RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-T11

Hide and Seek: How Threat Actors Respond in the Face of Public Exposure

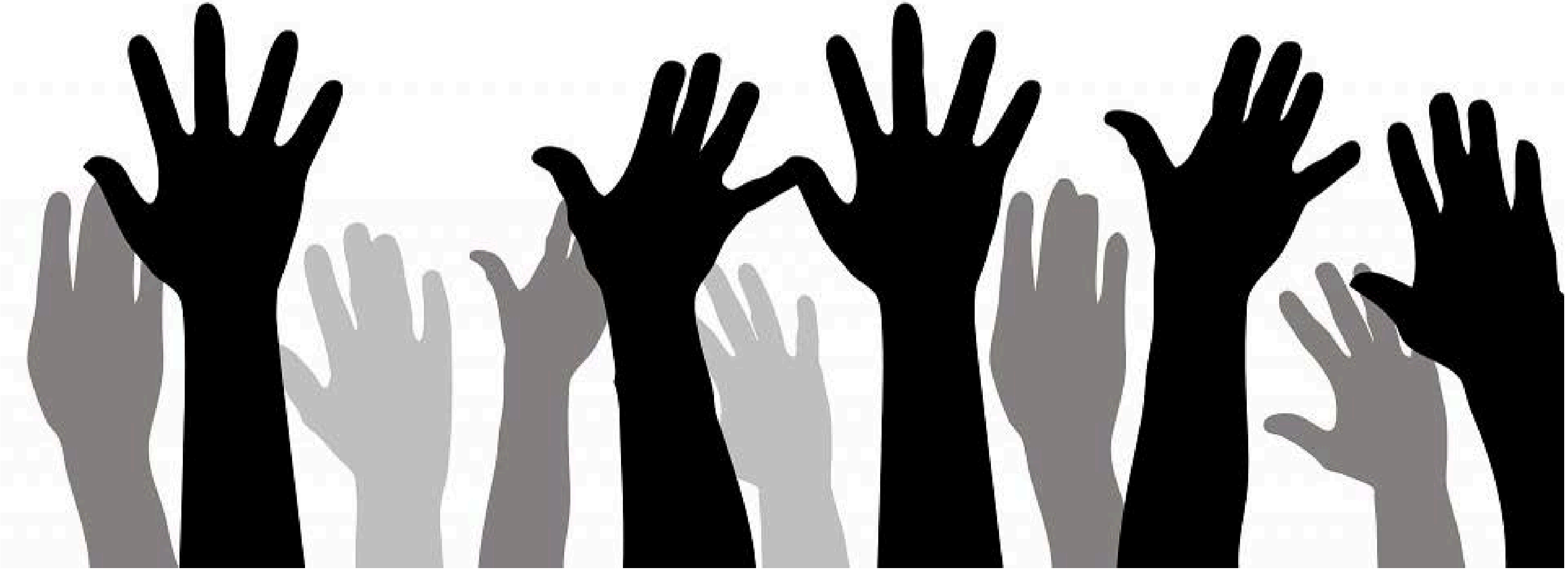
Kristen Dennesen

Senior Intelligence Analyst
FireEye, Inc.
@FireEye

#RSAC

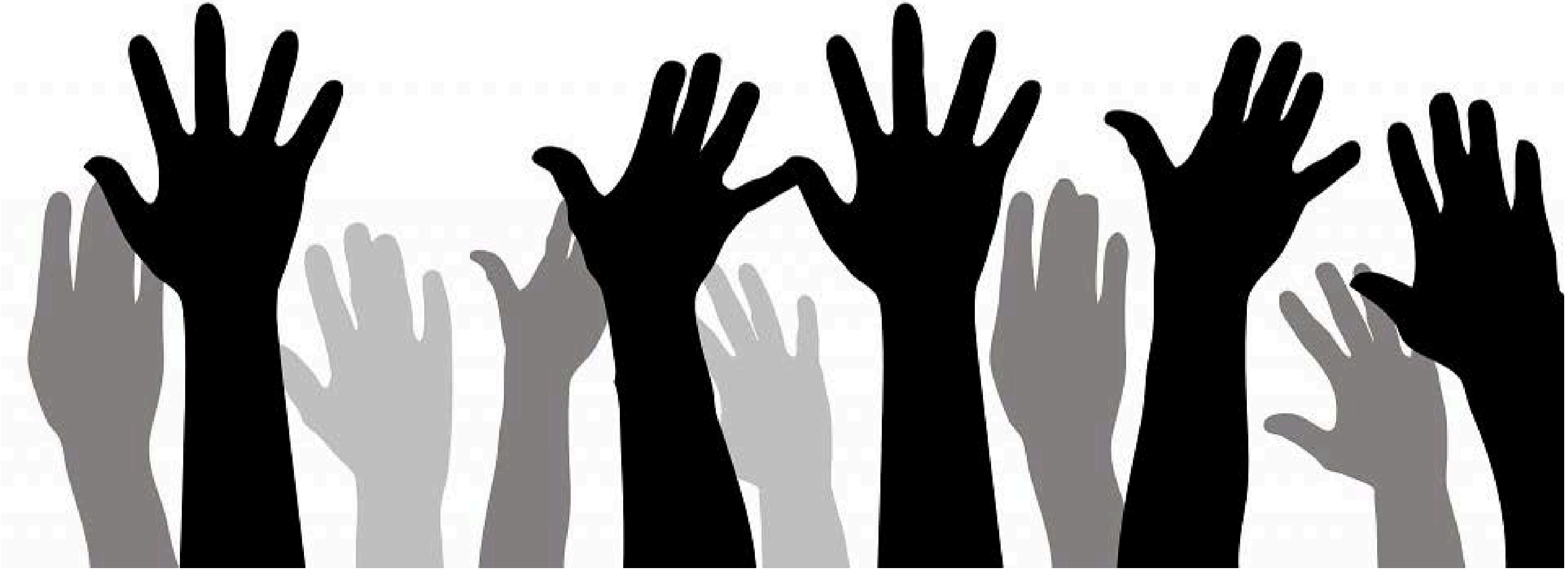
Show of Hands

Have you ever been directly involved in a public white paper or blog about a threat actor?



Show of Hands

Do you use vendor white papers or blogs to develop better situational awareness about threats to your organization?



Research Question

How do threat groups respond when their operations are exposed in public reporting?

Bottom Line Up Front

Public exposure is a major trigger for behavioral change

Apply

By the end of this presentation you'll be able to…

Evaluate the impact of a blog or white paper on an adversary's future operations

Road Map

Photo: Ryan Cadby @ryancadby on Flickr

- Introduction
- Key Concepts
- Case Studies
- Call to Action

A Tug of War

Intelligence collection

vs.

Computer network defense

Photo: William James ca. 1920 City of Toronto Archives

Why Does Exposure Matter?

Public spotlight creates a flashpoint of awareness of a group's ops, TTPS

- Security vendors sprint to detect publicized activity
- Net defenders more likely to hunt in their networks for evidence of a group, employ new IOCs or detection methods

Exposure triggers public awareness and increases threat groups' risk of detection/discovery.

Why Does Exposure Matter – Big Picture

- What ethical boundaries and obligations do security researchers face?
- Are we cultivating better OPSEC in the actors we expose?
- What is the best way to share?
- Mission vs. Marketing

Key Concept

Threat Shifting

> *“Response from adversaries to perceived safeguards and/or countermeasures, in which the adversaries change some characteristic of their [operations] in order to avoid and/or overcome those safeguards/countermeasures”*

— NIST Special Publication 800-30: Guide for Conducting Risk Assessments

Threat Shifting in Nature

Evolution to reduce the risk of predation

Mimickry: Heliconius butterflies mimic wing coloration patterns to signal toxicity to predators

Threat Shifting in Information Security

Examples of Threat Shifting

- Evolution of banking Trojans from clumsy keyloggers to highly flexible webinject offerings
- Adoption of Powershell and WMI for lateral movement and backdoor functionality

Four Domains for Adaptation

Threat shifting occurs across four domains:

TIMING

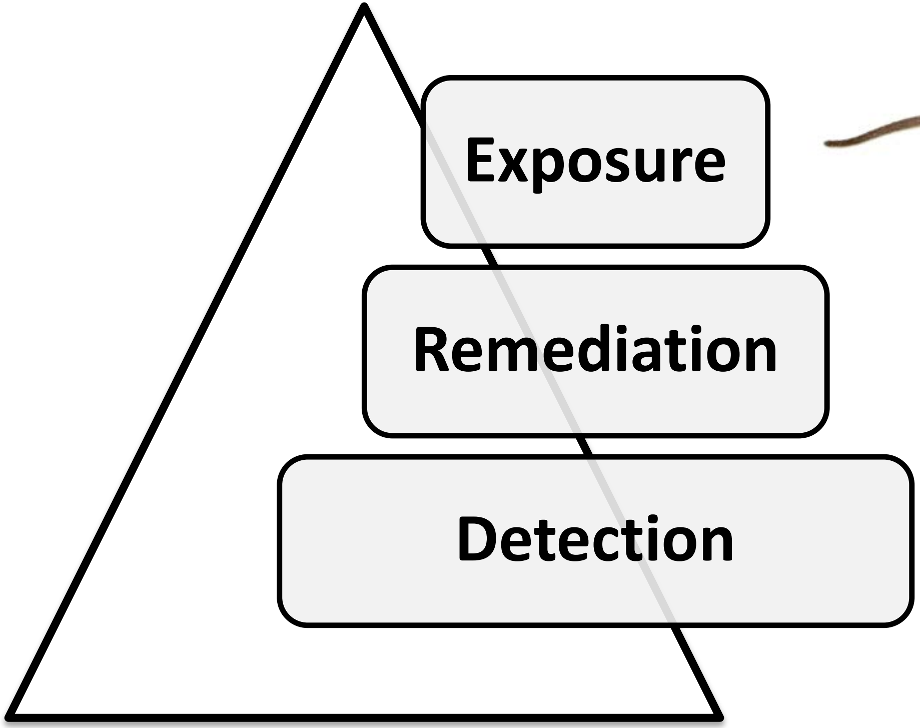
TARGETS

RESOURCES

PLANNING & METHODS

Image Sources: Public Domain @o5com on Flickr; Andrew Magill @amagill on Flickr

Trigger Points for Threat Shifting



Exposure

Remediation

Detection

A caveat…

Our observations are based on FireEye’s visibility.

