Respond Before Incident

Building proactive APT defense capabilities (Public Version)

TEAM T5
Cyber Security Research

Sung-Ting Tsai (TT), Chen-yu Dai (GD)

Dec 2017

Agenda

- Introduction
  - Popular cyber attack countermeasures
  - Evolution of cyber incident handling
  - Traditional incident handling challenges
  - Ideal CSIRT Resource Allocation
- Story of a long-term NPO victim
  - Original Compromised Situation
  - Attack campaigns and TTPs
  - Effective Mitigation Cycle
- Proactive Defense How-to
  - Situation Awareness & Visibility Building
  - Proactive Internal Visibility: Threat Hunting
  - External Situation Awareness: Threat Intelligence
  - Intelligence-driven Proactive Defense
- Threat Hunting In-action
  - Network-based & Host-based Threat Hunting
  - Detecting abnormalities via Modeling
  - Prioritizing with Threat Intelligence
  - Intelligence-driven Threat Hunting Cycle
- Conclusion: Be Proactive

Sung-ting Tsai (TT)

CEO at Team T5 Inc.

- Frequent Black Hat / hacker conference speaker
- Vulnerability researcher and owner of several CVE ID
- 10+ years on security product development
- 8+ years experience on cyber threat research
- Organizer of HITCON

✉ tt@teamt5.org

Chen-yu Dai (GD)

CTO & CSIRT Lead

- Digital Forensics & Incident Response background.
- Development of Threat Intel Platform and IR tools.
- Hacks in Taiwan Conference (HITCON) committee.
- Spoke at some conferences, played some CTF.

✉ gd@teamt5.org

✉

Introduction

TEAM T5
Cyber Security Research

Popular cyber attack countermeasures

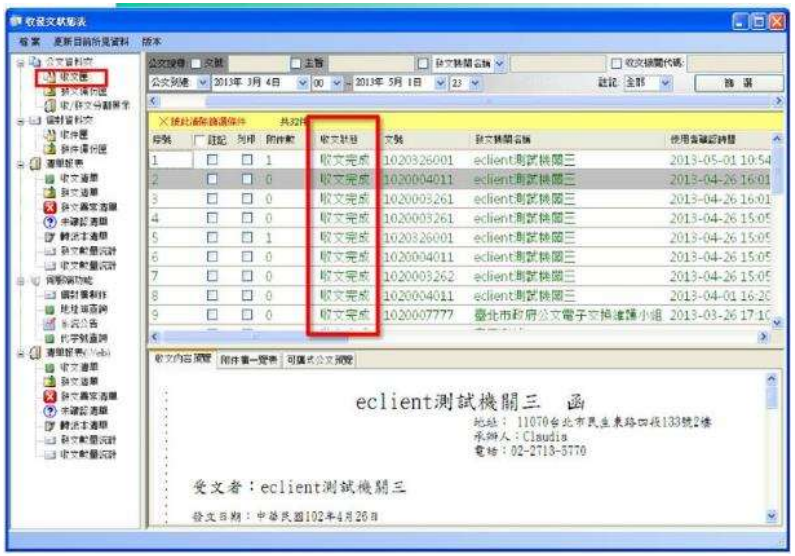
Network-exploit & Opportunistic → Endpoint-exploit & Targeted

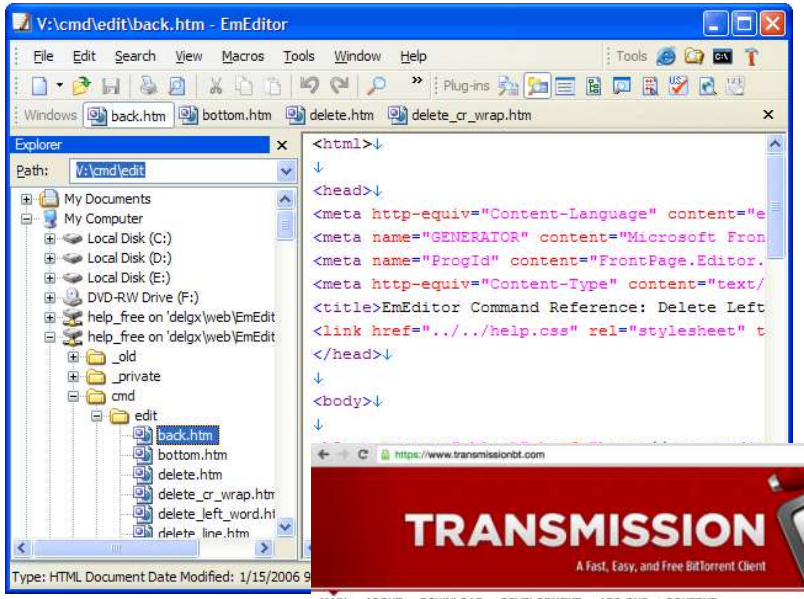
Password Login	Malware	Vulnerability / Worm	Drive-by Download	Email Phishing	Supply Chain
80″	90″	2000″	2005″	2010″	2015″
Firewall	Antivirus	IDS / IPS	UTM / NGFW	Sandbox	EDR / UEBA

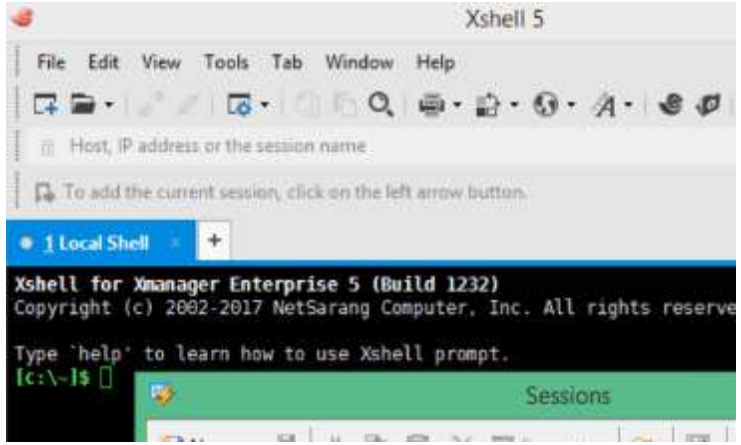




Supply Chain Attacks

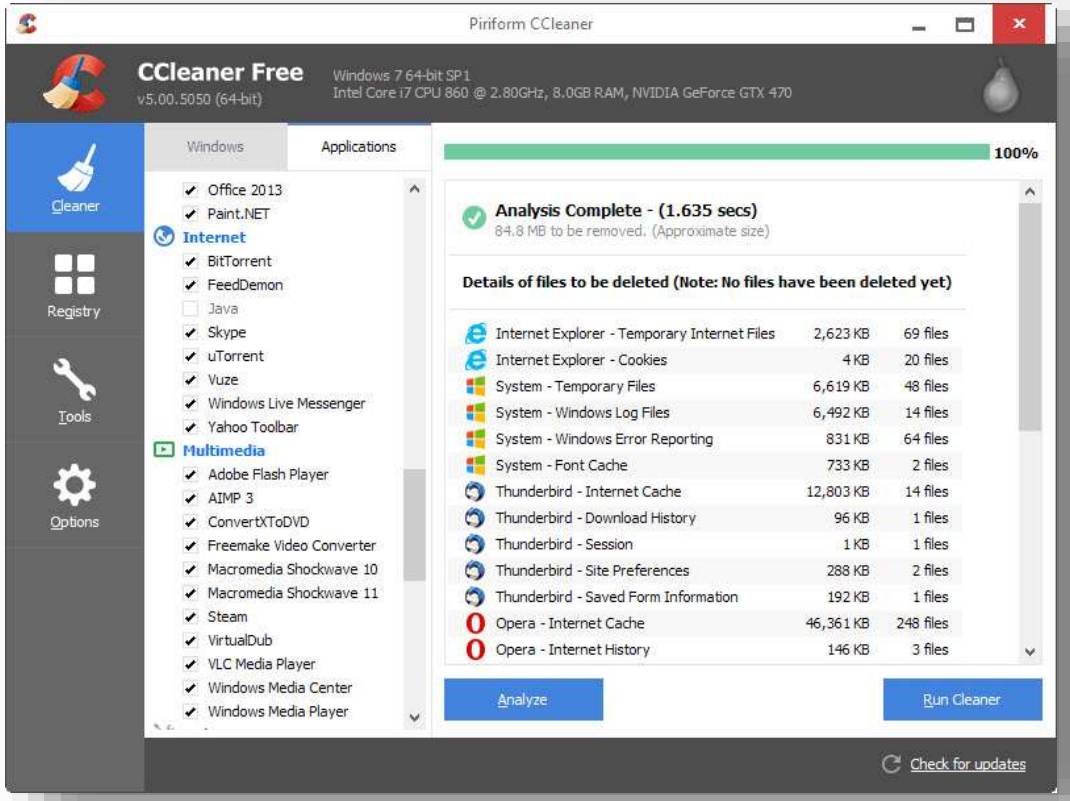






2017-08 CCleaner Incident

- Famous system clean-up software
- Official website trojanized for 1 month
  2 million user download and infected
- Only targeted user will received
  2nd stage RAT from github, wordpress
- Targets: Intel, Google, Microsoft, Akamai, Sony, Samsung, Vmware, HTC, Linksys, D-Link, Cisco
- Kaspersky: similar to APT17 base64



http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html
https://blog.avast.com/avast-threat-labs-analysis-of-ccleaner-incident

