Threat Landscape through VirusTotal MNSEC 2023

www.virustotal.com/contact

Steven Chen |Regional Lead | VirusTotal - North Asia

Google Cloud

virustotal.com/gui/file/dd9e96541c3d5857827b060c026136ecb8b14d6f061d6a33d41cc5ec0ff96f50/detection

dd9e96541c3d5857827b060c026136ecb8b14d6f061d6a33d41cc5ec0ff96f50

54 / 73

54 engines detected this file

dd9e96541c3d5857827b060c026136ecb8b14d6f061d6a33d41cc5ec0ff96f50
b%E7%AB%99%E5%BC%B9%E5%B9%95%E5%A7%AC_58@234128.exe

overlay peexe runtime-modules signed upx

1.07 MB Size

2020-05-28 10:13:44 UTC 28 minutes ago

Ad-Aware	Gen:Variant.Adware.Downloader.211	AegisLab	Adware.Win32.Generic.2!c
AhnLab-V3	PUP/Win32.Generic.C3478818	Alibaba	Downloader:Win32/Downer.69f5fc31
ALYac	Gen:Variant.Adware.Downloader.211	Antiy-AVL	Trojan/Win32.Fuerboos
SecureAge APEX	Malicious	Arcabit	Trojan.Adware.Downloader.211
Avast	Win32:PUP-gen [PUP]	AVG	FileRepMalware [PUP]
Avira (no cloud)	HEUR/AGEN.1126112	BitDefender	Gen:Variant.Adware.Downloader.211
CAT-QuickHeal	Trojan.Downer	Comodo	Malware@#1bdgqmd4cqmnr
Cylance	Unsafe	Cyren	W32/Trojan.HOQT-5448
DrWeb	Program.DownLoader.9	eGambit	Unsafe.AI_Score_99%
Emsisoft	Application.Downloader (A)	Endgame	Malicious (high Confidence)
eScan	Gen:Variant.Adware.Downloader.211	ESET-NOD32	A Variant Of Win32/RiskWare.Downer.B
F-Secure	Heuristic.HEUR/AGEN.1126112	FireEye	Generic.mg.47c1aed909d6019e
Fortinet	Riskware/Downer	GData	Gen:Variant.Adware.Downloader.211
Ikarus	PUA.RiskWare.Downer	Jiangmin	Downloader.Agent.nez
K7AntiVirus	Riskware (00544e421)	K7GW	Riskware (00544e421)
Kaspersky	Not-a-virus:Downloader.Win32.Agent.mh...	Malwarebytes	PUP.Optional.FastDownloader

