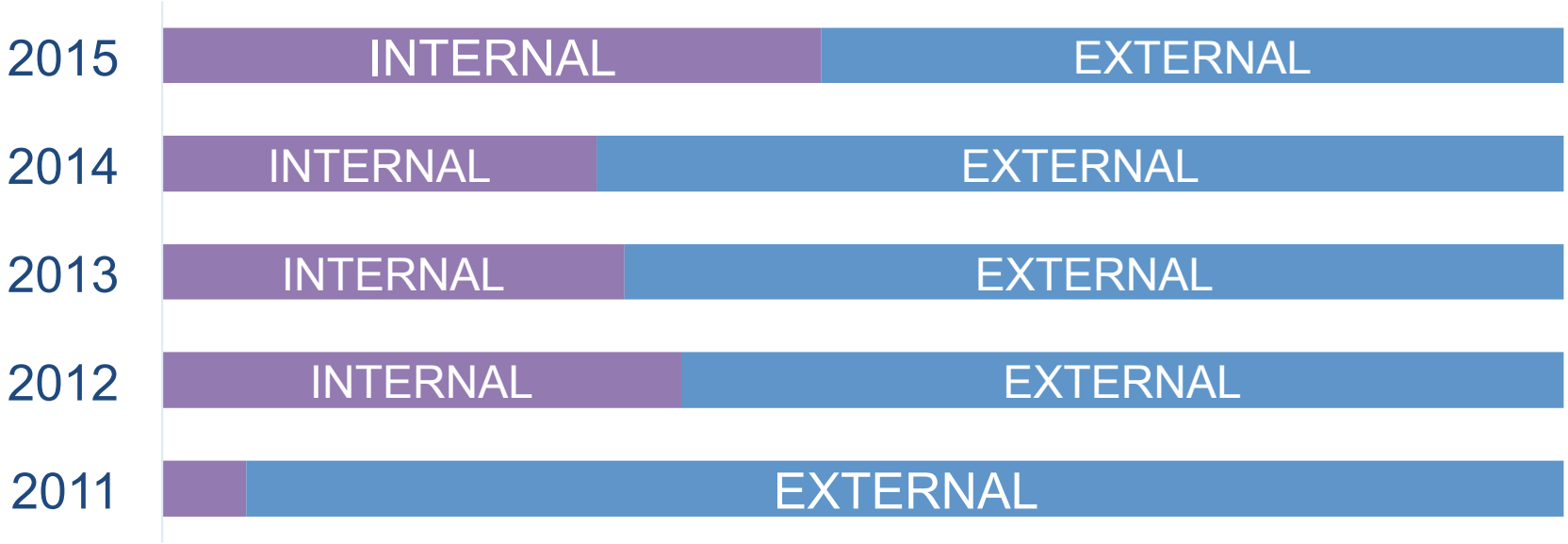
Threat Intelligence

- **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

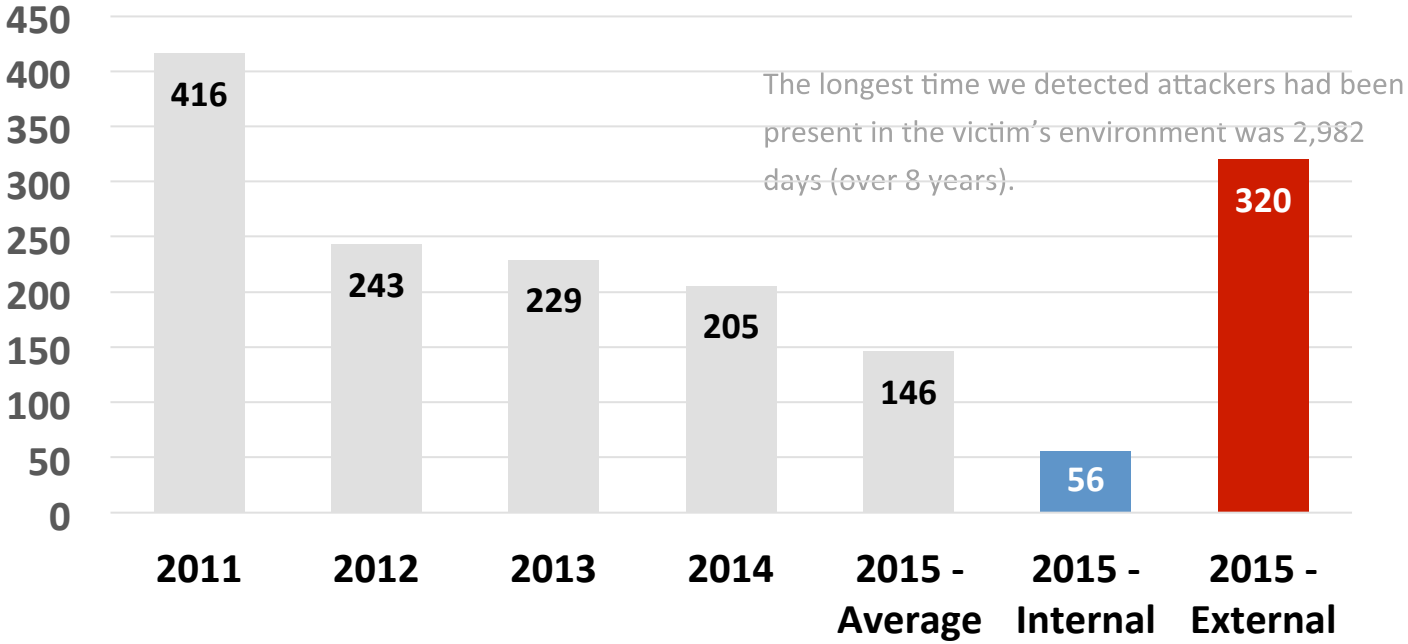
M-TRENDS: MEDIAN DAYS BEFORE DISCOVERY



M-TRENDS: INTERNAL DETECTION VS EXTERNAL NOTIFICATION



The typical incident saw attackers present for **4+ months**