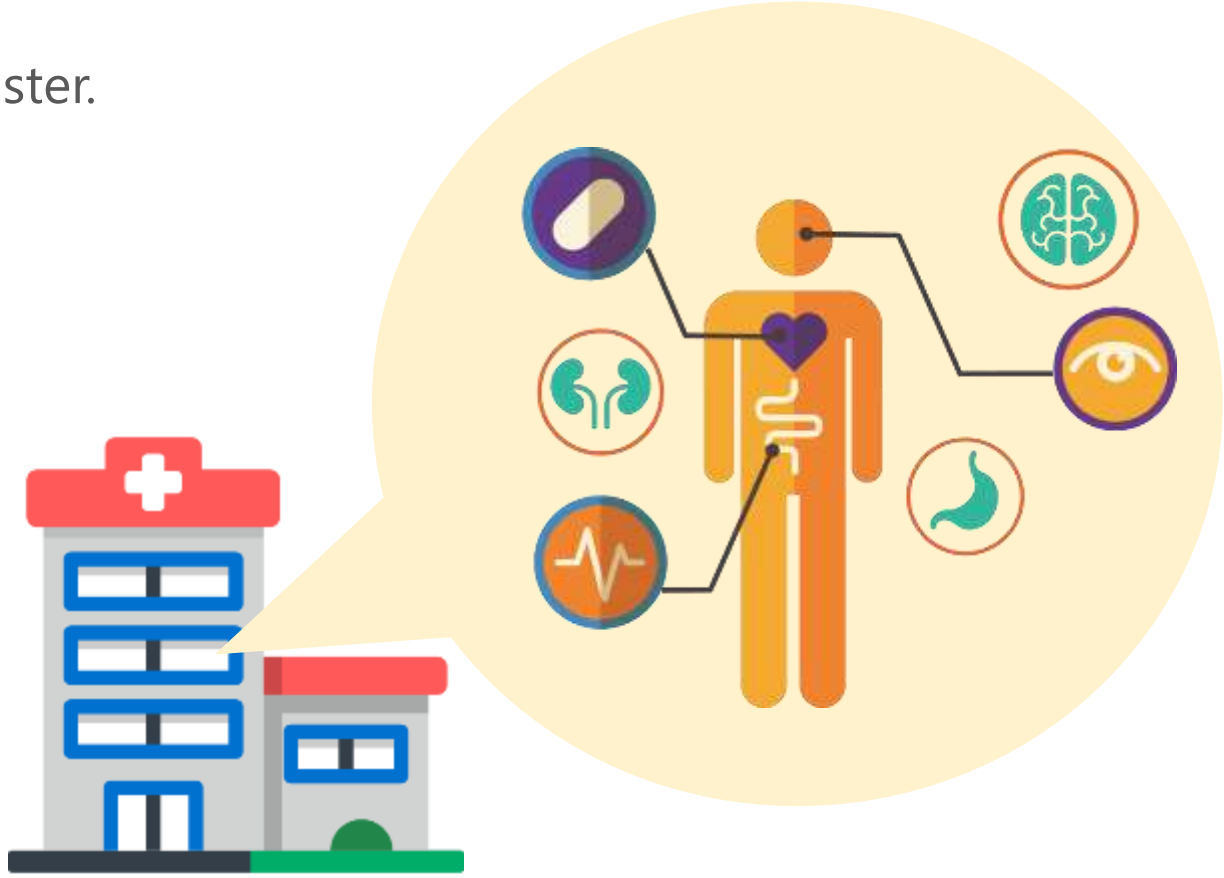
All Existing Countermeasures Failed

- Every vendor thinks it's false positive
  - Digitally Signed by CCleaner vendor
  - Parent company is Avast antivirus
- Host-based signature delayed 1m
  - 2017-08-15 CCleaner trojanized
  - 2017-09-14 ClamAV add signature
  - 2017-09-18 Cisco Blogged, only 10 detects
- Network-based traffic is encrypted
  - RAT payload on https://github.com , https://wordpress.com
  - Even if you decrypts HTTPS, malware command is normal blog search

2017-08-17 09:00:38	0/65	Antiy-AVL	-	3.0.0.1	20170816
2017-08-16 12:50:22	0/65	Arcabit	-	1.0.0.817	20170816
2017-08-16 09:16:58	0/65	Avast	-	17.5.3585.0	20170816
2017-08-16 09:14:22	0/64	AVG	-	8.0.1489.320	20170816
2017-08-16 07:19:54	0/65	Avira	-	8.3.3.4	20170816
2017-08-16 07:09:07	0/63	AVware	-	1.5.0.42	20170816
2017-08-16 05:59:55	0/64	Baidu	-	1.0.0.2	20170816
2017-08-16 04:35:30	0/63	BitDefender	-	7.2	20170816
2017-08-15 21:01:42	0/64	Bkav	-	1.3.0.9282	20170816
2017-08-15 20:00:53	0/64	CAT-QuickHeal	-	14.00	20170816
		ClamAV	-	0.99.2.0	20170816
		CMC	-	1.1.0.977	20170816
		Comodo	-	27612	20170816
		CrowdStrike	-	1.0	20170804
		Cylance	-	2.3.1.101	20170816
		Cyren	-	5.4.30.7	20170816

“You will eventually be pwned” mindset

- Every human got sick eventually
  - Nobody never get sick.
  - Flu is not a big risk if you can recover fast.
  - Exercise your body every day to recover faster.
- Systems eventually got compromised.
  - 100% Blocking is difficult.
  - Detect early, recovery faster.
  - Periodically health checks
- Hunt for unknown threats!



Evolution of cyber incident handling

Digital Forensics → Incident Response → Proactive Incident Handling

Disk Forensics

1997

Memory Forensics

2001

Private CSIRT

2005

Stuxnet / APT

2010

Remote Forensics EDR

2013

Threat Hunting

2016

1999

Network Forensics

2003

National CERT

2007

SIEM, SOC, MSSP

2011

Threat Intelligence

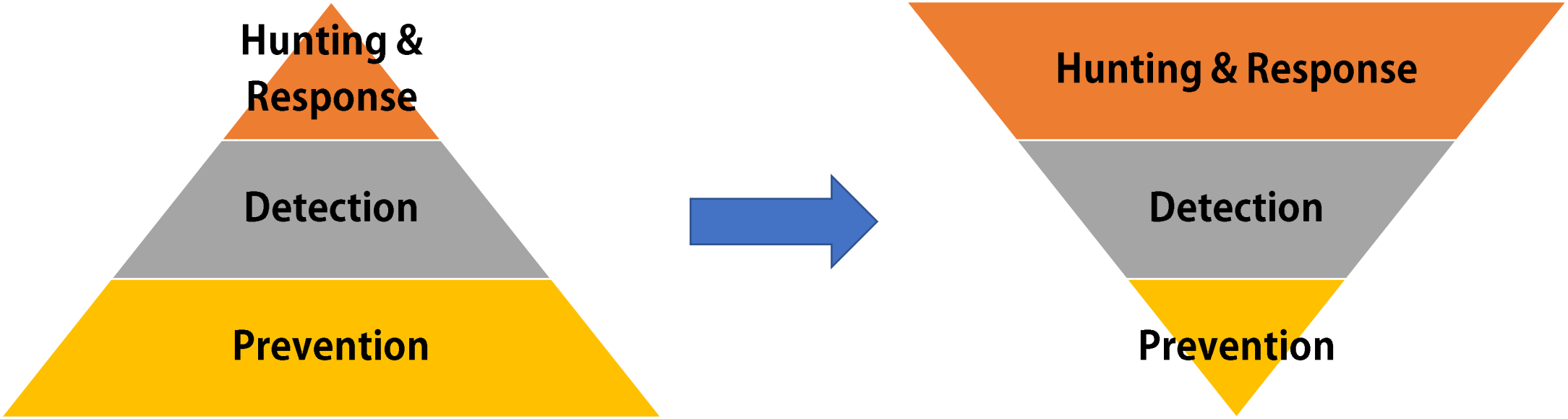
2015

Orchestration

Traditional Incident Handling Challenges

	Traditional CSIRT	Ideal Proactive CSIRT
Incoming Data	Large quantity false alarms	Alarms categorized and prioritized
Staff duty	Overwhelming work-loads	Time to research and tracking
Routine Jobs	Call-center like response Solving incoming tickets	Discovering abnormalities Patrolling Constituency
Event Systems	Separated Vendor-silos Human apply settings	Automated orchestration Playbook and self-remediation
Response System	Various tools fragile reports	Integrated reporting

Ideal CSIRT Resource Allocation



Current Majority Organizations

Ideal Proactive Organizations

Story of a long-term NPO Target

TEAM T5
Cyber Security Research

Background - The Attractive Target

- A research NPO in Taiwan
- 500~1000 PC and servers
- Most users are autonomous and difficult to regulate
  - Researchers
  - Professors
- IT budge: Pretty Limited, rsyslog on a few servers
- Network visibility: NAT built-in firewall
- Endpoint visibility: only one antivirus

Q1 Incident Response

- MIS says they
  - Received FW blocking alert everyday
  - Received VPN logon notification everyday (but don’t know why)
  - Received Antivirus quarantine notification every few days
- Action taken
  - Reinstall the system every time large number of alerts triggered
- What actually happened
  - Attacker compromised director, IT manager, RD system and installed backdoors.