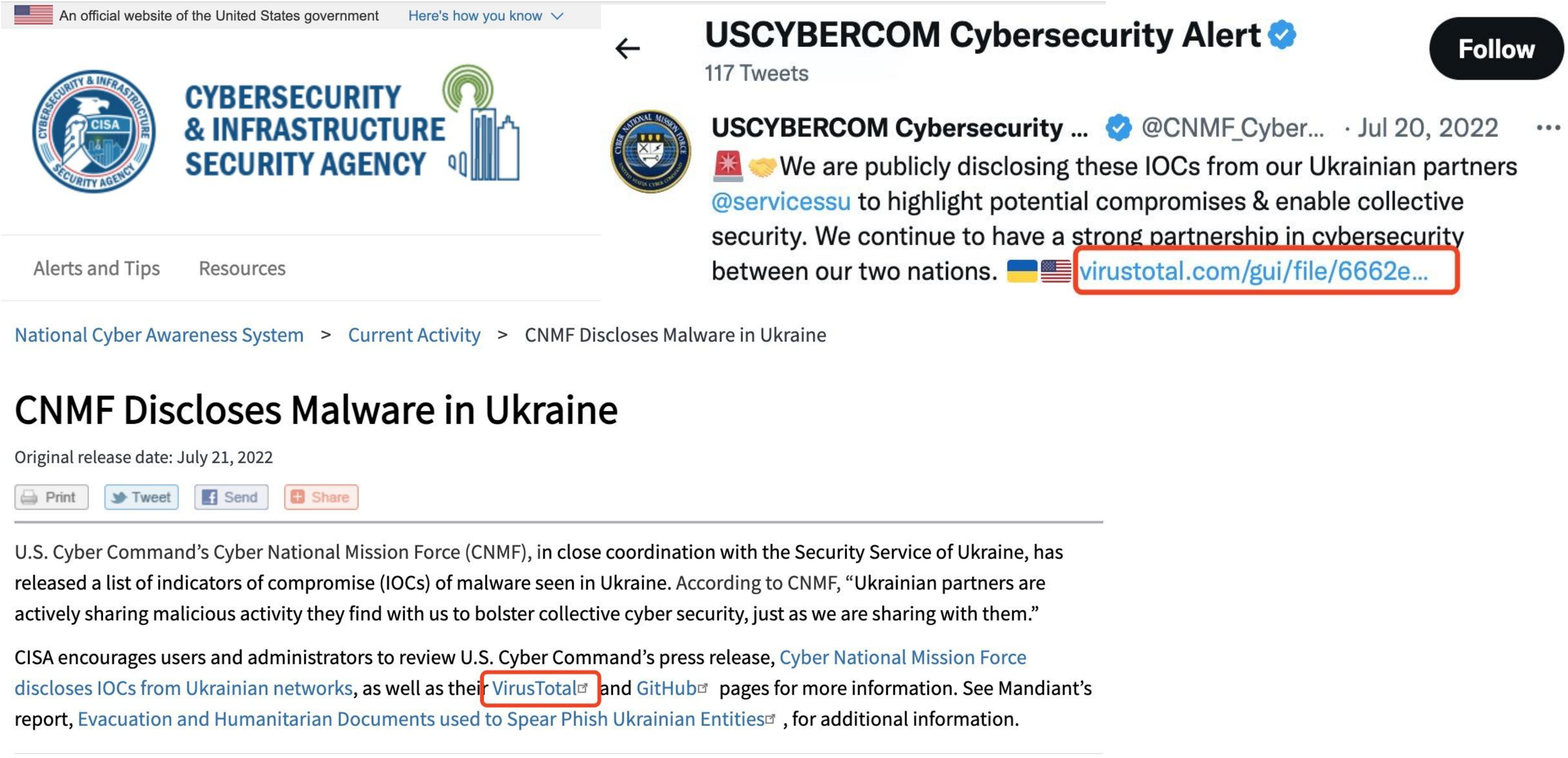
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

Free public service

Upload a file and get a second opinion by 70+ antivirus solutions

www.virustotal.com

Russia Ukraine war



An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

USCYBERCOM Cybersecurity Alert

117 Tweets

USCYBERCOM Cybersecurity ... @CNMF_Cyber... · Jul 20, 2022

🚨🤝We are publicly disclosing these IOCs from our Ukrainian partners @servicessu to highlight potential compromises & enable collective security. We continue to have a strong partnership in cybersecurity between our two nations. 🇺🇦🇺🇸 virustotal.com/gui/file/6662e...

National Cyber Awareness System > Current Activity > CNMF Discloses Malware in Ukraine