The longest time we detected attackers had been present in the victim's environment was 2,982 days (over 8 years).

M-TRENDS 2016: MEDIAN DAYS BEFORE DISCOVERY

Primary Exploitation Vectors

Compromised
Software Updates

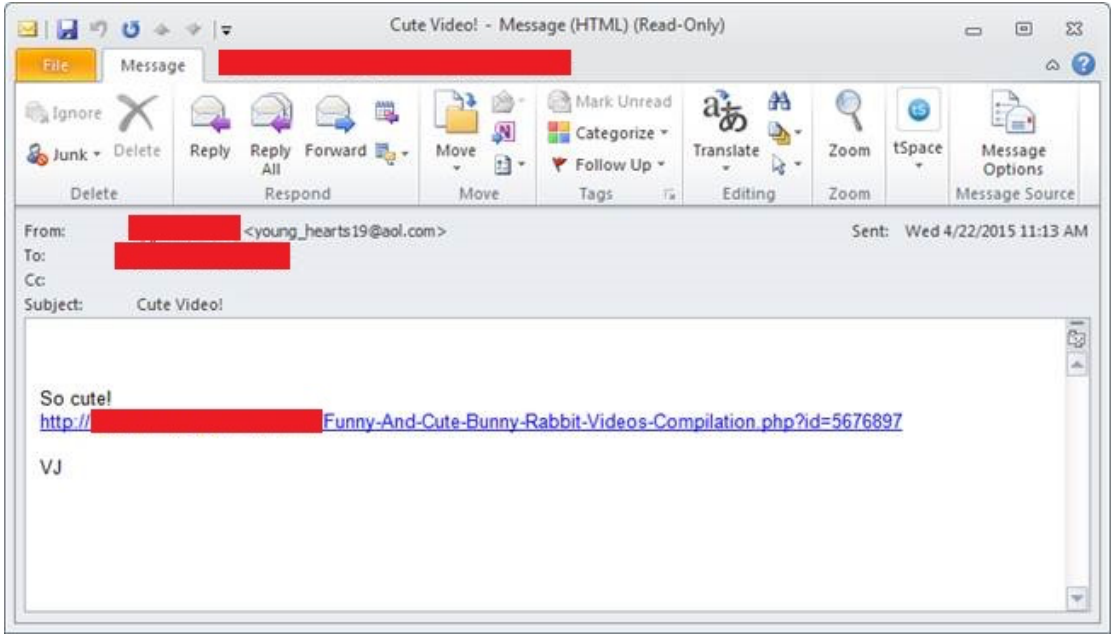
Spear Phishing Using
“Weaponized” Attachments