Q1 Incident Response

- Critical servers were controlled by attackers for a long time
  - HR and ERP system: database leaked.
  - AD server: Distributed malware with GPO. Credentials dumped.
  - Office Scan server: Signature update was replaced with malware.
  - Exchange server: Credentials leaked. Attackers were able to login OWA.
  - Web server: Web app upload webshell, compromised for a long time.

Q2 Mitigation Plans

- Multi-Layered defense reinforcement
  - Install Email sandbox, IPS, WAF etc
  - Deploy full packet recording and EDR
- Exam the effectiveness of current security solution.
  - Check all system anti-virus works?
  - Write more rules on firewall
- Fusing internal and external intelligence
  - Create Case management SOP
  - Block C2 from previous incidents to firewall

Q3 Strategic Planning

- Applied our mitigation defense cycle
- Helped to monitor and responds. Incidents decrease 95% in 3 months.

Results

- Daily compromise assessment scanning.
- Responding to attacks promptly.
- Less spear-phishing emails.
- Attacker shifted TTP
  - target web server
  - cracking VPN
  - exchange OWA password

Proactive Defense How-to

TEAM T5
Cyber Security Research

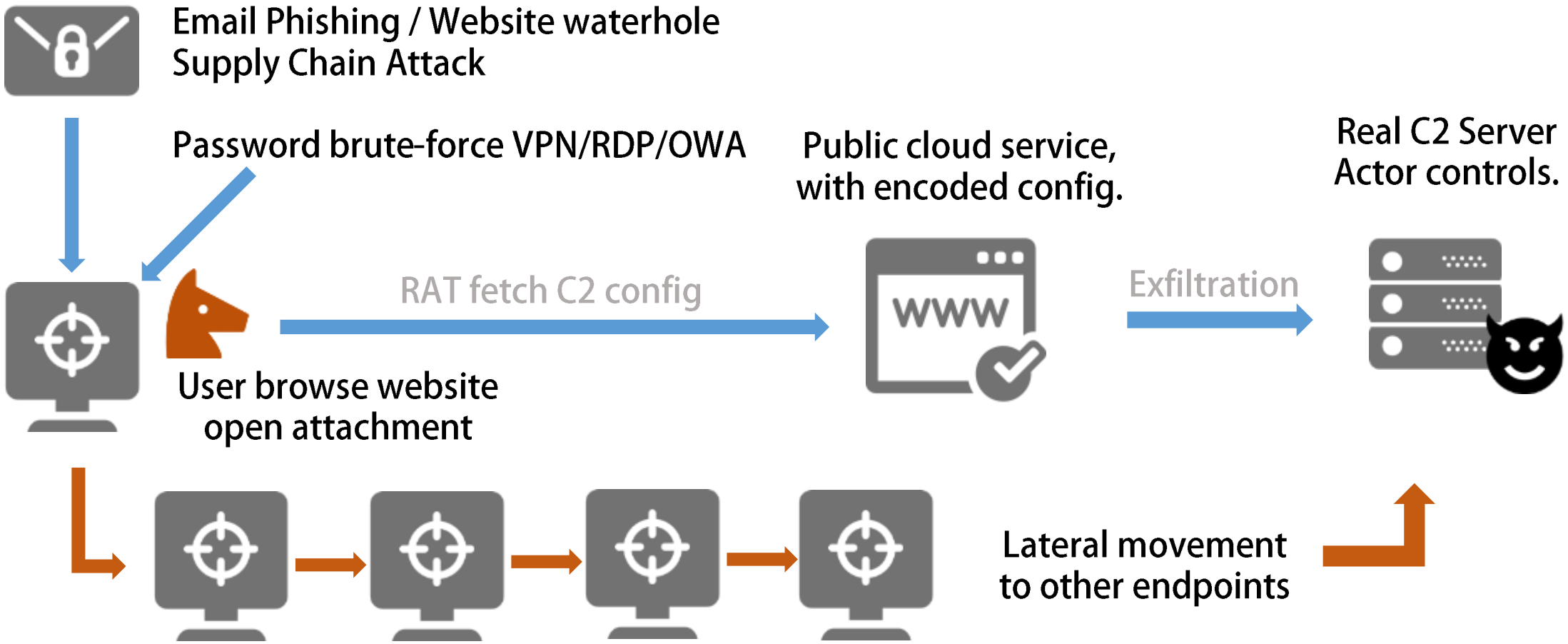
Visibility Building & Situation Awareness

- Visibility is surveillance camera on all corners of your constituency
  - Critical Data, Users, Assets, Network, Backup Plan, Physical Location
- Situation Awareness is knowing “what happened” all the time
  - Know what to know, too much information is no information.

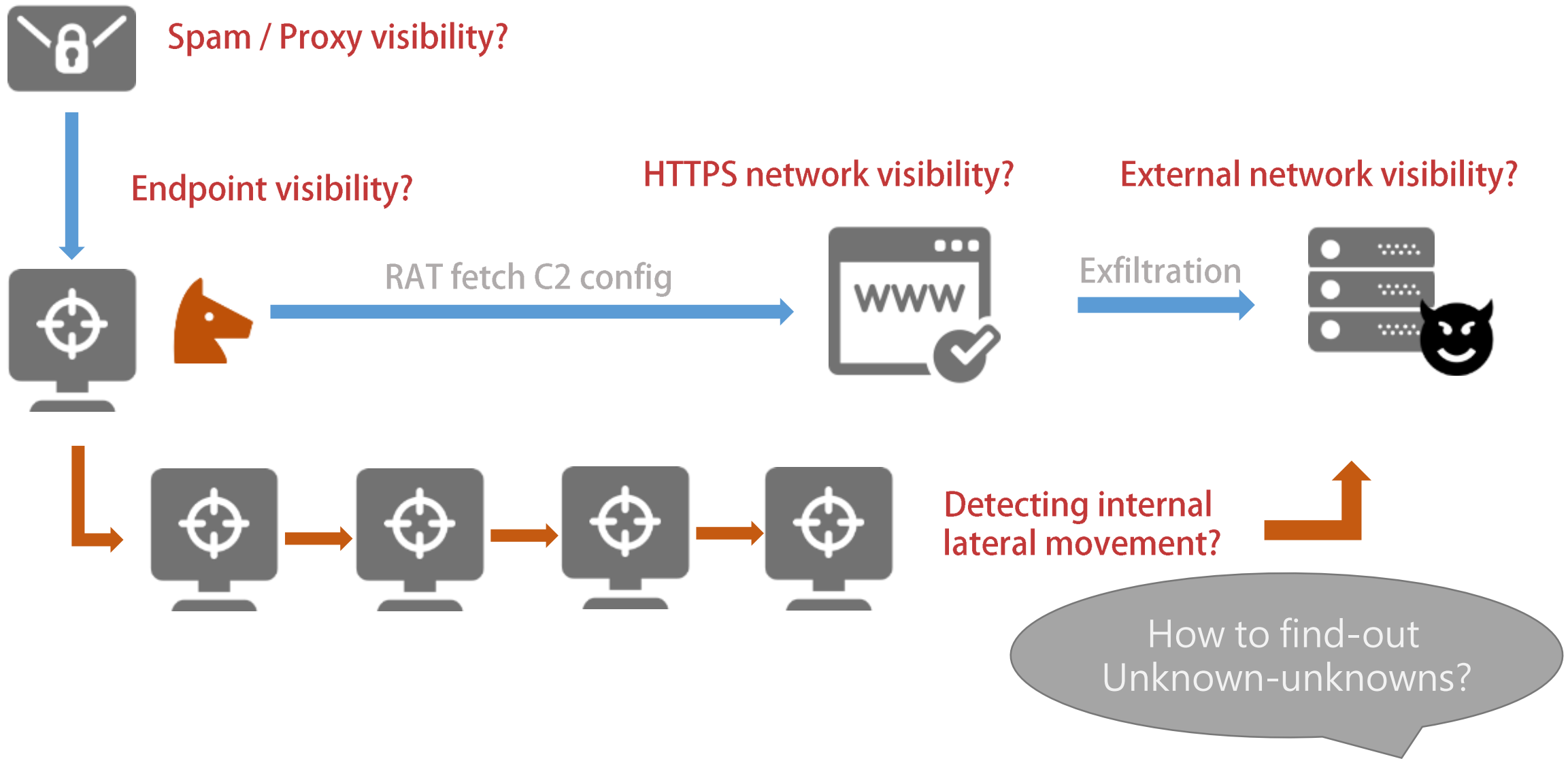
External Situation: Sight, cloud, weather, wind speed outside?

Internal Situation: Navigation, radio, engine speed dashboard?