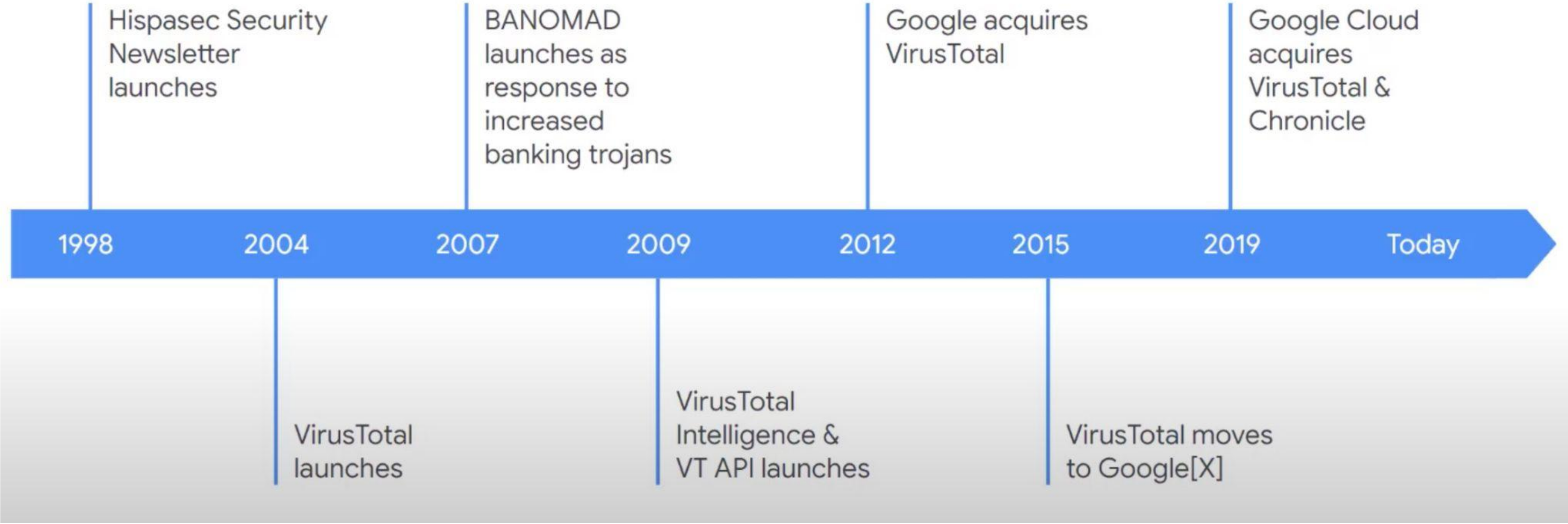
CNMF Discloses Malware in Ukraine

Original release date: July 21, 2022

U.S. Cyber Command's Cyber National Mission Force (CNMF), in close coordination with the Security Service of Ukraine, has released a list of indicators of compromise (IOCs) of malware seen in Ukraine. According to CNMF, "Ukrainian partners are actively sharing malicious activity they find with us to bolster collective cyber security, just as we are sharing with them."

CISA encourages users and administrators to review U.S. Cyber Command's press release, Cyber National Mission Force discloses IOCs from Ukrainian networks, as well as their VirusTotal and GitHub pages for more information. See Mandiant's report, Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities, for additional information.