Strategic Web
Compromises

Infected Thumb Drives

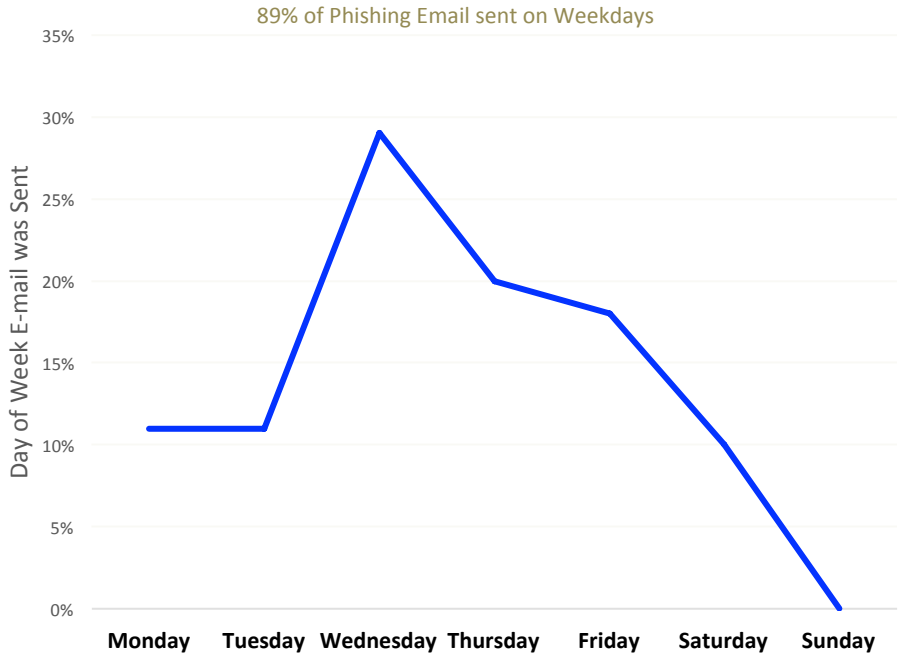
Spear Phishing

- Emails designed to exploit willingness to trust
- Weaponized attachments or documents, links to benign-sounding webpages that host exploits and MACROS
- This example was sent to a victim with the FROM address spoofed to resemble that of the victim's close relative