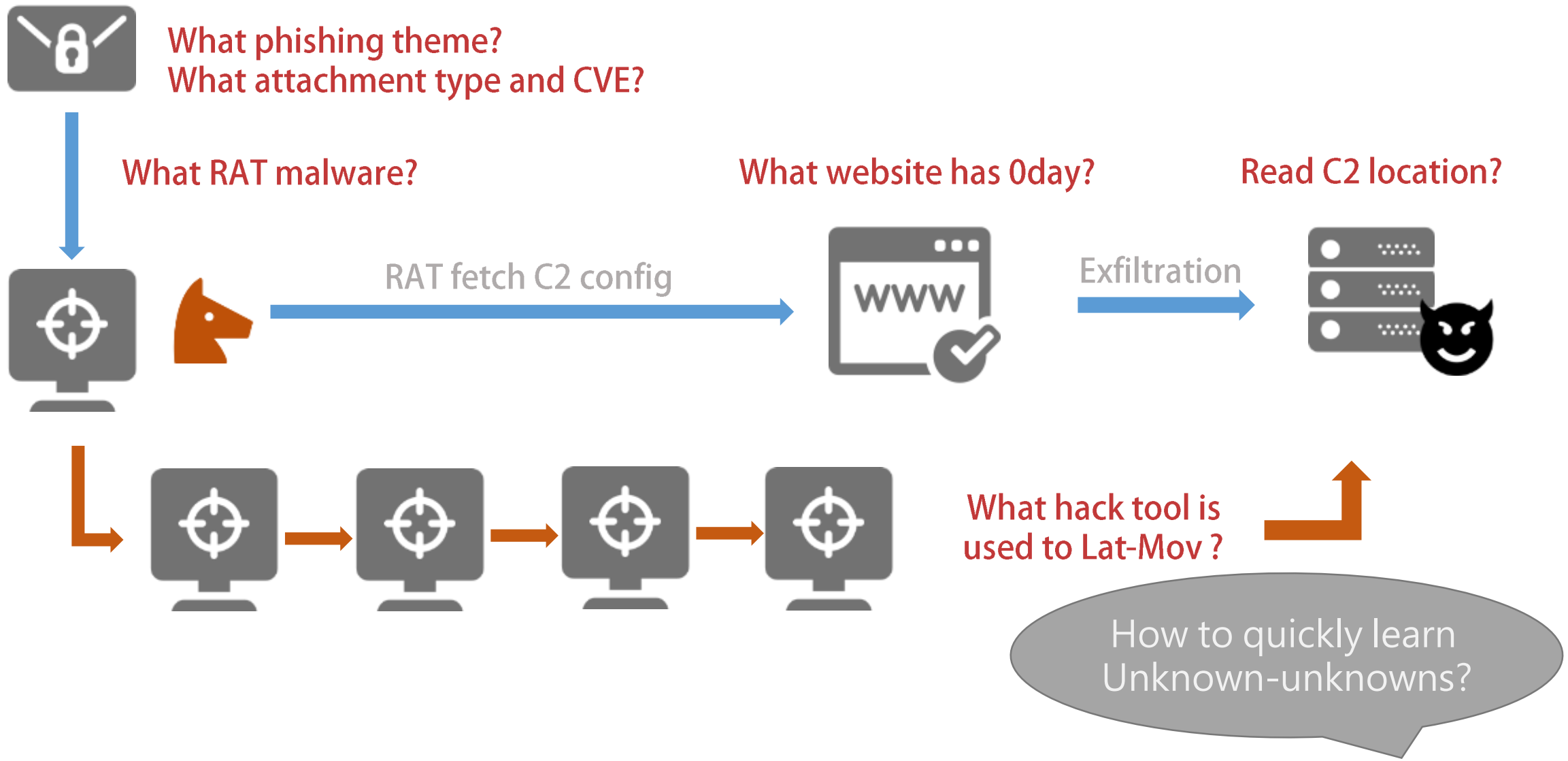
Typical Targeted Attack TTP



Proactive Internal Visibility: Threat Hunting

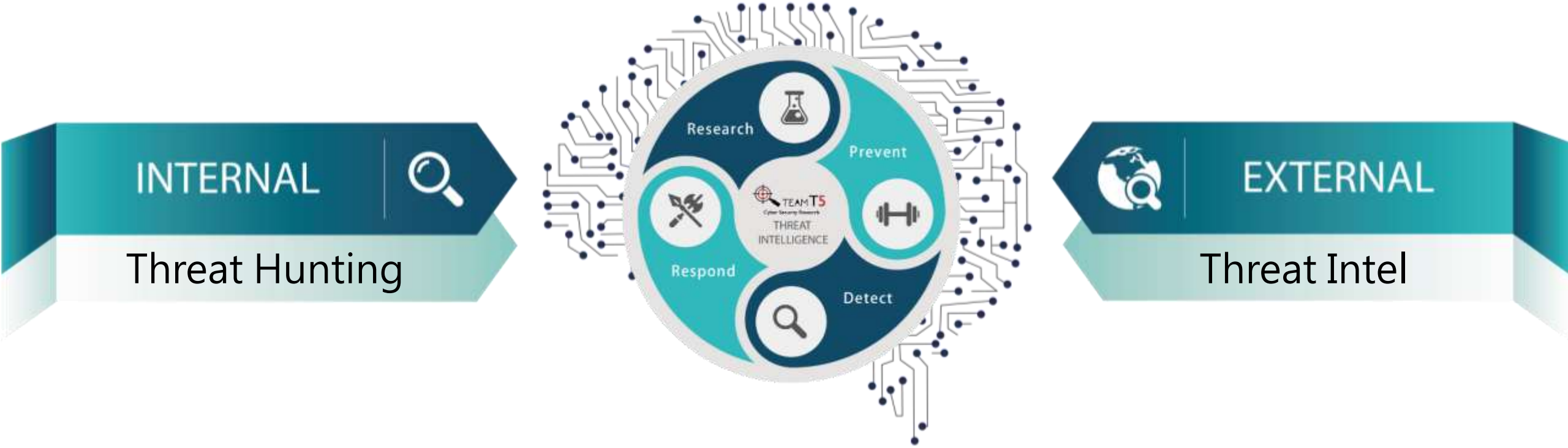


Ext. Situation Awareness: Threat Intelligence



Internal Visibility + External Awareness

Intelligence Platform



Proactive Defense Cycle

Combining Threat Hunting + Threat Intelligence

Experienced Analyst
Reverse Engineer
Co-relate Intel Report

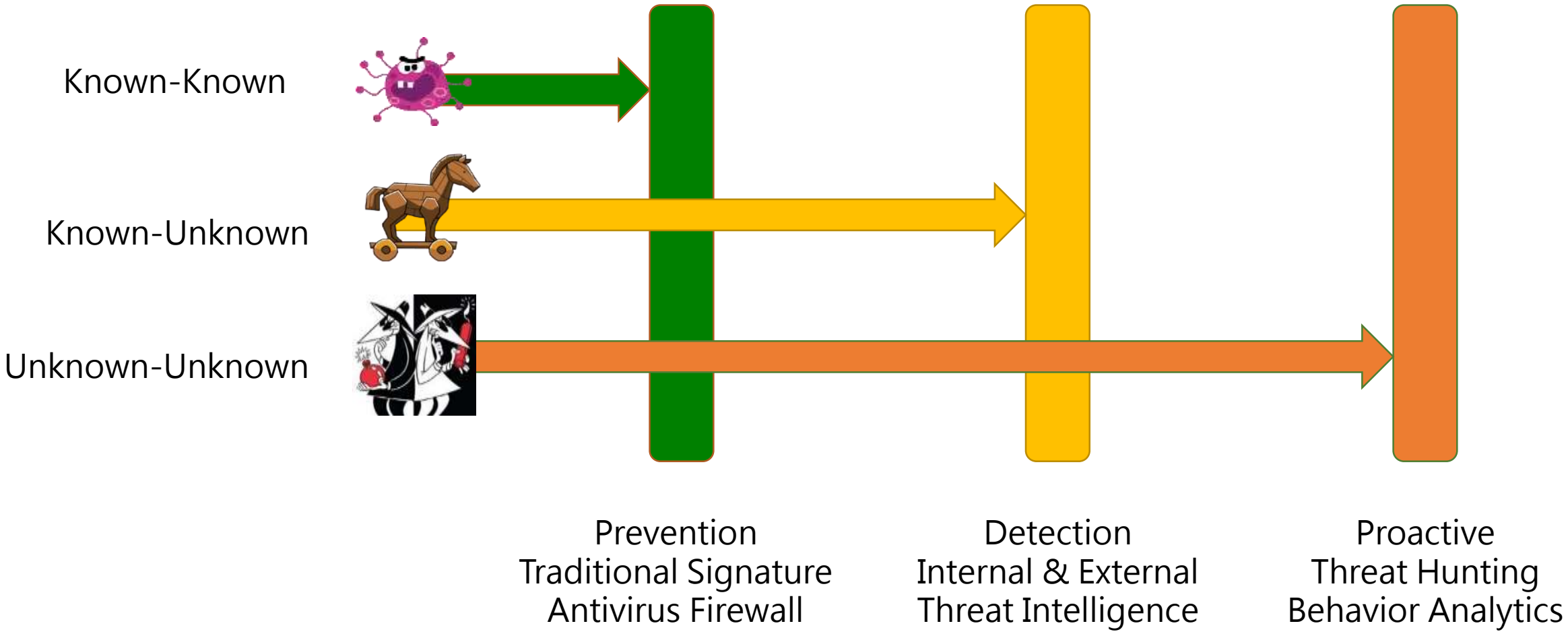
Understand Trends
Industry Common
Attack Surface

Intel Platform

Incident Forensics
Traces of 0day
Quick triage

C2 Blacklist
Social Engineering
Malware signature

Multi-Layer Defense Strategy



Threat Hunting In-action

TEAM T5
Cyber Security Research

2 Threat Hunting Types

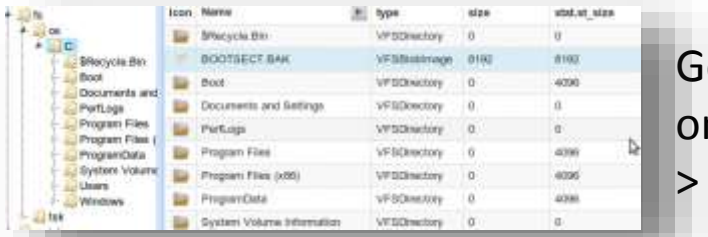
- Network-based Hunting
  - Target: C&C channel, lateral movement, data exfiltration
  - Monitor: Firewall, IPS, Proxy, NAT, Moloch, etc
  - Outliers: packet with most outbound IP, longest, largest amount?
  - Easy to scale-up, can search 10000 endpoint connection logs.