Research Question

How do threat groups respond when their operations are exposed in public reporting?

They know.

Threat groups are often keenly aware of research & reporting on their operations.

They know.

APT28 signals they are aware of security researchers' blogs (and none too pleased…)

- July 2015 blog on APT28 spear phishing campaign that leveraged a Java zero-day
- Within 1 day, APT28 updated DNS info for domain hosting exploit to point to TrendMicro's IP space

* APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

Keenly aware of research and reporting

Threat Actors Read the News, Too.

- **APT1:** Major interruption to APT1's operations
- **Careto/Mask**: "…after the post was published, the Mask operators **shut everything down within about four hours**"
- **APT3 aka UPS:** Changed tactics on the fly in direct response to FireEye blog

Keen awareness: APT29

APT29 aka the Dukes, CozyDuke, TEMP.Monkey, Cozy Bear

Security researchers likely analyzing samples; probing staging server

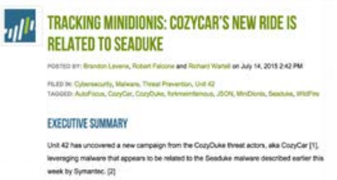
July 3, 2015
Downloader compiled

July 7, 2015
Phish sent: National Endowment for Democracy lure

July 8, 2015
Phish payload submitted to VT

July 14, 2015
Payload files **deleted** from compromised server

July 14, 2015



TRACKING MINIDIONIS: COZYCAR'S NEW RIDE IS RELATED TO SEADUKE

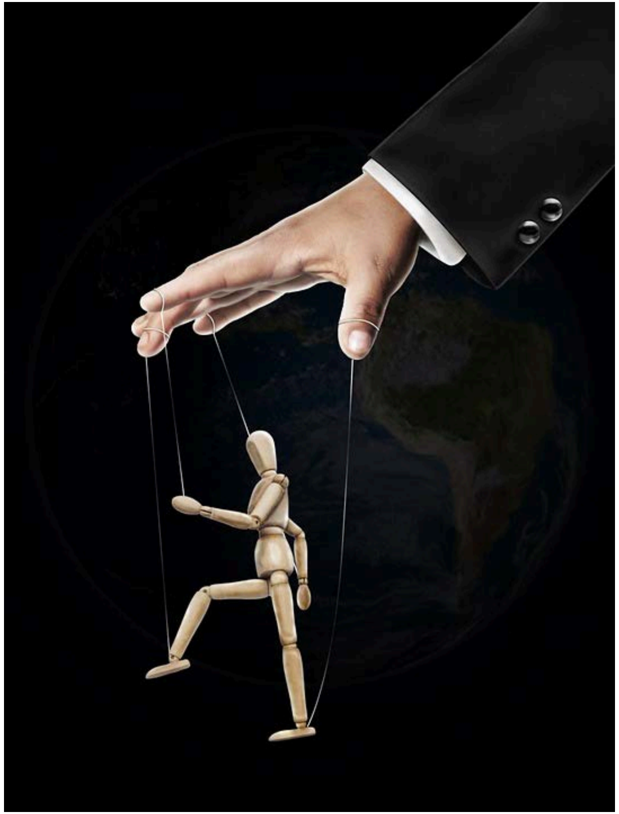
POSTED BY: Brandon Levene, Robert Falcone and Richard Wartell on July 14, 2015 2:42 PM

FILED IN: Cybersecurity, Malware, Threat Prevention, Unit 42
TAGGED: AutoFocus, CozyCar, CozyDuke, forkmeiamfamous, JSON, MiniDionis, Seaduke, WildFire

EXECUTIVE SUMMARY

Unit 42 has uncovered a new campaign from the CozyDuke threat actors, aka CozyCar [1], leveraging malware that appears to be related to the Seaduke malware described earlier this week by Symantec. [2]

Not only are they keenly aware…



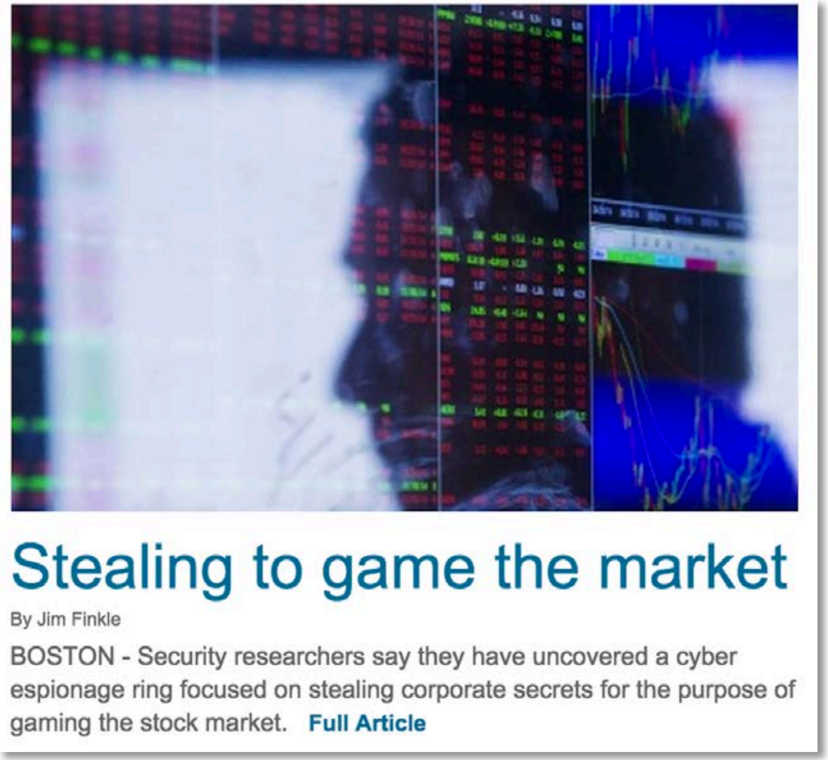
Some actors actively seek to **MANIPULATE** public perception.

Public reports can be deeply disruptive to a threat group’s operations… or not.

Incentives matter.

FIN4: Cybercriminals Playing the Market

FIN4: Targeted 100+ organizations in seek of information that would convey a stock trading advantage

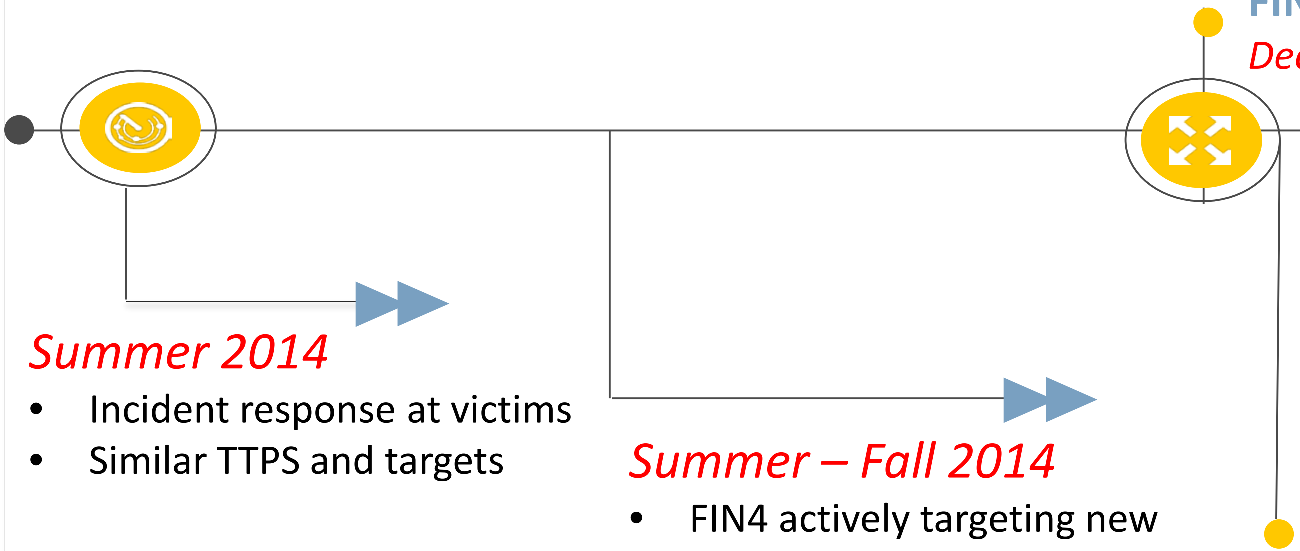


Stealing to game the market

By Jim Finkle

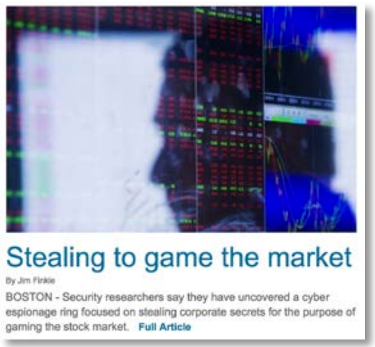
BOSTON - Security researchers say they have uncovered a cyber espionage ring focused on stealing corporate secrets for the purpose of gaming the stock market. **Full Article**