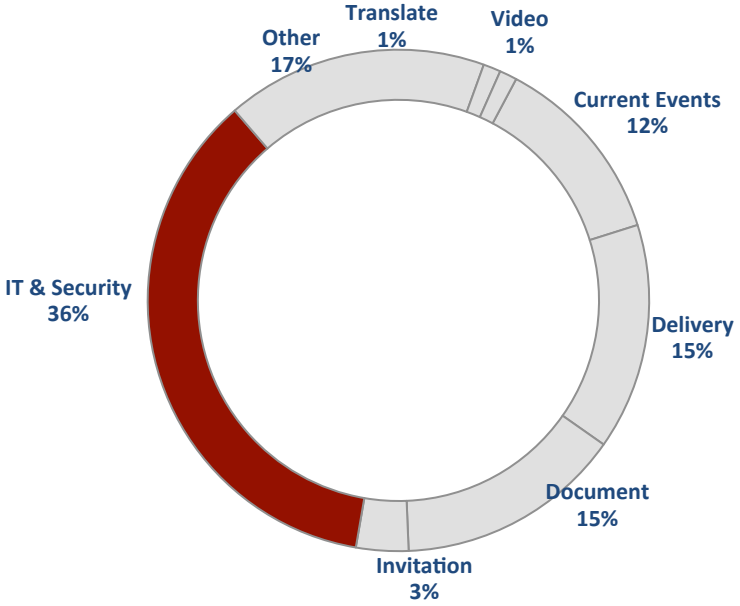


Email Trends

Days Victims Received Phishing E-mails

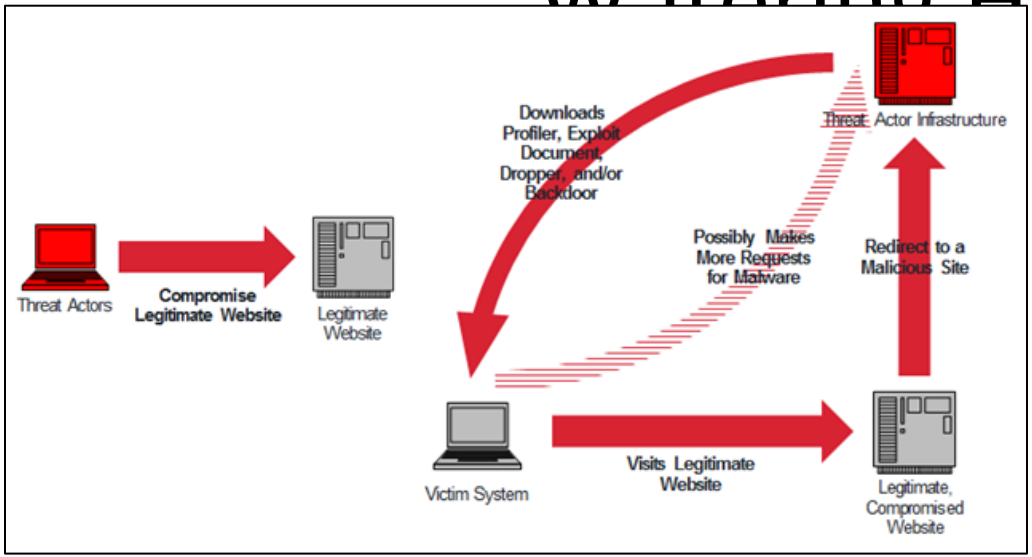


Phishing Themes



Majority of phishing emails were IT or security related, often attempting to impersonate the targeted company´s IT Department or an anti-virus vendor

Strategic Web Compromises / Watering Holes



- Strategic web compromises are frequently used to stealthily conduct reconnaissance against a user base
- Pages visited by system operators can be compromised to host malicious 'drive-by' malware that is downloaded to the user's machine without their knowledge
- Imagine going to the doctor for an annual check up and contracting the flu or tuberculosis

Lateral Movement ≠ Malware

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

Keeping Access – Operational Intel

Manage Emergency Access Tokencodes

for emergency access when the user has lost, broken, or misplaced a token. The user authenticates with his or her current PIN + the emergency tokencode pro