- Host-based Hunting
  - Target: Compromised system, host, device
  - Monitor: Process, File, Service, MBR, Registry, Eventlog, etc
  - Outliers: Hidden process, Unique artifacts, Autorun entry, etc
  - Difficult to scale-up without proper tool or hunting platform
  - Application artifacts are more complicated than OS artifacts.

Pivoting: Hypothesis & Ping-Pong

%Temp%\RarSFX1\1.exe looks suspicious dropper,
Is this a ransomware, banking Trojan or APT ?
> Not sure, check network side.

Any suspicious outgoing connection or DNS from this endpoint at the timeframe of alert?
> Yes, one suspicious VPS IP found.



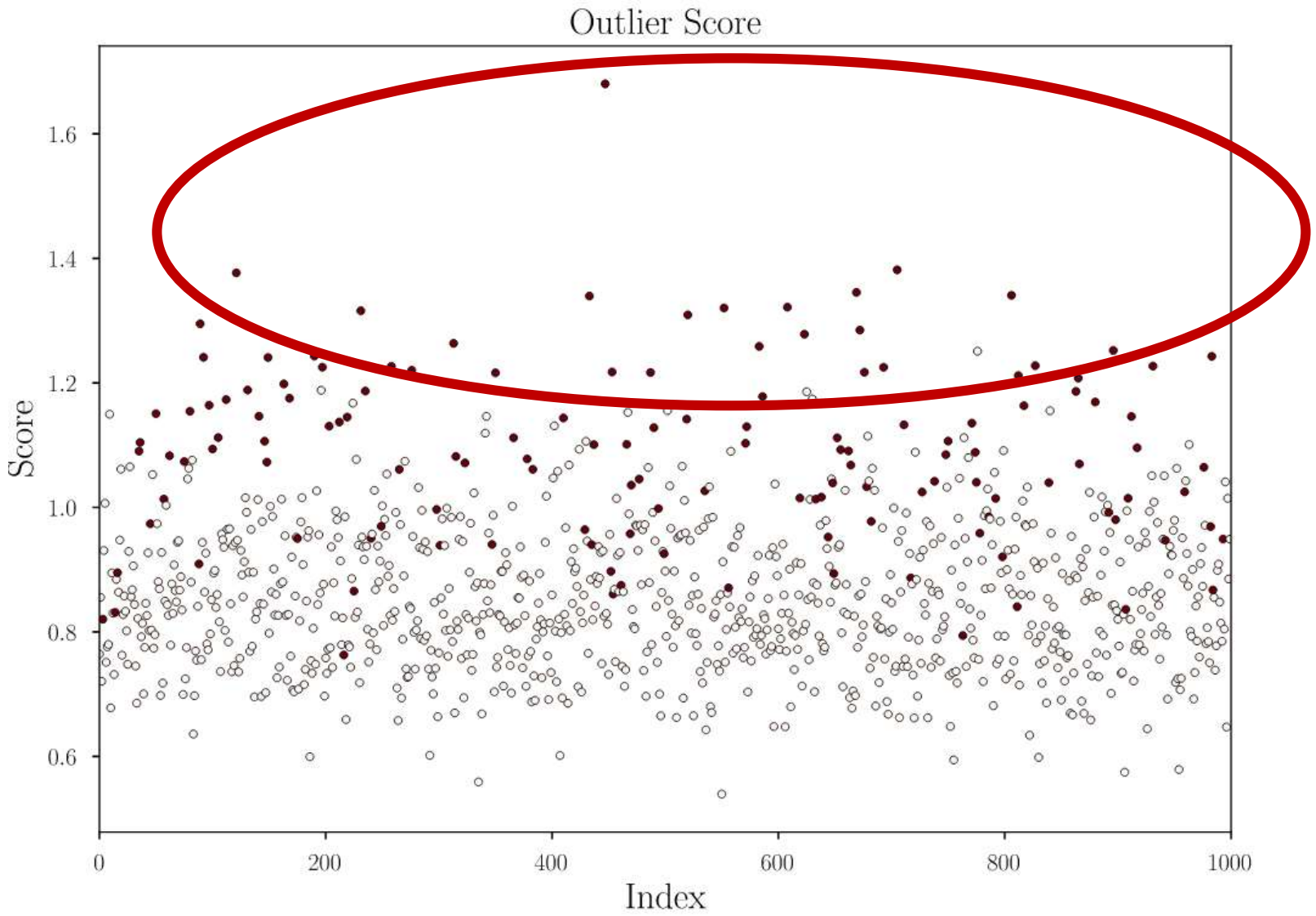
Get me additional logs to build activity timeline on this endpoint using remote forensics tools?
> Yes, this host has been compromised

Is there any other host in my organization connecting to the same IP?
> Yes, please block all of them.

Last 50 firewall log entries. Max(50)

Act	Time	If	Source	Destination
	May 8 21:10:34	WAN	50.88.20.66:4092	89.201.193.170:18724
	May 8 21:10:35	WAN	174.31.156.120:39896	89.201.193.170:18724
	May 8 21:10:35	WAN	209.89.215.71:61227	89.201.193.170:18724
	May 8 21:10:35	WAN	69.224.44.222:62038	89.201.193.170:10000
	May 8 21:10:35	WAN	68.150.135.132:58775	89.201.193.170:18724

Modeling: Find the Outliers.



Host-based Hunting Strategy

- Standalone threats
  - Malware does not try hide itself or hijack other process
  - File name or hash is special, only appears on a few endpoints.

- Masqueraded threats
  - Hiding methods: Loaded using svchost.exe, DLL-Hijacking, etc.
  - Same filename but different in-memory attributes.

- System Forensics
  - EventLogs, Web logs, File system, Startup artifacts
  - File-less threats: PowerShell, WMI Script, In-memory

Hunting standalone threats

- How many version of Office Word is in my organization?
- Which endpoint has a rarely seen Word version?