Can’t Take the Heat: FIN4 Halts Operations



FIN4 REPORT PUBLISHED

Dec. 1, 2014



Stealing to game the market

By Jim Finkle

BOSTON - Security researchers say they have uncovered a cyber espionage ring focused on stealing corporate secrets for the purpose of gaming the stock market. **Full Article**

Summer 2014

- Incident response at victims
- Similar TTPS and targets

Summer – Fall 2014

- FIN4 actively targeting new victims
- Adds dozens of new targets in week prior to public report

FIN4 DISCONTINUES OPS

Dec. 2014

- FIN4 appears to shut down entirely

APT28: Collecting Intelligence for a State Sponsor

APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

APT28: global intelligence collection operation targeting information tightly aligned w/ Russian government interests.

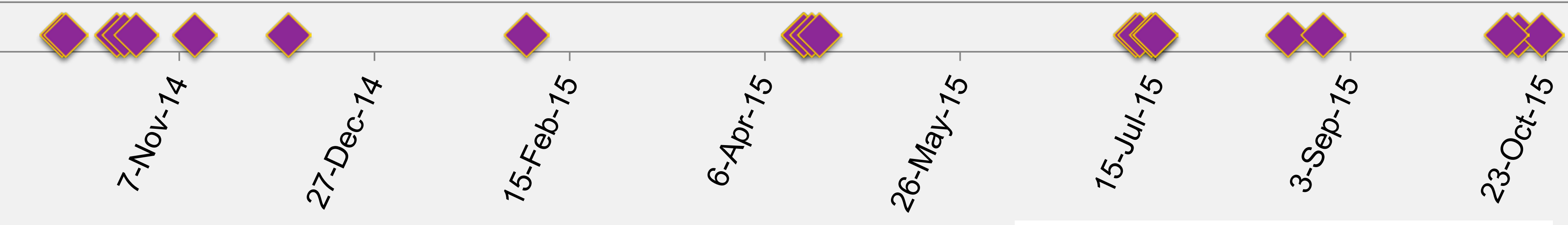
APT28: Keep on Truckin’

APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

20+

Reports examining APT28 TTPS

Oct. 2014 – Oct. 2015



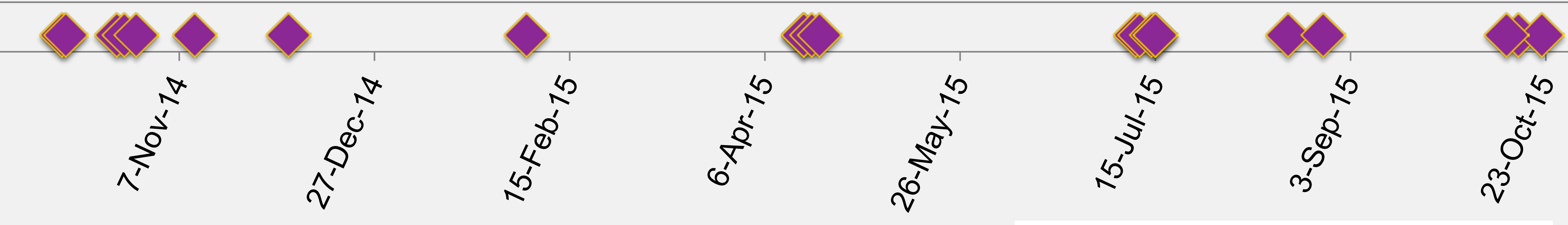
Timeline of APT28 Exposures

◆ Public report examining APT28’s operations

APT28: Keep on Truckin'

APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

In spite of repeated exposure APT28 has sustained operations

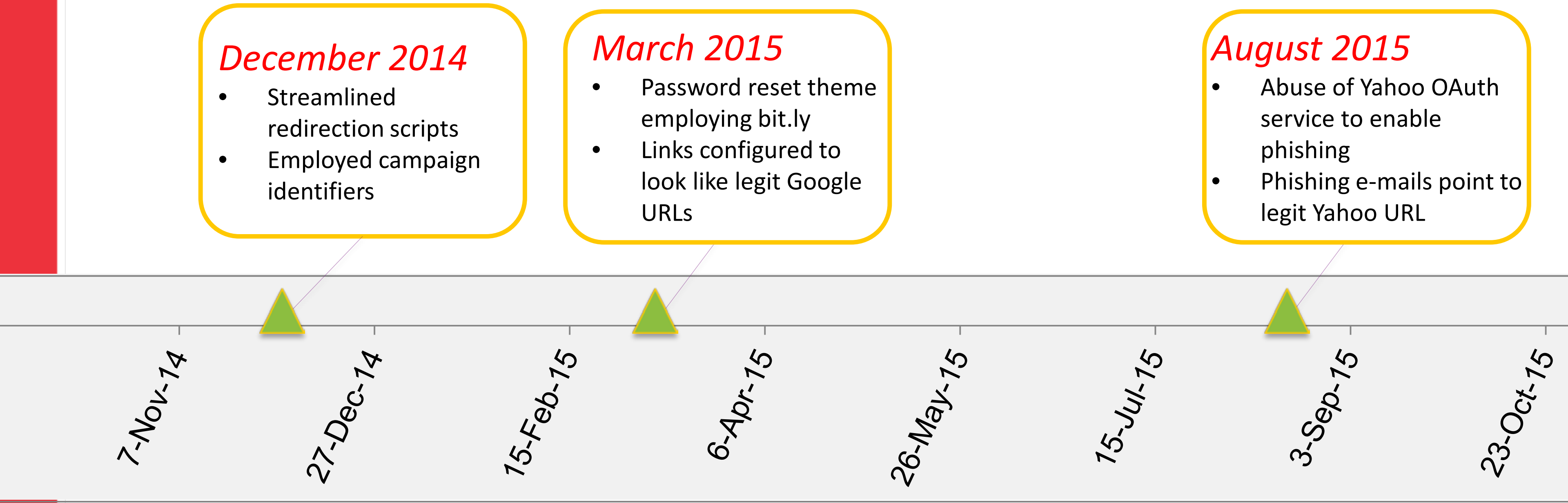


Timeline of APT28 Exposures

◆ Public report examining APT28's operations

APT28: Keep on Truckin’

APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium



December 2014

- Streamlined redirection scripts
- Employed campaign identifiers

March 2015

- Password reset theme employing bit.ly
- Links configured to look like legit Google URLs

August 2015

- Abuse of Yahoo OAuth service to enable phishing
- Phishing e-mails point to legit Yahoo URL

Timeline of APT28 Exposures

▲ New Phishing Tactic Observed

Incentives Matter.

Opportunistic

vs.

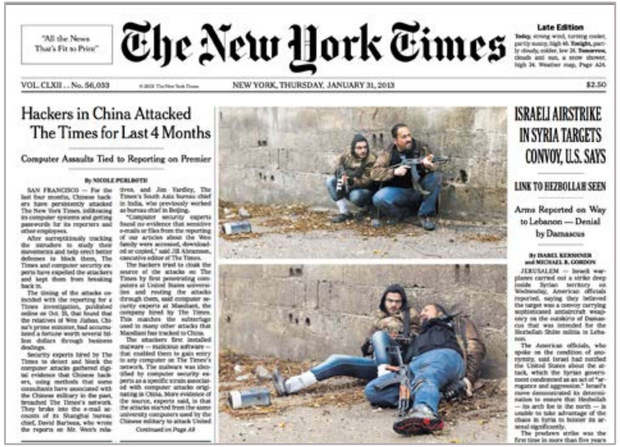
Requirements Driven

Public reports are a common trigger for retooling

APT12: “Darwin’s Favorite APT Group”

APT12 aka DNSCALC, IXESHE, CALC Team, DynCalc, Numbered Panda

- **Jan. 31, 2013**: New York Times exposes APT12 intrusion in their environment
  - Exposure triggered brief pause in activity and immediate changes in TTPs
- **June 6, 2014**: APT12’s RIPTIDE aka Etumbot backdoor is the subject of a comprehensive white paper
  - White paper triggered rapid shift in toolset.



“All the News That’s Fit to Print”

The New York Times

Late Edition

Today, strong wind, turning cooler, partly sunny, high 46. **Tonight**, partly cloudy, colder, low 26. **Tomorrow**, clouds and sun, a snow shower, high 34. Weather map, Page A24.