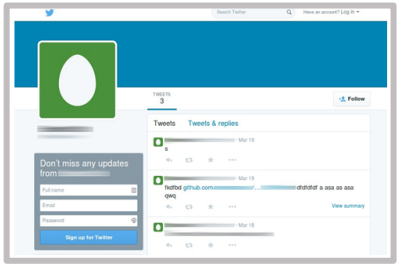
Cancel | Reset | Save

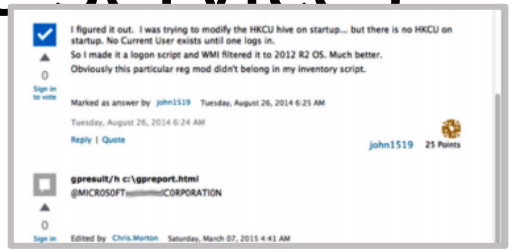
* Required field

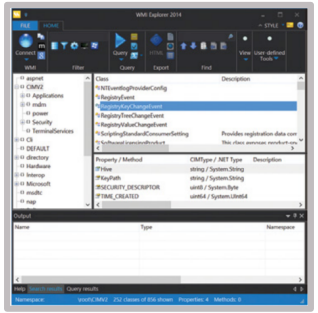
Online Emergency Access

Online Emergency Access:	☑ Enable authentication with an online emergency access tokencode
Type of Emergency Access Tokencode(s):	◉ Temporary Fixed Tokencode ○ Set of One Time Tokencodes
Online Emergency Access Tokencode:	Generate New Code (Tokencodes will not be assigned to user until you click Save)
Emergency Access Tokencode Lifetime:	◉ No expiration ○ Expire on
If Token Becomes Available:	○ Deny authentication with token ◉ Allow authentication with token at any time and disable online emergency tokencode ○ Allow authentication with token only after the emergency access code lifetime has expired and disable o
Last Used to Authenticate:	

Increasing Use of Consumer or Legitimate Services







Social Media

Cloud Storage Services

Comment Sections

Enterprise Management Tools

- ✓ Traffic looks 'benign'…like the normal user going to social media, a cloud storage site
- ✓ Greater control to the attacker on the victim network
- ✓ Flexible method to re-enter a network
- ✓ More difficult to detect with Encryption (SSL connections) and Infrequent timing

Cyber Crime

- **Most Prevalent Cyber Activity:** Billions of dollars in damages
  - FireEye actively monitors C2 infrastructure of 100+ crimeware families; tracks C2 beacons from over 10 million IPs every week
- **Vast Majority:** Opportunistic, Isolated Compromise
  - Seek to take what's immediately available
  - Opportunism can lead to targeted threats
- **Subset:** Targeted, Seek Lateral Movement, Capable Tools

FireEye

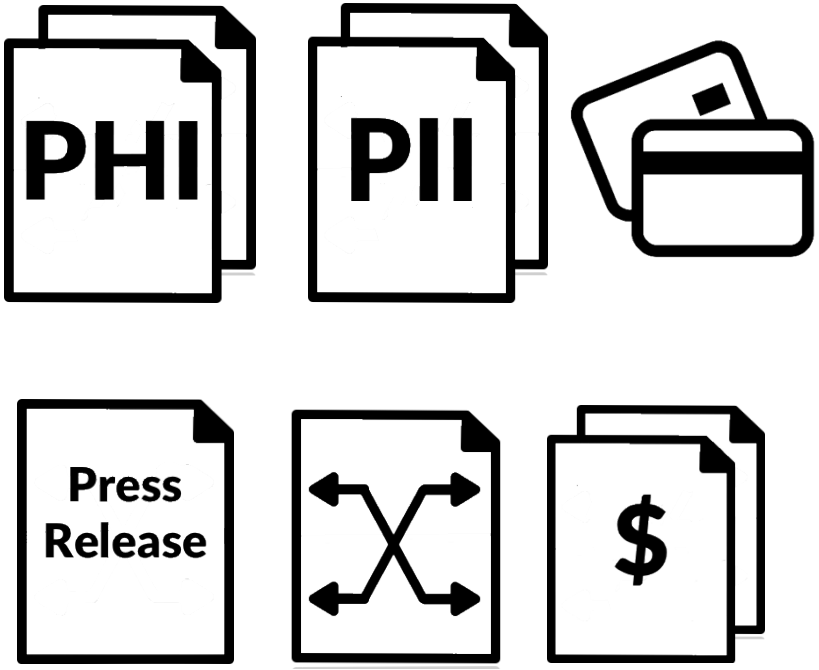
PII “Look Up” Services on Underground Forums

Active Criminal Market for Personal Information Databases

- Actors offer:
  - Databases stolen from specific organizations
  - PII “Look-up” Services offering personal data on specific individuals of interest
    - Illicit PII “search engines” that charge per query
    - Data sources include stolen DBs and data stolen via malware and phishing kits
- Stolen data purchased to enable fraud; ID theft; follow-on targeting of individuals/orgs of interest