Name
WINWORD.EXE

Threat level 2

Scan Type
Process

Levels

Max Lv.	
2	73
1	133

Statistics

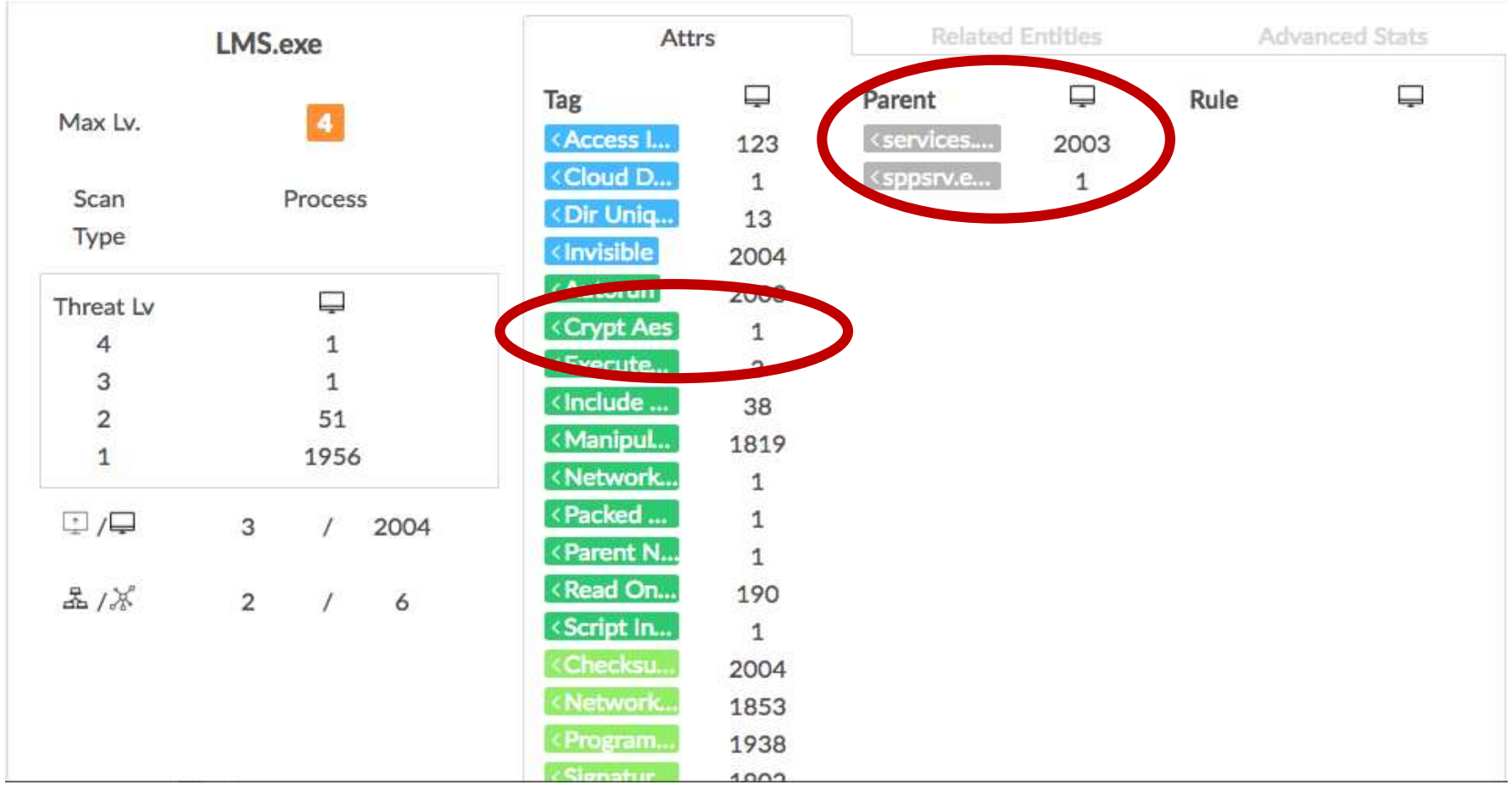
	/	
18	/	206

Alias | Sample | Imp Hash | DLL | Account

SHA256 Hash	VT Count		Size	Time Stamp	
FC7B9D27EF7EC0A899C5E9E4D43786C4B323FB0BE82DCF312043DF2FBD7B5335	0 / 65	VT	1432256	2017-06-04 08:04:00 +0800	97
DC973455AAF8B32E8B69F18D3D17A56DB1513B9797CD0C52E8B1B834CDD92D95	0 / 64	VT	1931960	2017-07-12 00:17:37 +0800	22
DCE38EBA77DADC00A73919CC8A07876FB11ECA9A926C417DB2A5C3381E856FB0	0 / 65	VT	1934008	2017-07-12 01:09:37 +0800	21
D91679CFE64CE511C20A1CF8C33B4FB4E0B92213CB3D2D91DFDA715A178B5E52	0 / 65	VT	1922720	2015-02-18 01:30:28 +0800	7
637D651C8A7EE0183B3AB58F60B7459D4E6826F2026FE78E2C765B349D261D3E	0 / 65	VT	1924768	2015-02-18 02:13:32 +0800	2
61B79E56DEBA03D9854563506822C361427AB13666E3D9507D94F4265F9D997D	0 / 64	VT	1922712	2014-11-12 15:37:30 +0800	2
FB5FF55789A7424D58CD29238911F16CEB5A90206C0B01E45A3619D270D35788	0 / 65	VT	1934008	2017-04-11 23:35:55 +0800	1

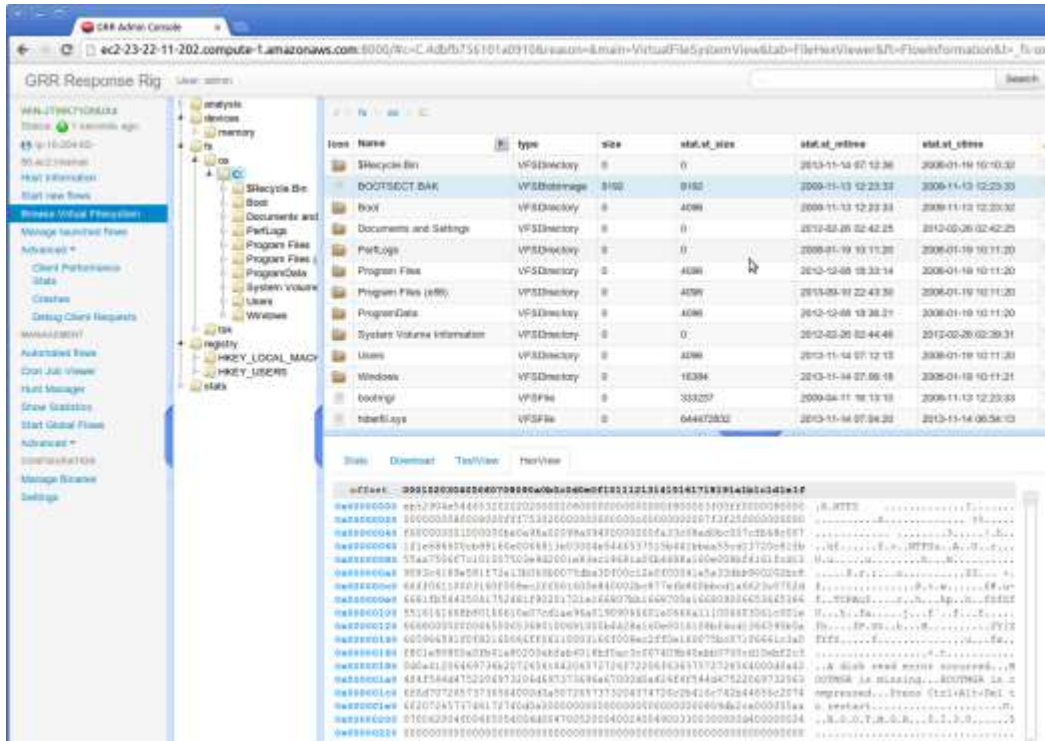
Hunting masqueraded threats

- Who has different parent process than others?
- Why is the intel driver using AES cryptography?



Open-source Host-hunting Tools

- GRR, Google Rapid Response
  - https://github.com/google/grr
  - Powerful but difficult to use
- OsQuery, Facebook Performant Endpoint Visibility
  - https://osquery.io/
  - Generic wmi-like system information access
- LOKI, Simple IOC Scanner
  - https://github.com/Neo23x0/Loki
  - Easy to use, cannot remediate or clean-up



Network-based Hunting Strategy

- Packet Content-based
  - Traditional IDS/IPS: Pattern recognition
  - Deep-Packet Inspection: Application-aware NG-FW
  - Full Packet Retention: Moloch etc
  - Expensive, slow, but comprehensive preservation (c.f. DLP).

- Metadata-based
  - Netflow connections: Easy to preserve for a long while.
  - Passive DNS replication: What IP does DNSName resolved to?
  - Retro-Hunting: Compare with latest intelligence feeds.
  - Lightweight, fast, but cannot see what data leaked.

Hunting Intranet & Internet Connections

- Who is most accessed endpoint?
- Why is there office access to non-server endpoints?

52 Internal IPs of 42 Endpoints

Search IP | View: IP | Org

Status

All	52
Unscanned	9
Scanned	43

Department

- All
- [redacted]

Show Others

Internal | External

Name	Org	First Seen	Last Seen	Accessed By Endpoint	Accessed By Process
172.30.8.13	-NONE-	2017/05/04 10:03:16 CST	2017/06/07 10:48:26 CST	41	5
172.30.8.109	-NONE-	2017/04/26 10:11:40 CST	2017/06/06 22:36:05 CST	10	4
172.30.8.108	-NONE-	2017/04/22 15:48:32 CST	2017/06/06 22:36:05 CST	10	4
172.30.8.91	-NONE-	2017/04/13 04:58:18 CST	2017/06/06 22:56:06 CST	7	4

Hunting by ISP / Organization

- How many IP organization did finance department access?
- Why are there endpoints connecting to China?

72 IPs of 193 Endpoints

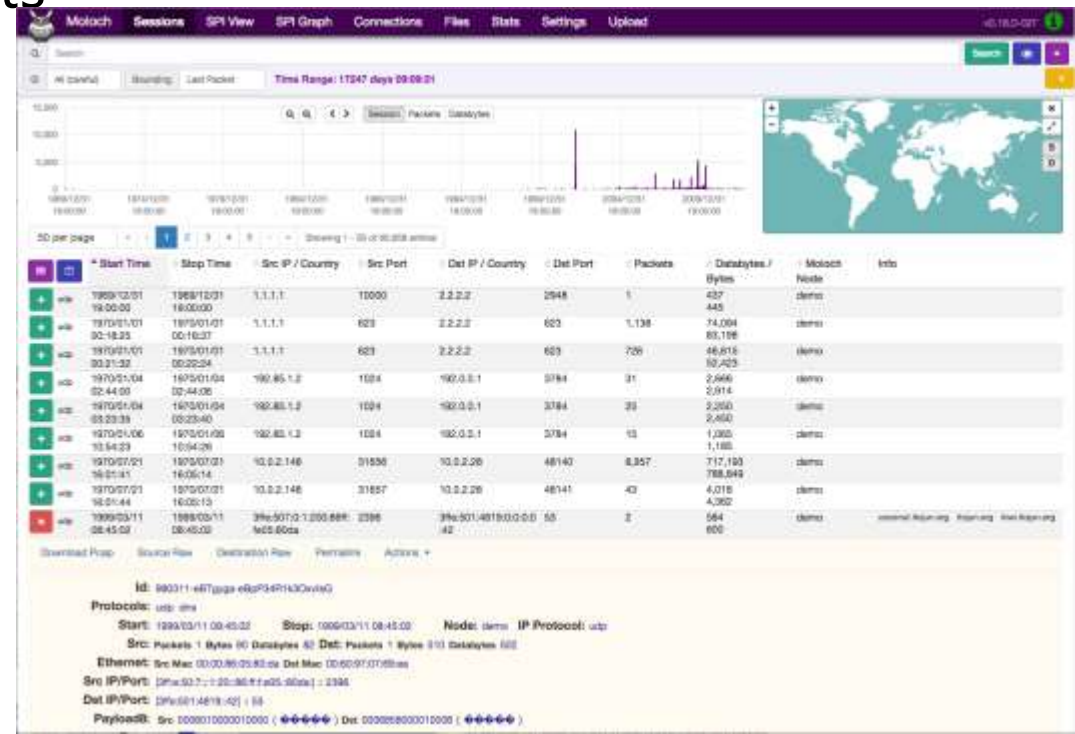
org ~ china and not org ~ yahoo and not org ~ alibaba