VOL. CLXII . . No. 56,033 © 2013 The New York Times NEW YORK, THURSDAY, JANUARY 31, 2013 $2.50

Hackers in China Attacked The Times for Last 4 Months

Computer Assaults Tied to Reporting on Premier

By NICOLE PERLROTH

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

After surreptitiously tracking the intruders to study their movements and help erect better defenses to block them, The Times and computer security experts have expelled the attackers and kept them from breaking back in.

The timing of the attacks coincided with the reporting for a Times investigation, published online on Oct. 25, that found that the relatives of Wen Jiabao, China’s prime minister, had accumulated a fortune worth several billion dollars through business dealings.

Security experts hired by The Times to detect and block the computer attacks gathered digital evidence that Chinese hackers, using methods that some consultants have associated with the Chinese military in the past, breached The Times’s network. They broke into the e-mail accounts of its Shanghai bureau chief, David Barboza, who wrote the reports on Mr. Wen’s relatives, and Jim Yardley, The Times’s South Asia bureau chief in India, who previously worked as bureau chief in Beijing.

“Computer security experts found no evidence that sensitive e-mails or files from the reporting of our articles about the Wen family were accessed, downloaded or copied,” said Jill Abramson, executive editor of The Times.

The hackers tried to cloak the source of the attacks on The Times by first penetrating computers at United States universities and routing the attacks through them, said computer security experts at Mandiant, the company hired by The Times. This matches the subterfuge used in many other attacks that Mandiant has tracked to China.

The attackers first installed malware — malicious software — that enabled them to gain entry to any computer on The Times’s network. The malware was identified by computer security experts as a specific strain associated with computer attacks originating in China. More evidence of the source, experts said, is that the attacks started from the same university computers used by the Chinese military to attack United

Continued on Page A9

ISRAELI AIRSTRIKE IN SYRIA TARGETS CONVOY, U.S. SAYS

LINK TO HEZBOLLAH SEEN

Arms Reported on Way to Lebanon — Denial by Damascus

By ISABEL KERSHNER and MICHAEL R. GORDON

JERUSALEM — Israeli warplanes carried out a strike deep inside Syrian territory on Wednesday, American officials reported, saying they believed the target was a convoy carrying sophisticated antiaircraft weaponry on the outskirts of Damascus that was intended for the Hezbollah Shiite militia in Lebanon.

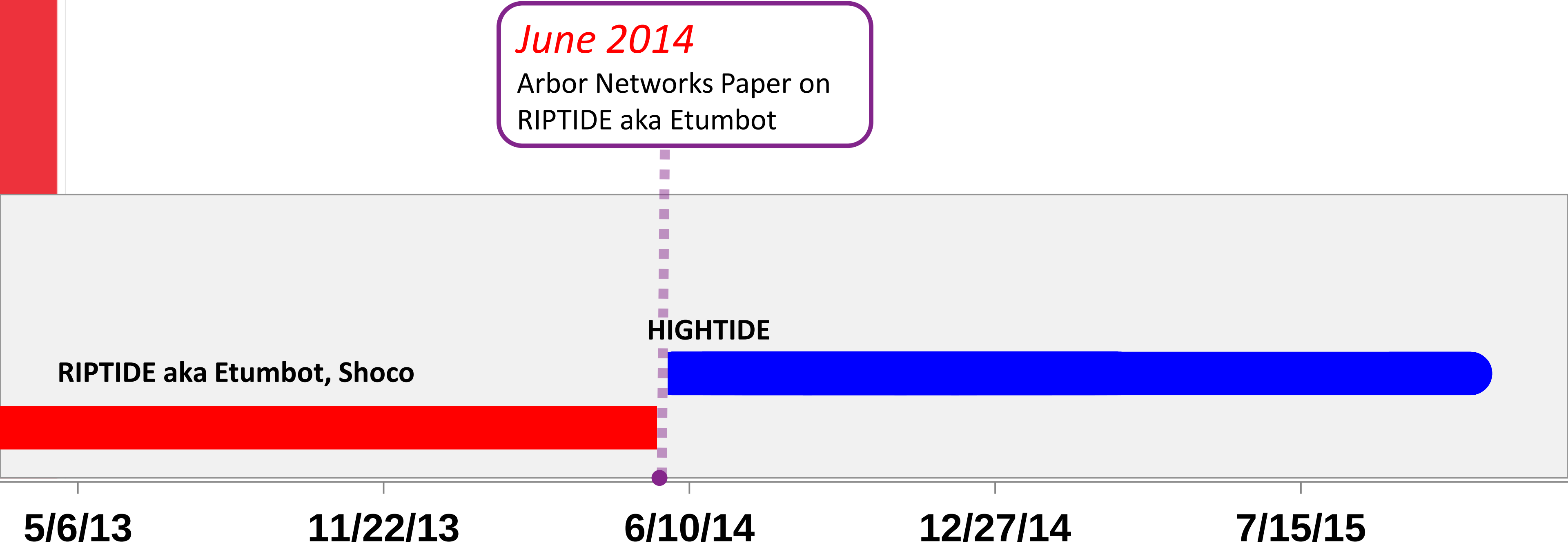
The American officials, who spoke on the condition of anonymity, said Israel had notified the United States about the attack, which the Syrian government condemned as an act of “arrogance and aggression.” Israel’s move demonstrated its determination to ensure that Hezbollah — its arch foe in the north — is unable to take advantage of the chaos in Syria to bolster its arsenal significantly.

The predawn strike was the first time in more than five years

New York Times — Jan. 31, 2013

APT12 Retools After RIPTIDE White Paper

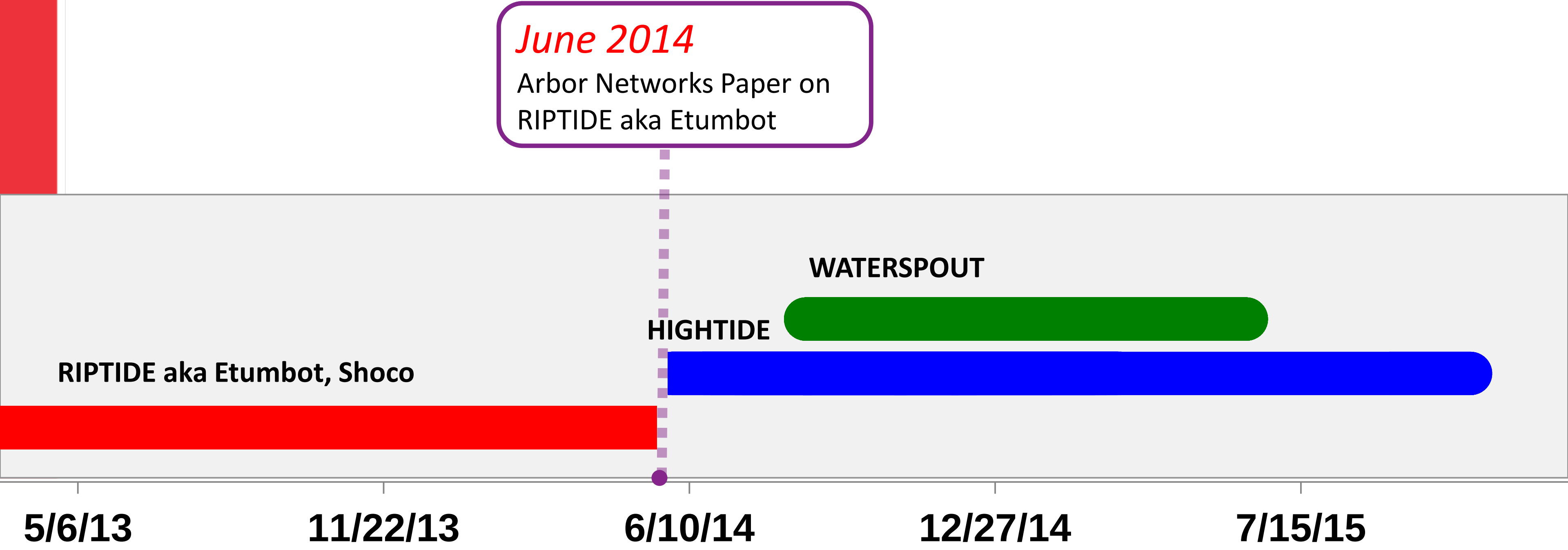
APT12 aka DNSCALC, IXESHE, CALC Team, DynCalc, Numbered Panda


June 2014

Arbor Networks Paper on RIPTIDE aka Etumbot

APT12 Retools After RIPTIDE White Paper

APT12 aka DNSCALC, IXESHE, CALC Team, DynCalc, Numbered Panda



June 2014

Arbor Networks Paper on RIPTIDE aka Etumbot

Operation SMN — Axiom Group Interdiction

APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda

More than an exposure effort:

- Coalition sought to eradicate specific ‘high value’ tools and make it more expensive for APT17 to operate
- Coordinated action was accompanied by public materials to aid detection and educate victims

Operation SMN coalition went into the effort with eyes wide open:

- Acknowledged from outset that APT17 was skilled, equipped to adapt and would very likely retool

NOVETTA

Operation SMN:

Axiom Threat Actor Group Report
公理队

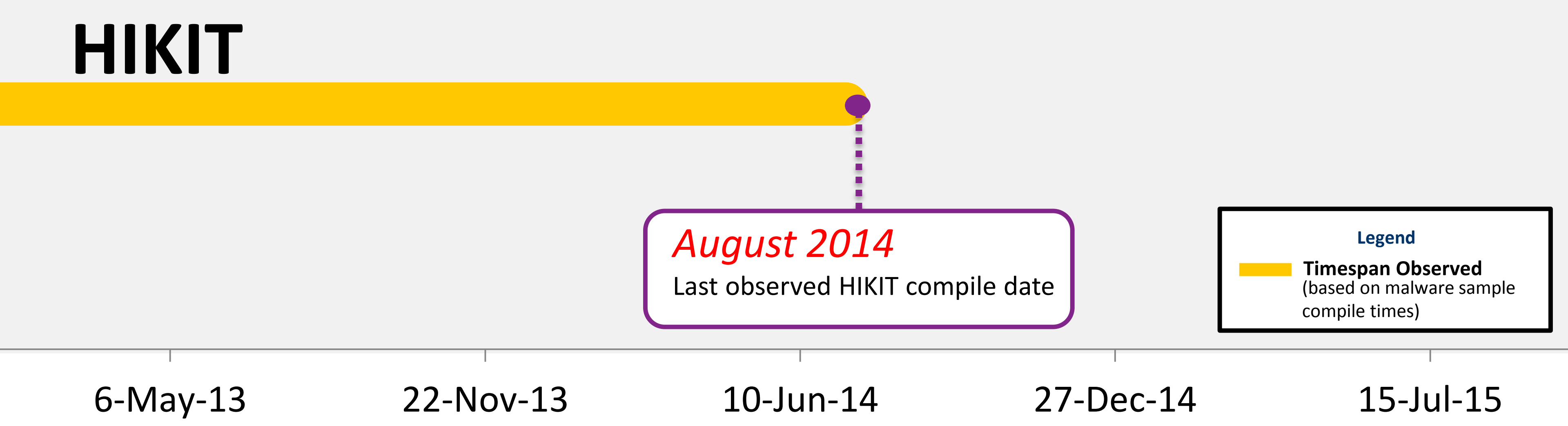
Thank you to our public partners:

Bit9 + CARBON BLACK ARM YOUR ENDPOINTS. CISCO F-Secure FireEye
iSIGHTPARTNERS tenable THREATCONNECT
ThreatTrack VOLEXITY

Operation SMN sought to KNOCK OUT APT17'S high value tools such as HIKIT

Before and After Operation SMN

APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda

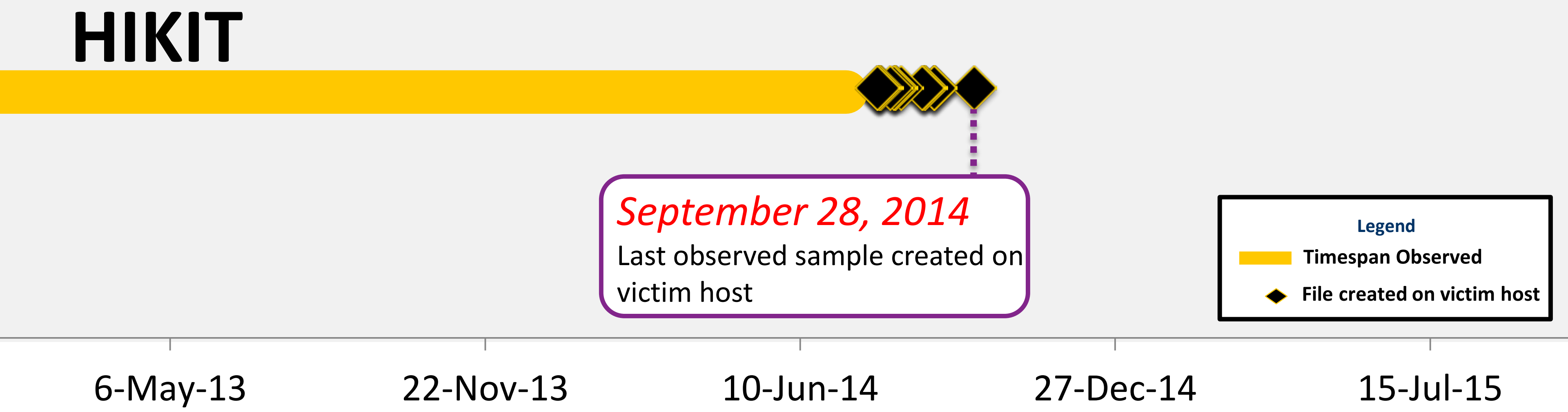


August 2014

Last observed HIKIT compile date

Before and After Operation SMN

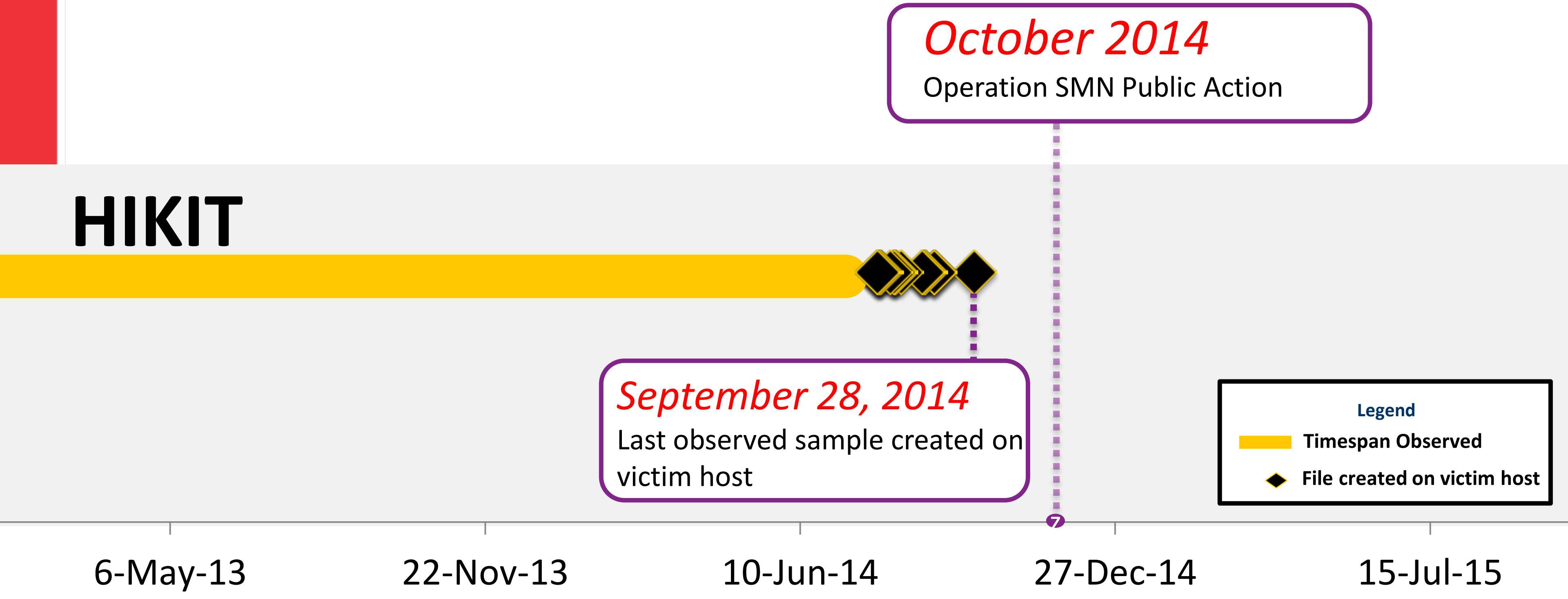
APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda



September 28, 2014
Last observed sample created on victim host

Before and After Operation SMN

APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda



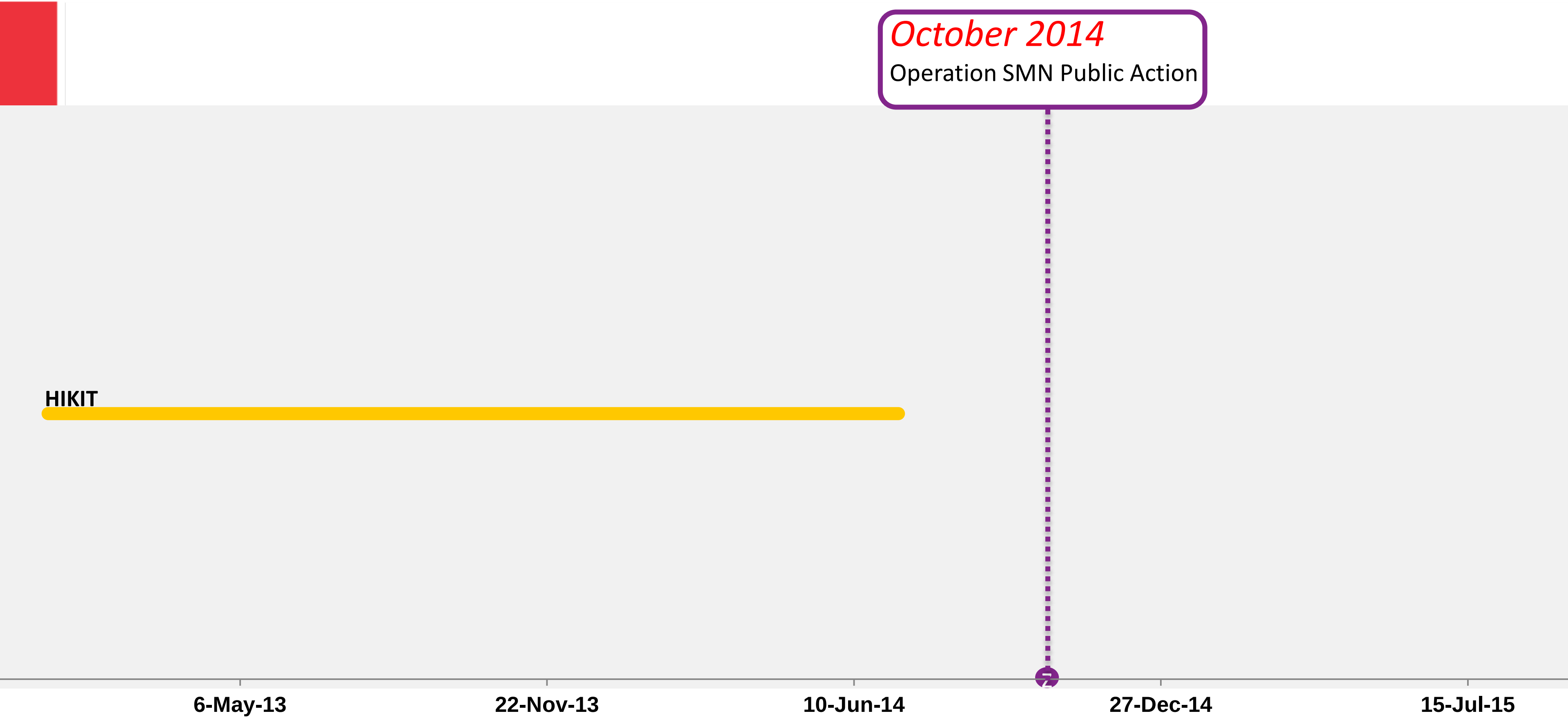
October 2014

Operation SMN Public Action

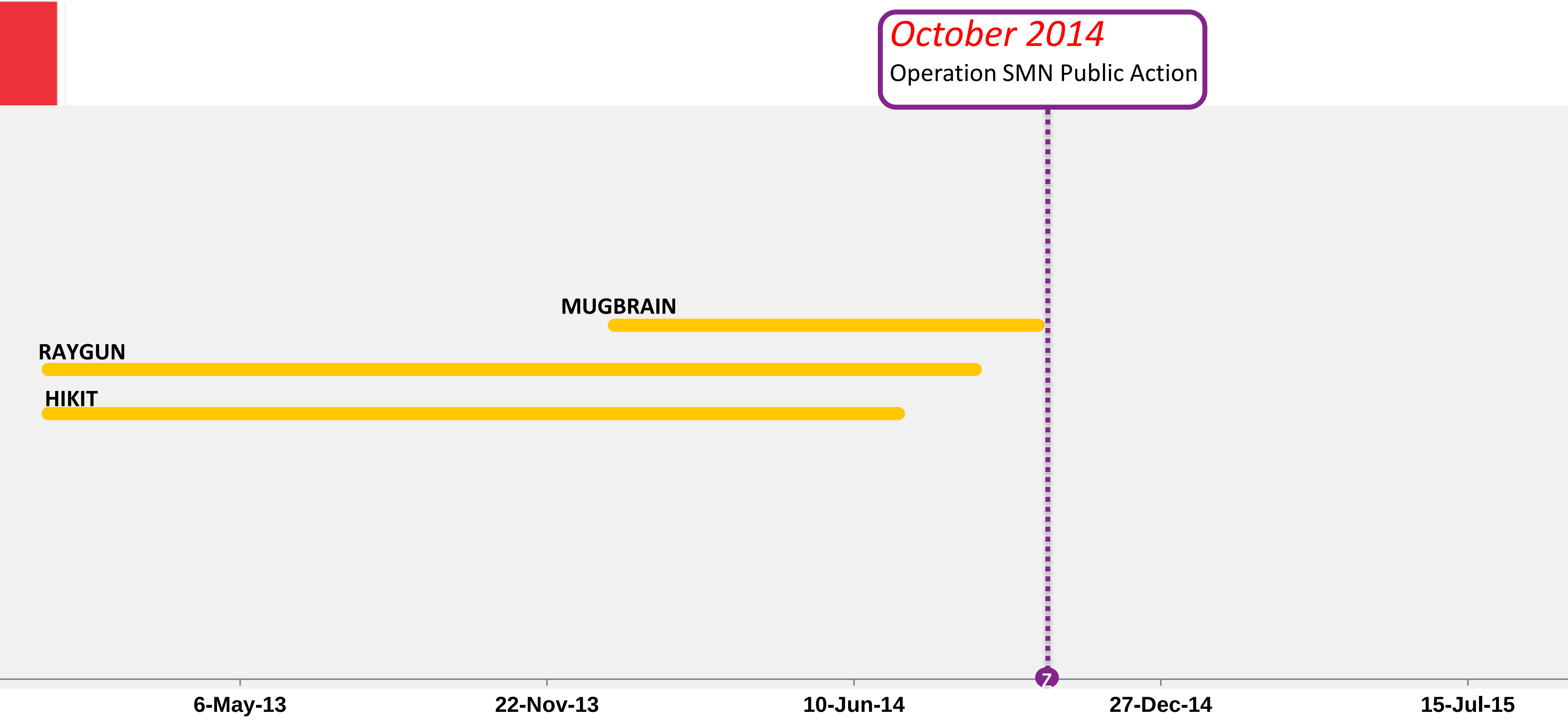
September 28, 2014

Last observed sample created on victim host

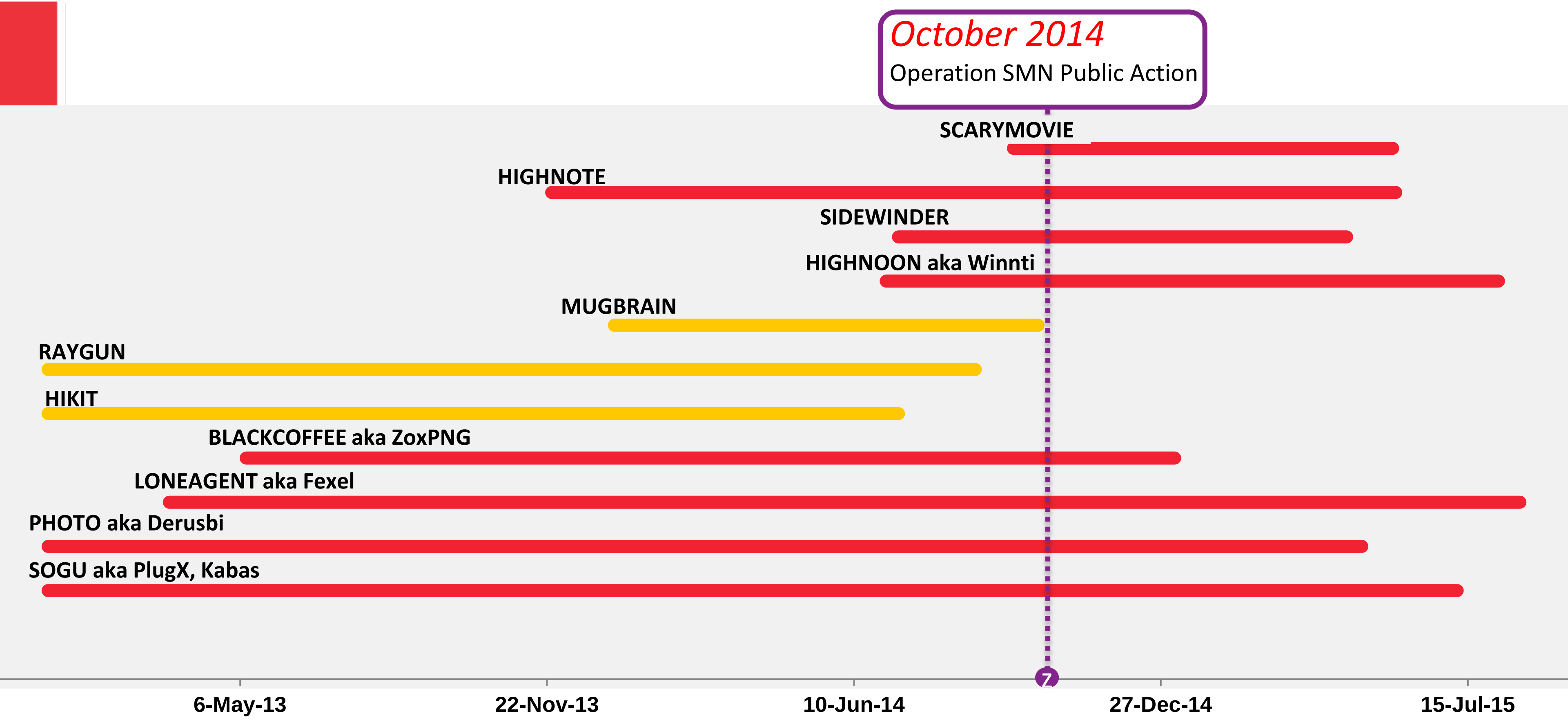
Before and After Operation SMN



Before and After Operation SMN



Before and After Operation SMN

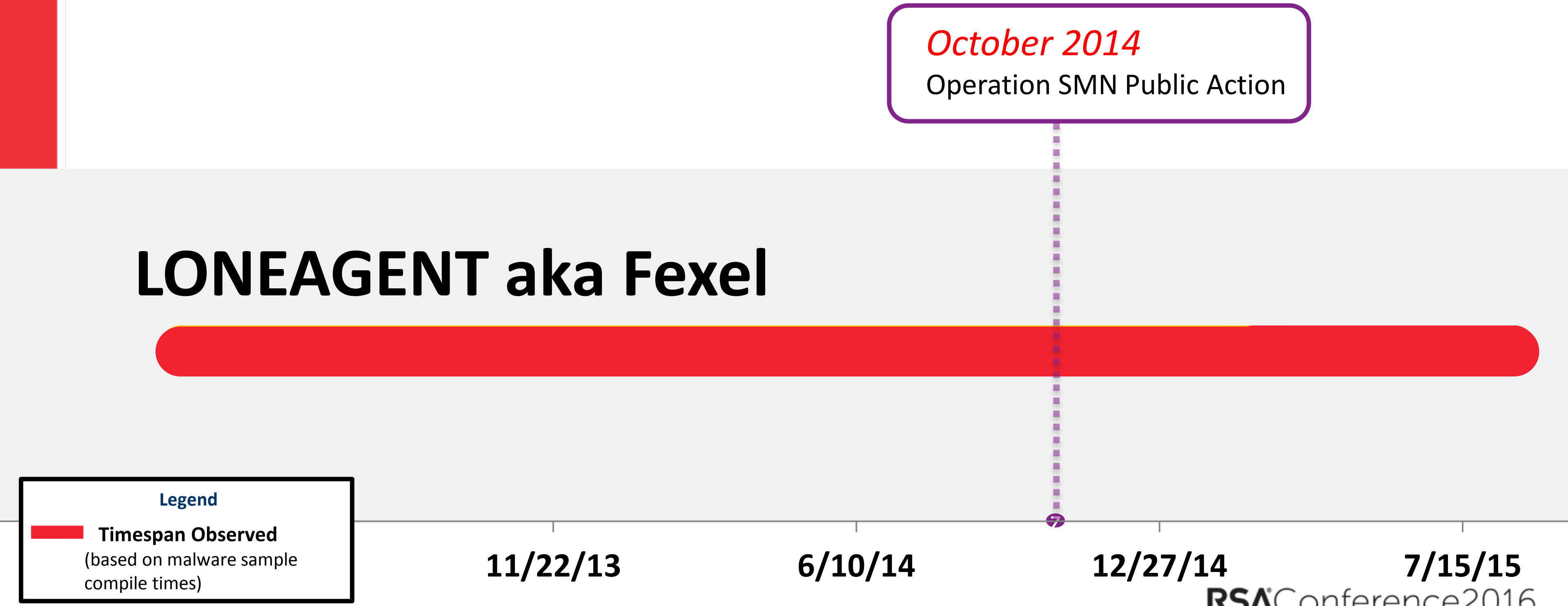


October 2014

Operation SMN Public Action

Before and After Operation SMN

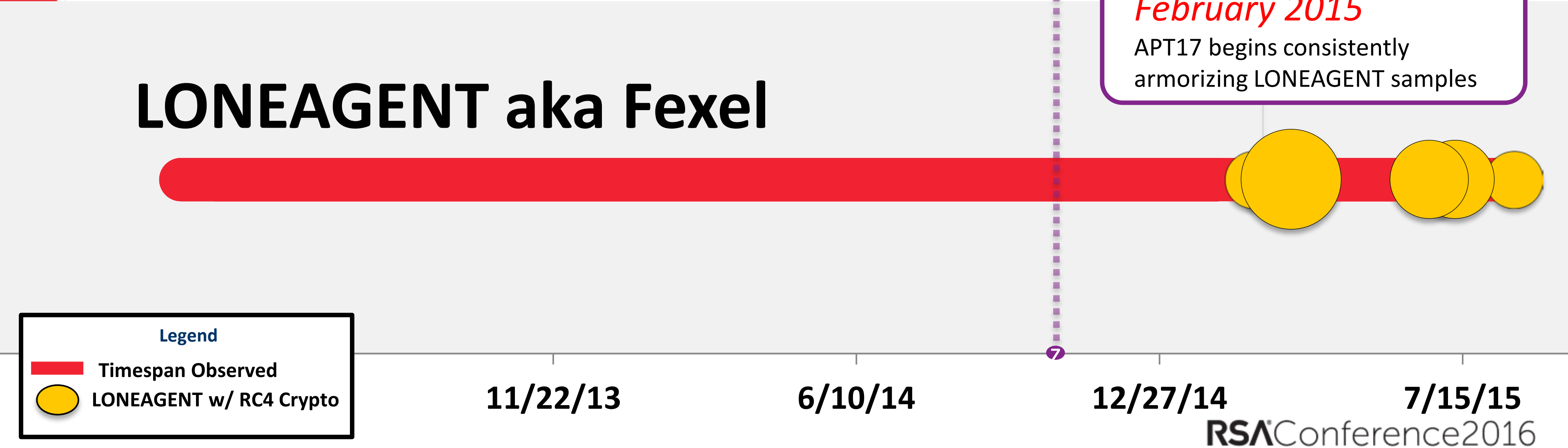
APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda



October 2014
Operation SMN Public Action

Before and After Operation SMN

APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda



October 2014
Operation SMN Public Action

February 2015
APT17 begins consistently armorizing LONEAGENT samples

Before and After Operation SMN

APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda

Quick retooling and adaptation

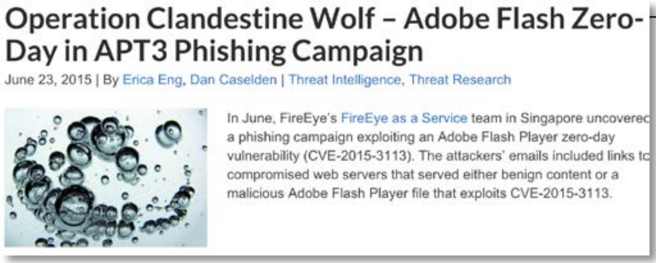
As part of retooling, threat actors can turn on a dime

APT3 Modifies Attack Following Release of Operation Clandestine Wolf

APT3 aka UPS, Gothic Panda

Clandestine Wolf Blog

June 23, 2015



Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign

June 23, 2015 | By Erica Eng, Dan Caselden | Threat Intelligence, Threat Research

In June, FireEye's FireEye as a Service team in Singapore uncoverec a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links tc compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113.

One Day Later

APT3 continued, with modifications:

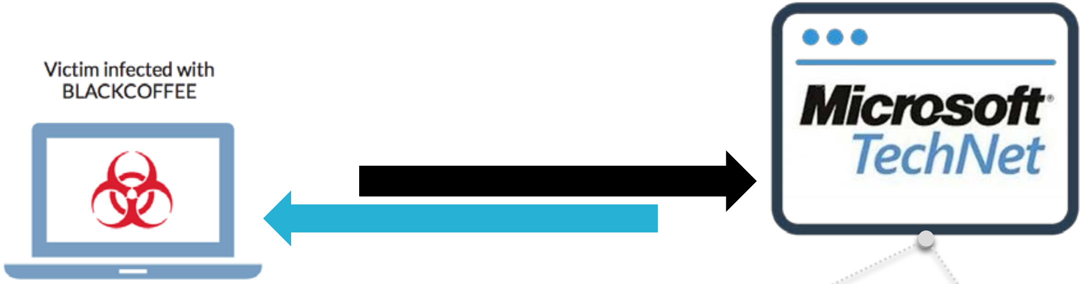
- Created new phishing emails
- Removed mechanism to profile end user systems
- Modified filenames of files used for exploitation
- Altered shellcode
- Compiled new payloads with updated C2; increased obfuscation

The path of least resistance rules.

“If it ain’t broke, don’t fix it.”