Every Piece of Data Can Be Monetized

- **Sell data available on cyber criminal underground**
  - Not just credit cards
  - Personally Identifiable Information
  - Personal Health Information
- **Monetize for other ways**
  - Confidential business information for insider trading cases
  - Sell vulnerabilities
- **Ransomware**
  - **Extortion**



FireEye

Ransomware

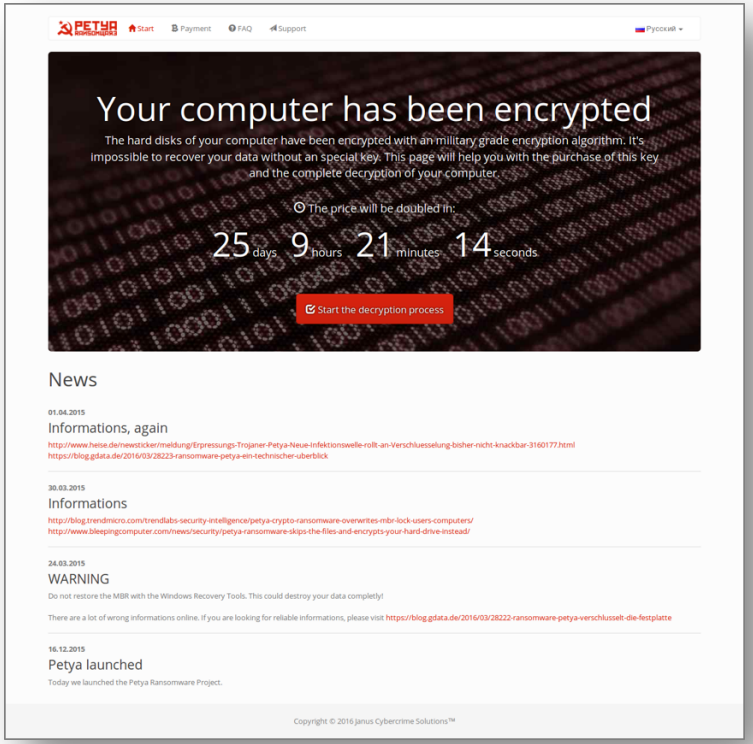
Impact of Media Attention

- Malware authors alter code
- Encryption flaws are fixed
- Draws more customers to affiliate programs
- Increases “scare” factor prompting more users to pay the ransom.
- TorrentLocker is a great example of malware authors versatility, fixing encryption flaws in less than a week:

[Analysis of ‘TorrentLocker’ – A New Strain of Ransomware Using Components of CryptoLocker and CryptoWall]

[TorrentLocker – New Variant with New Encryption Observed in the Wild]

- Petya is an excellent example of malware authors monitoring public reporting and media