Scope | IP | Org

IP	Org	First Seen	Last Seen	Accessed by Endpoint	Accessed by Process	
117.121.28.5	China Unicom Beijing Province Network	2017/08/19 08:17:32 CST	2017/08/20 08:24:09 CST	2	1	VT
117.121.28.4	China Unicom Beijing Province Network	2017/08/09 12:35:04 CST	2017/08/16 10:00:30 CST	2	1	VT
220.181.7.190	IDC, China Telecommunications Corporation	2017/08/13 02:16:13 CST	2017/08/16 17:07:04 CST	2	1	VT
112.84.34.31	CNCGROUP China169 Backbone	2017/08/19 01:11:50 CST	2017/09/01 02:06:12 CST	2	1	VT
123.125.115.164	China Unicom Beijing Province Network	2017/07/25 10:56:11 CST	2017/08/16 17:07:04 CST	2	1	VT
106.75.18.244	China Unicom Beijing Province Network	2017/07/29 16:23:33 CST	2017/07/29 17:36:22 CST	1	1	VT

Open-source Network-hunting Tools

- Bro or Snort or Suricata, the old friends are always useful
  - Write snort rule, de-facto industrial standard
- Moloch, full packet capturing, indexing, and database
  - https://github.com/aol/moloch
  - Extremely useful when investigating incidents
- Bro, Network Security Monitor
  - https://www.bro.org/
  - Powerful, has many plugins