VirusTotal History



1998

Hispasec Security Newsletter launches

2004

VirusTotal launches

2007

BANOMAD launches as response to increased banking trojans

2009

VirusTotal Intelligence & VT API launches

2012

Google acquires VirusTotal

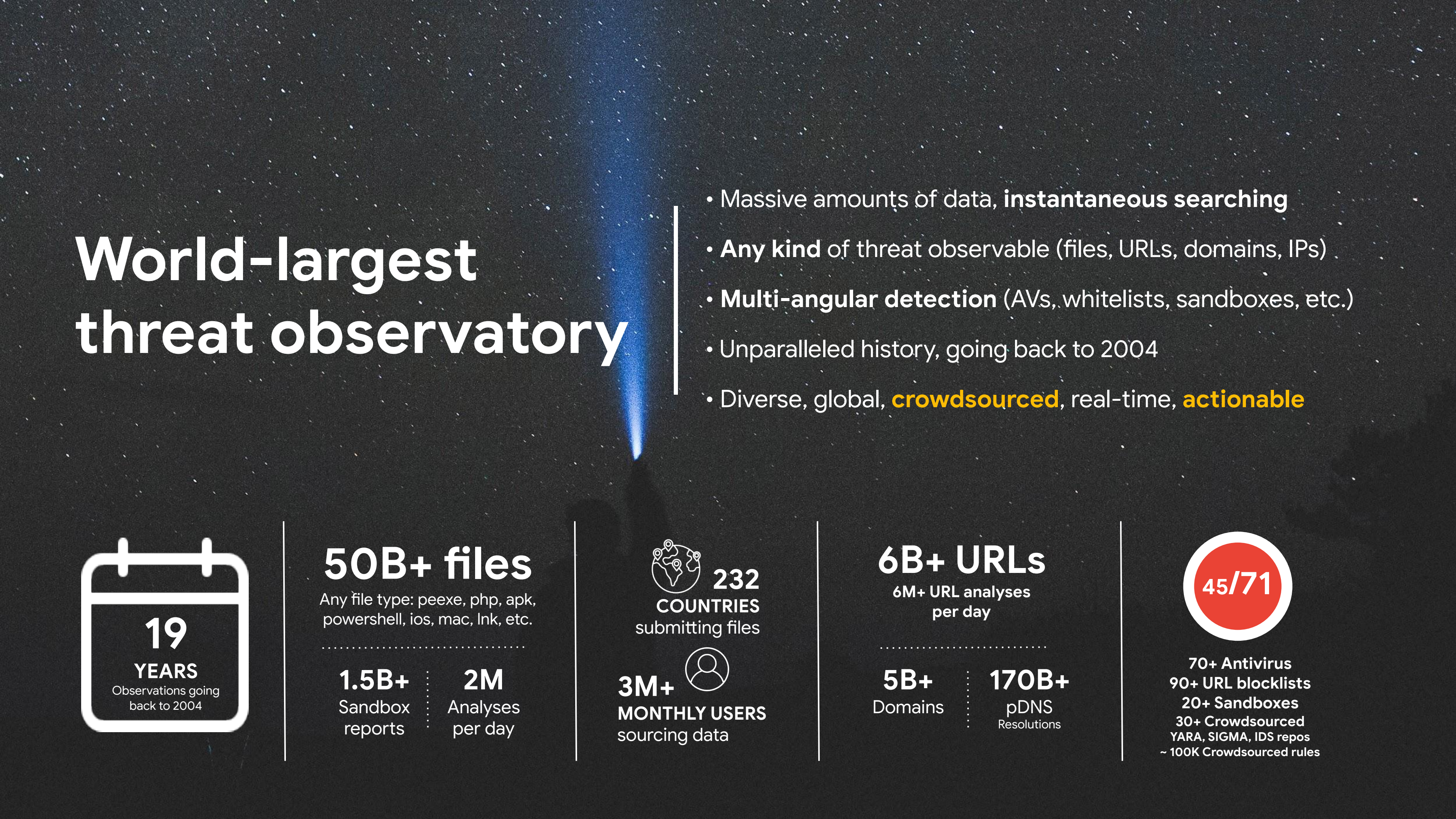
2015

VirusTotal moves to Google[X]

2019

Google Cloud acquires VirusTotal & Chronicle

Today



World-largest threat observatory

- Massive amounts of data, **instantaneous searching**
- **Any kind** of threat observable (files, URLs, domains, IPs)
- **Multi-angular detection** (AVs, whitelists, sandboxes, etc.)
- Unparalleled history, going back to 2004
- Diverse, global, **crowdsourced**, real-time, **actionable**

19
YEARS
Observations going back to 2004

50B+ files
Any file type: peexe, php, apk, powershell, ios, mac, lnk, etc.