* Reports published on Legacy iSIGHT Blog

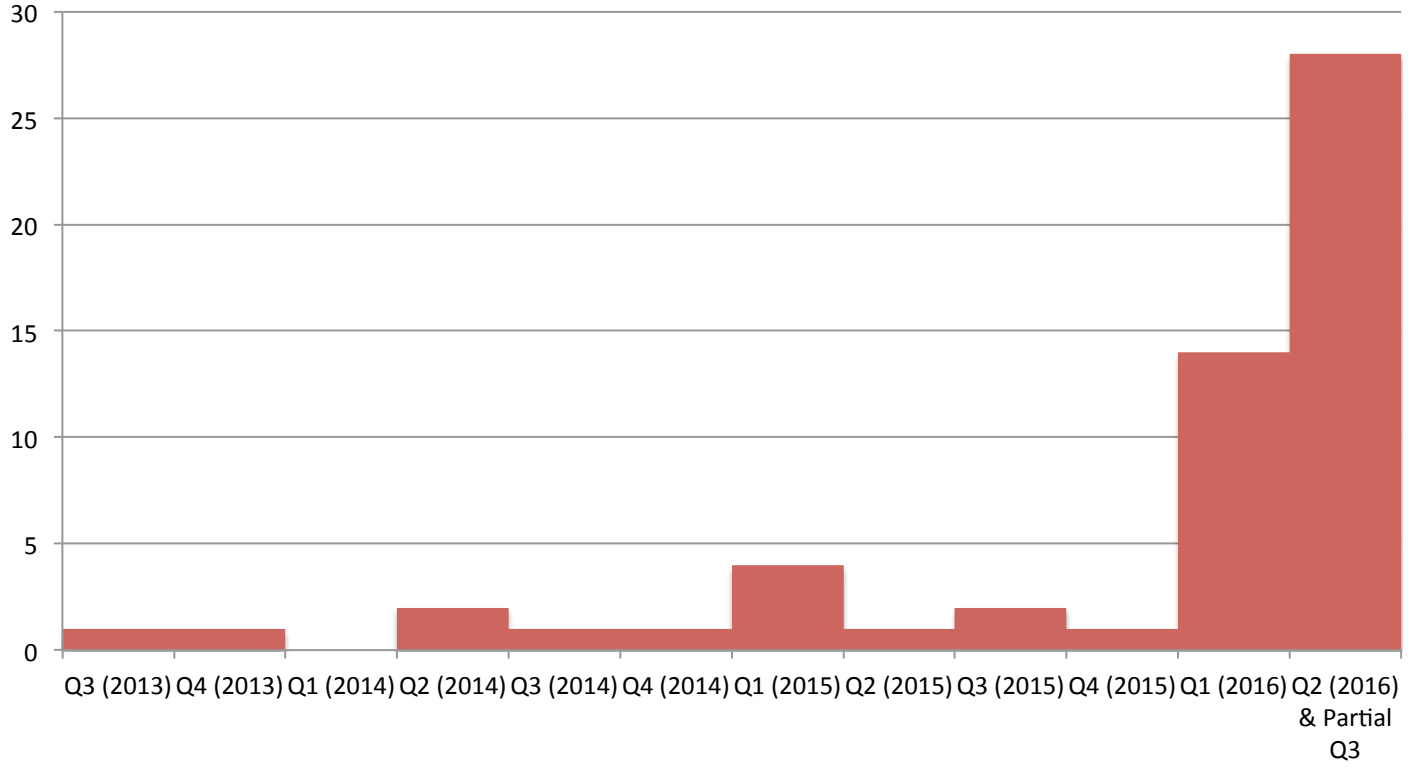
FireEye

Ransomware Services on E-Crime Markets

A variety of ransomware-related goods and services are offered through eCrime markets:

- Copies of ransomware
- Ransomware "builders”
- Affiliate programs where distributors are paid for spreading ransomware.
- Customization services to tailor ransom messages
- Money laundering services specifically for ransomware operators.