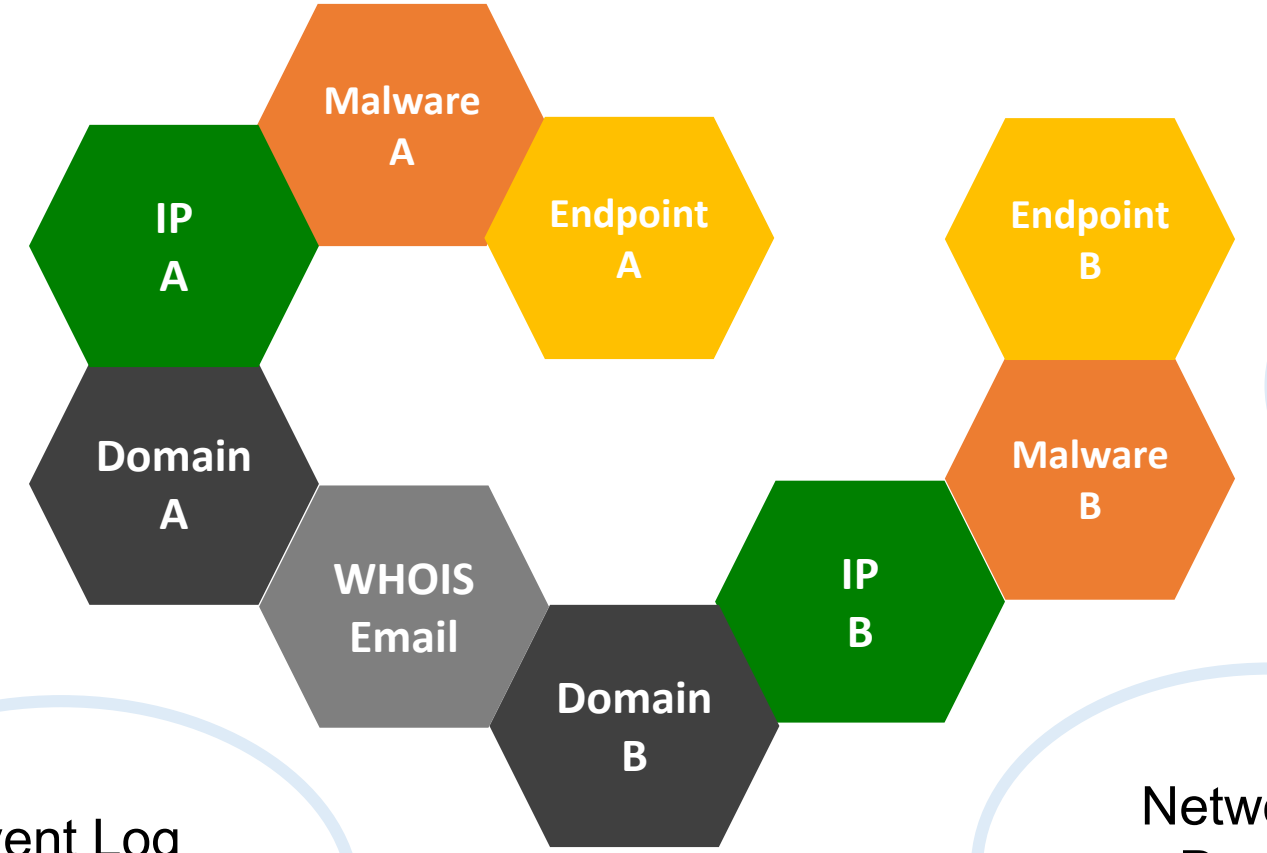


Pivoting Host & Network Indicators

Endpoint
User
Department

File Hash
Path Name
Attributes

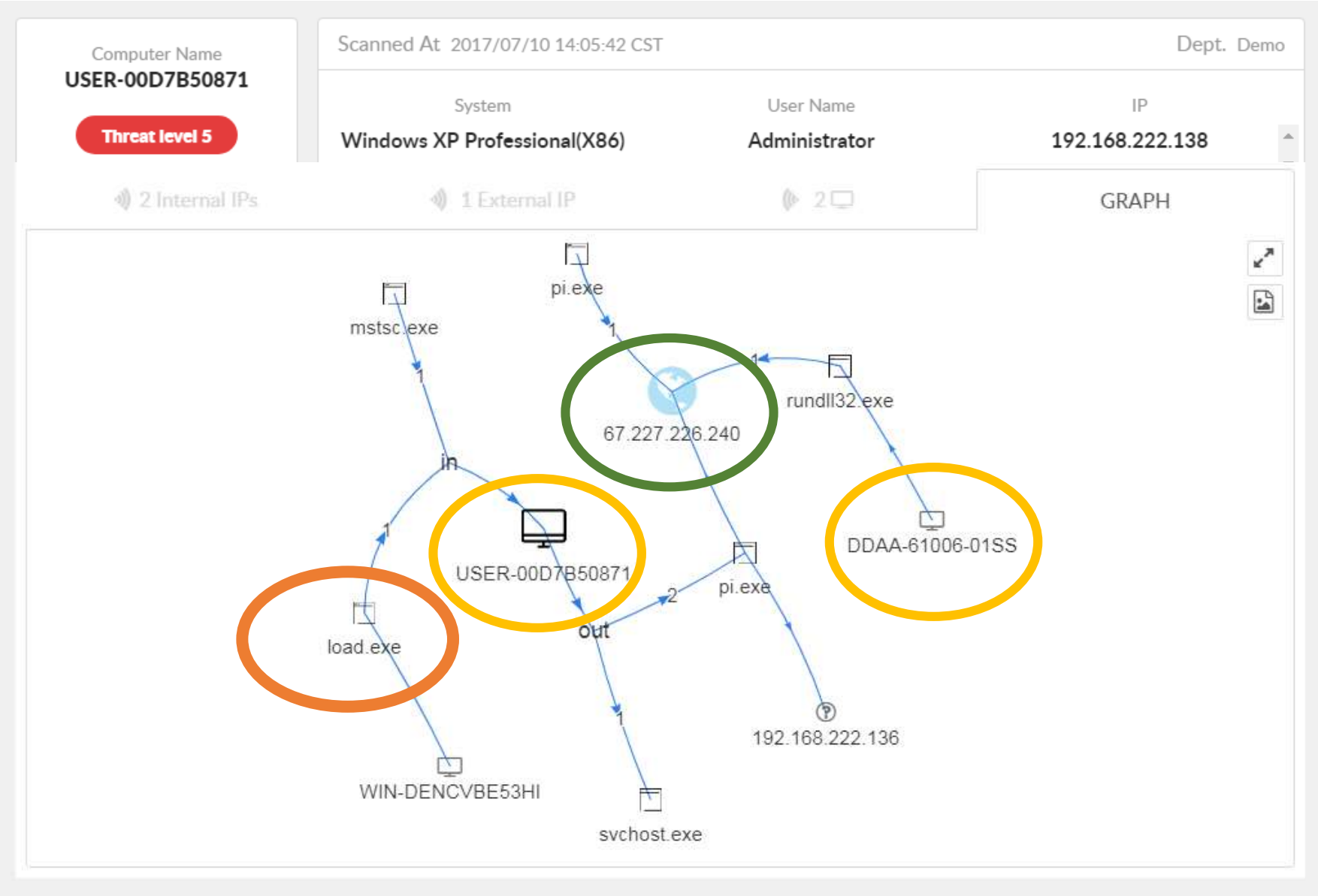
Event Log
MBR Startup
WMI Script



Custom IoC
Yara Rule

Network IP
Domain
Organization

Graph visualization & pivoting

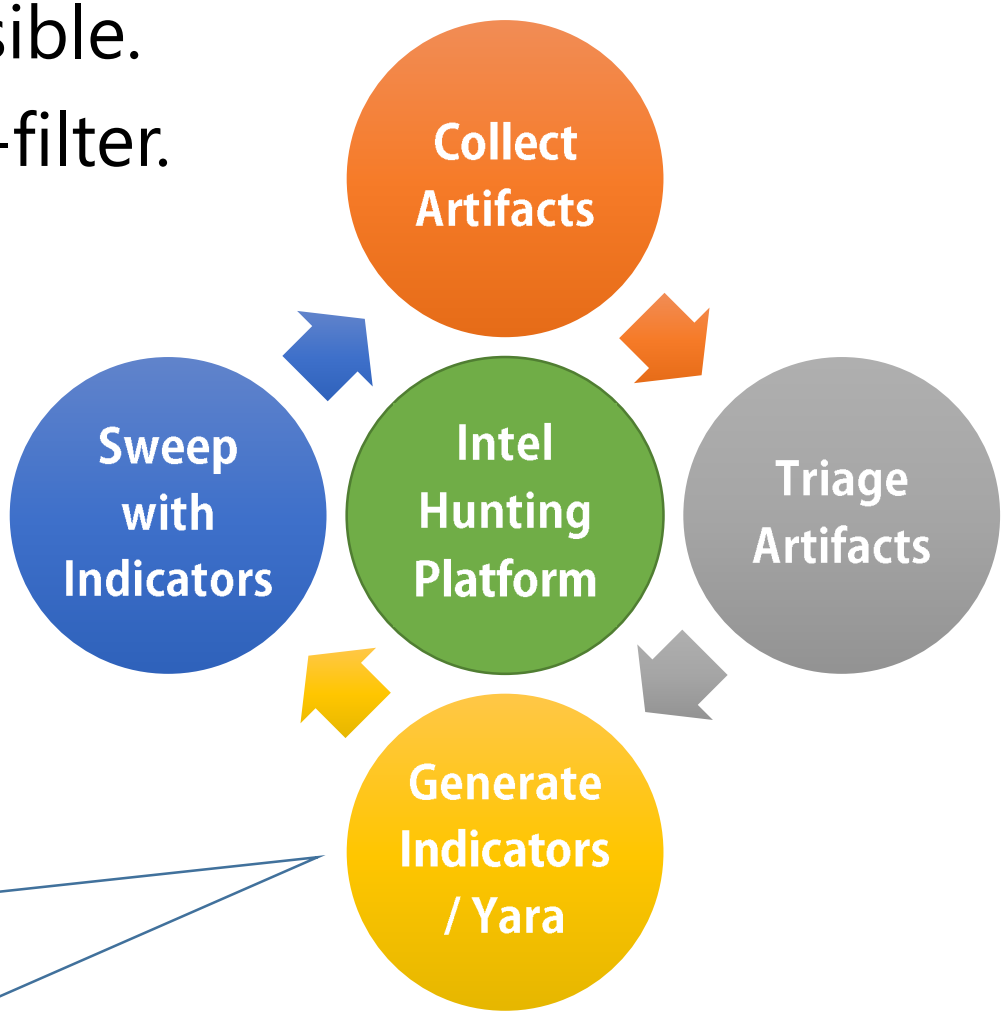


Prioritizing with Threat Intelligence

- Bring external situation awareness into your constituency
- Source: OSINT blog, commercial feeds, bring-your-own
- Matching Indicators: IP, Domain, IoC, Snort, Yara rule

Intel-driven Threat Hunting Cycle

- Collect artifacts: As precise as possible.
- Triage artifacts: Pre-filter and post-filter.
- Generate new indicators
  - Create Yara Rule on-the-fly
- Sweep with indicators
  - Host & Network-based




```
rule exploit_LNK_CVE_2017_8464
{
strings:
    $ShortCut = { 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 00 00 00 46 }

    $MyComputer = { 1F ?? E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D }
    $ControlPanel = { 2E ?? 20 20 EC 21 EA 3A 69 10 A2 DD 08 00 2B 30 30 9D ?? ??  ?
    $SpecialFolderData = { 10 00 00 00 05 00 00 A0 03 00 00 00 28 00 00 00 }

condition:
    $ShortCut at 0 and ($MyComputer and $ControlPanel and $SpecialFolderData)
}
```

Open-source Incident Platforms

- CRITS, MITRE Collaborative Research Into Threats
  - https://crits.github.io/
  - Powerful but complicated entity model
- Cyphon, Incident Management and Response Platform
  - https://www.cyphon.io/
- YETI, Your Everyday Threat Intelligence
  - https://yeti-platform.github.io/
  - Powerful and easy to use

Intelligence-driven Proactive Defense

INTERNAL

Threat Hunting

Host-based activity
Network-based traffic
Central log management
Suspicious system activity
Previous security incidents

Intelligence Platform

Proactive Defense Cycle

EXTERNAL

Threat Intel

0day / CVE vulnerability
Latest attack method TTP
Adversary campaign tracking
Industrial Attack Trends
External Incident Sharing

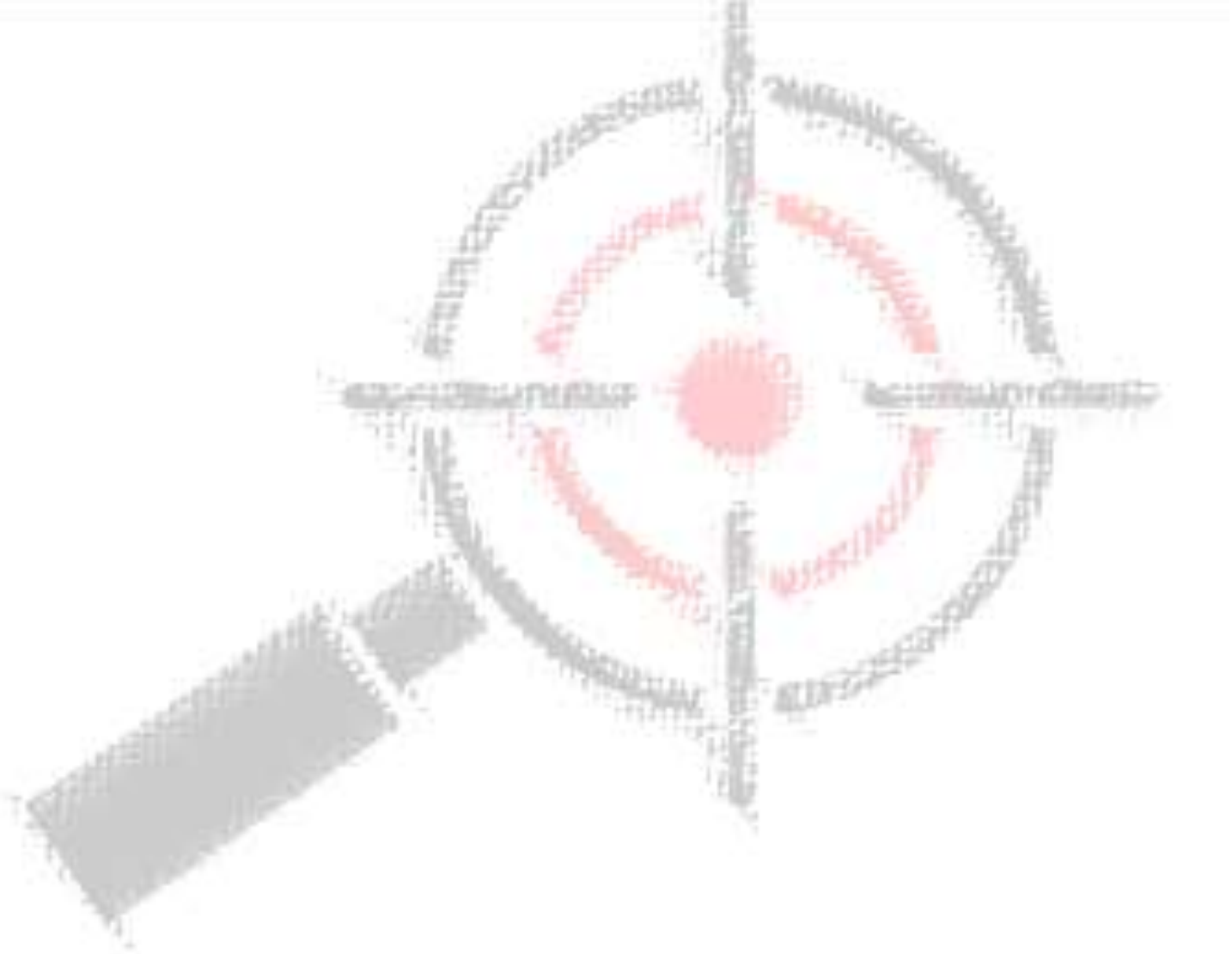
Conclusion

TEAM T5
Cyber Security Research

Respond before Incident: Be Proactive

- Don’t response only when there’s incident
  - When you see a bear, you run faster than other people.
  - When you see Crime attack, you run faster than other victim.
  - When you see APT attack, you must run faster than APT actor.

- Re-think about your strategy
  - Effective Mitigation Cycle
  - Intelligence-driven Proactive Defense Strategy
  - Intelligence-driven Threat Hunting Cycle



Q&A

tt@teamt5.org
gd@teamt5.org

References

- FIRST CSIRT Framework 1.1 (FIRST)
- Security Operations Center on a Budget (AlienVault)
- Evolving to Hunt (Arbor Networks)
- Definitive Guide to Cyber Threat Intelligence (Fireeye iSIGHT)
- Threat Hunting Academy: Threat Hunting Essentials (Sqrrl Data)