APT17: Hiding in Plain Sight Redux

APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda



C2 Location

“@MICR0S0FT” <encoded C2 location> “C0RP0RATI0N”

May 2015
FireEye and Microsoft coordinate takedown of BLACKCOFFEE Technet abuse; Report technique publicly

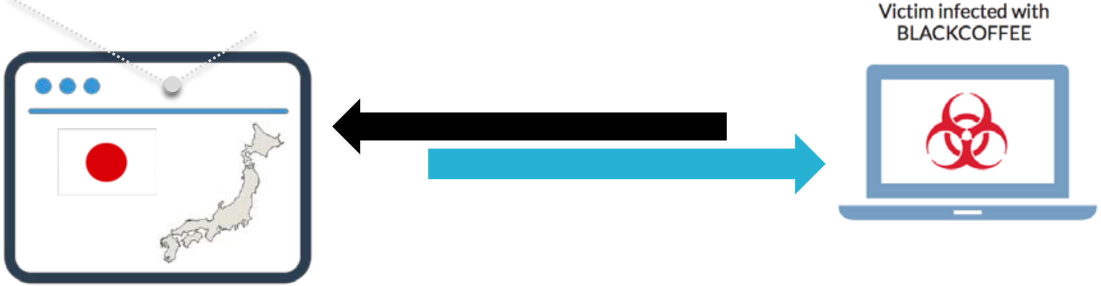
APT17: Hiding in Plain Sight Redux

APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda

August 2015:
Modified BLACKCOFFEE variant targeting JP organizations

C2 Location

“l0ve y0u 4 eveR" <encoded C2 location> "Reve 4 u0y ev0l”



When needed, threat actors will add more resources to get the job done

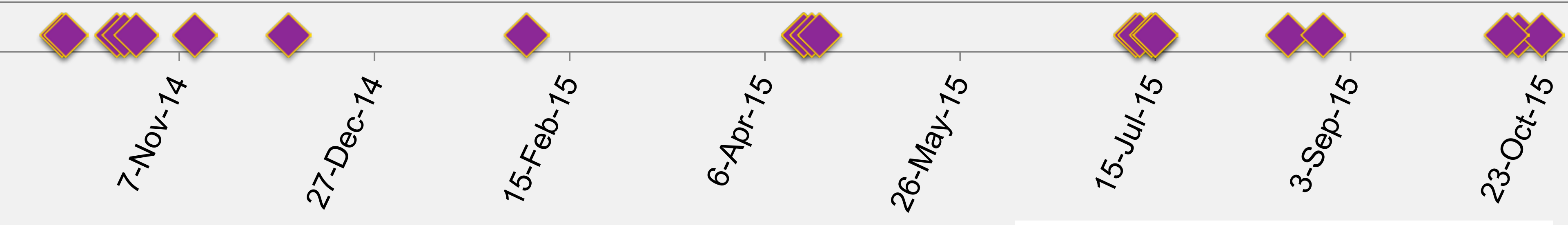
APT28: Keep on Truckin’

APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

20+

Reports examining APT28 TTPS

Oct. 2014 – Oct. 2015

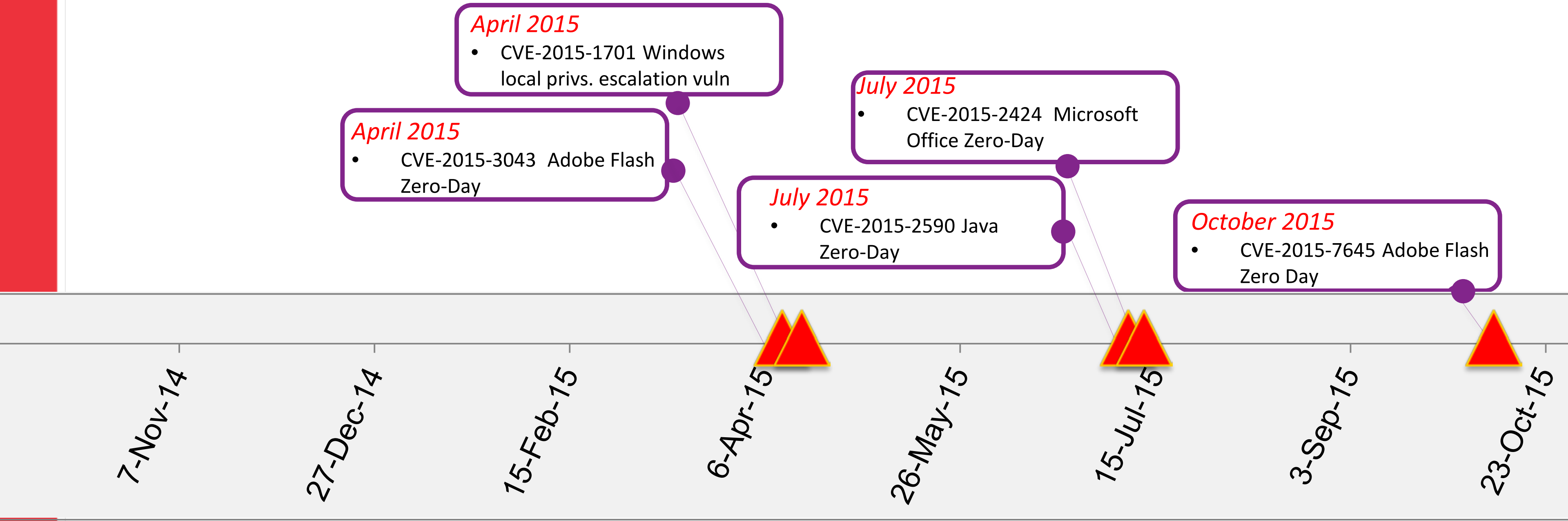


Timeline of APT28 Exposures

◆ Public report examining APT28’s operations

APT28: Keep on Truckin’

APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium



April 2015
- CVE-2015-1701 Windows local privs. escalation vuln

April 2015
- CVE-2015-3043 Adobe Flash Zero-Day

July 2015
- CVE-2015-2424 Microsoft Office Zero-Day

July 2015
- CVE-2015-2590 Java Zero-Day

October 2015
- CVE-2015-7645 Adobe Flash Zero Day

Timeline of APT28 Exposures

▲ Zero Day

APT28: Keep on Truckin'

APT28 aka Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium

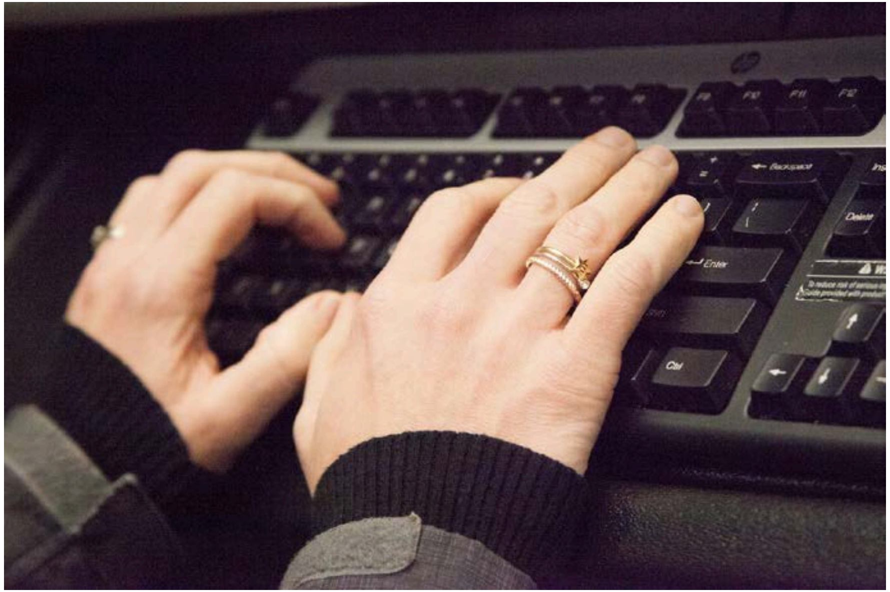


Image Source: Wellness GM @wellness_photos on Flickr

APT28 continues to develop new tools

- March 2015: new variant of **CORESHELL**
- Dec. 2015: New **Backdoor**
- Jan. 2016: New **Launcher**

In Summary…

Key Takeaways

- Threat actors are often keenly aware of reporting on their operations
- Exposure can disrupt an actor's operations… if the incentives are right.
- Public reporting triggers retooling
  - Actors may abandon tools or develop new ones.
  - The path of least resistance is often king.
- Sometimes, actors solve the problem by adding resources: time, money, tool development

Hide and Seek: How Threat Actors Respond in the Face of Public Exposure

Exposure is a balancing act

Security researchers must continually weigh the benefits of public awareness against possible disruptions to detection and loss of visibility.

When executed well, exposure benefits victims, network defenders and the security community at large.

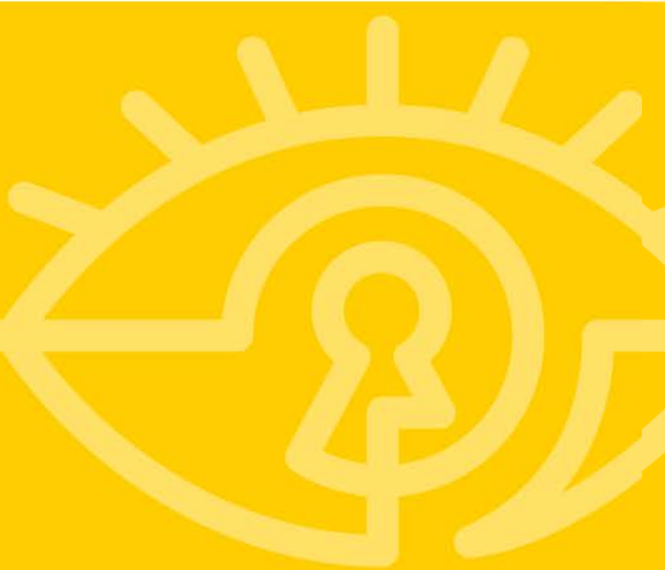
Questions to Ask

When evaluating whether exposing an adversary is the best course of action:

- What impact do we want to have on the adversary?
- How will exposure help/hurt victims and likely future targets?
- How will exposure impact 'big picture' concerns like law enforcement efforts?
- Will exposure degrade our ability to detect and respond to future activity?

When evaluating how a threat actor will likely respond when their operations are exposed:

- How adaptive and capable is the group?
  - Groups with a flat toolset and low adaptive capability are more likely to be disrupted
- How determined are they to maintain access to specific targets?
- What shifts to targeting, timing, resourcing & TTPs is the actor likely to make?



Thank you