Timeline: Ransomware Discovery by Quarter



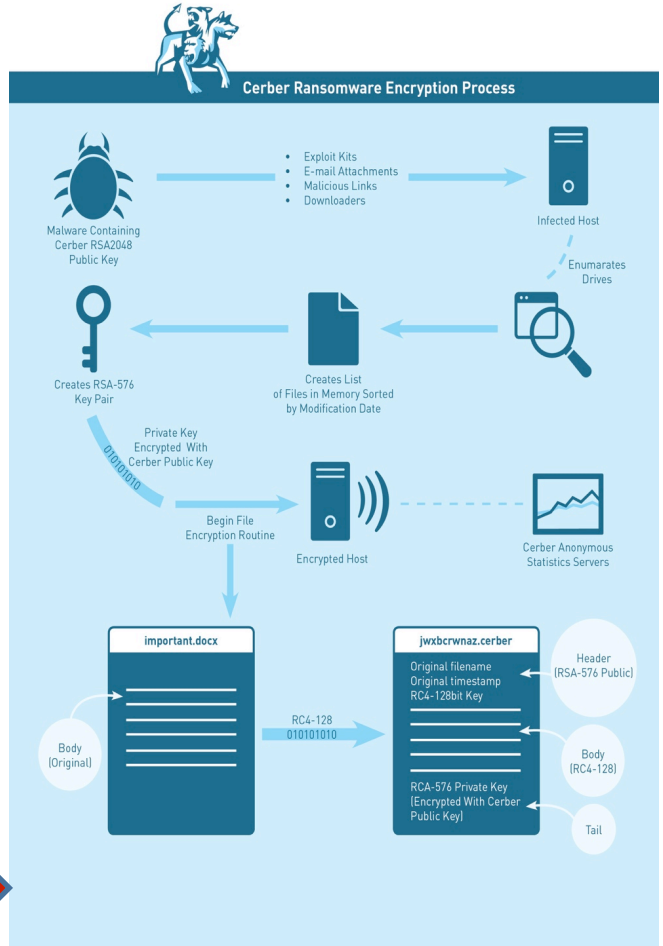
- *Data aggregated based on ransomware families that have unique capabilities, have been successful or had a high impact*
- *Data from Q2 and Q3 2016 may be revised in the future*

FireEye

Properties/Phases: Encryption Capabilities

- CryptoWall
  - Uses Windows crypto libraries
  - Random AES 256 key per file, uses public key from X509 certificate to encrypt AES keys
  - **Requires Network for public key retrieval**
- Locky
  - Uses Windows crypto libraries
  - Random AES 128/192 key per file, public RSA **key retrieved from C&C prior to encryption**
- Samas
  - Random AES 128 key per file, 512-bit HMAC signature, and RSA 2048 public key
  - Encrypts files immediately, **no network connection needed**

* Cerber: Example of differing encryption using RSA576, RC4, a
RSA2048.



FireEye

Critical Systems

- Scheduled task that deleted the Windows directory using the Microsoft robocopy
- Targeted critical systems within the environment.

```
mkdir “C:\emptydir”
robocopy “C:\emptydir” “C:\windows\system32” /MIR | shutdown /s /t 1800
```

FireEye

Case Study 2

- An attacker created multiple variants of malware designed to wipe Windows systems
- Attempted to automatically spread to other systems in the network
- For DC, malware delayed destruction so that the server could continue to provide Windows authentication services, allowing the malware to spreading more comprehensively

Some other key differences of the versions included:

- 1. Workstation – killed the antivirus process and wrote a custom MBR to the disk.
- 2. Server – disabled terminal services.
- 3. Mail Server – stopped the mail service and disabled terminal services.
- 4. Domain Controllers - disabled terminal services and executed the wiper code after a period of time to allow the malware to continue spreading.

FireEye

LOOKING TO THE FUTURE

Growth of Ransomware as a Service

Ransomware After Credential Theft

Ransomware on Previously Compromised Systems

Advanced Mobile Ransomware

FireEye

RECOMMENDATIONS

- User Education
- Patch Software
- Comprehensive Backups
- Up to date Anti-virus, HIPS
- Network Monitoring
- Blocking Macros
- Finding Open Network Shares

FireEye

Post-breach recommendations

- Better protection against malware
  - Sandboxing technology
- Make lateral movement harder
  - Unique admin passwords and password vaulting
  - Two-factor for jump servers and critical systems (e.g. password vault, virtual infrastructure)
- Make IR easier
  - Asset management
  - Centralized log management
  - Large scale packet capture

2016
and beyond…

- Advanced attackers will seek to:
  - Protect their tools through enhanced victim profiling and selective delivery
  - "Hide in the noise" of crimeware and hacktivism
  - Exploit poorly secured third parties as an initial entry point to targets
- Intrusions without conventional malware will become more common
  - Backdoors that increasingly employ legitimate cloud services for C2 and exfil
  - More abuse of built-in mechanisms (e.g., PowerShell, WMI, WSH, Kerberos)
  - Malware outside the OS (e.g., UEFI, VBR) may be used to avoid detection

THANK YOU