1.5B+
Sandbox reports

2M
Analyses per day

232
COUNTRIES
submitting files

3M+
MONTHLY USERS
sourcing data

6B+ URLs
6M+ URL analyses per day

5B+
Domains

170B+
pDNS
Resolutions

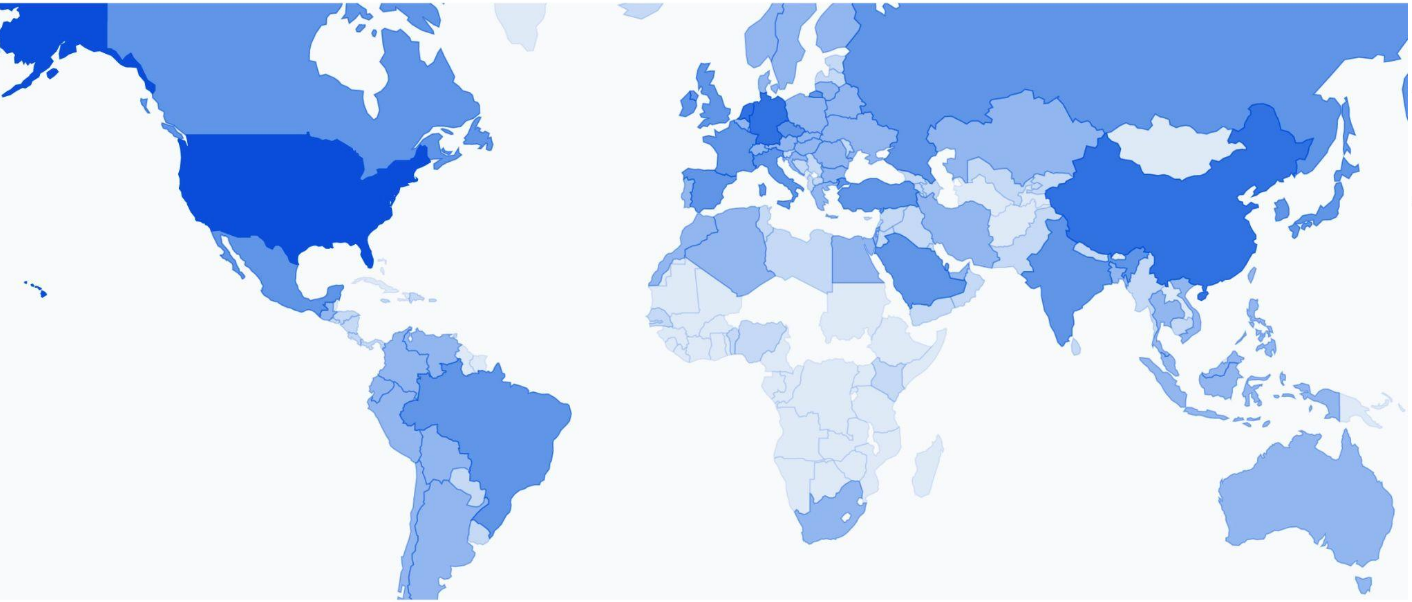
45/71

70+ Antivirus
90+ URL blocklists
20+ Sandboxes
30+ Crowdsourced
YARA, SIGMA, IDS repos
~ 100K Crowdsourced rules

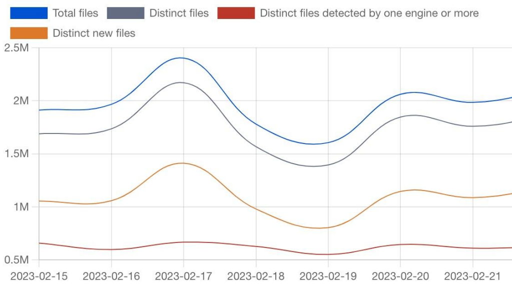
New sample ingested **Daily:**
2M+ file | 400k+ sandbox
3M+ URL | 1M+ IP Address | 25M+ domain

Global data source: www.virustotal.com/gui/stats

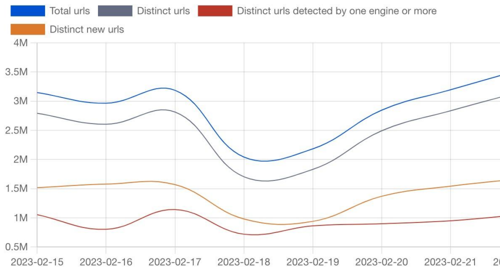
SUBMISSIONS BY COUNTRY



PROCESSED FILES



PROCESSED URLS



Global Partner/Contributor

McAfee™

SOPHOS

kaspersky

Alibaba.com®

paloalto® NETWORKS

TREND MICRO™

Yandex

Microsoft

CROWDSTRIKE

elastic

Bai du 百度

Google

FORTINET®

FIREEYE™

NSFOCUS

Full Partner/ Contributor list

Agenda

❏ Incident Response

❏ Automation and enrichment for SOC

❏ Threat Hunting

❏ VT Reference from JPCERT

Incident Response

01

Google Cloud

- Log4j
- Hafnium
- Ransomware

SUSPICIOUS FILE DETECTED

mkSandboxService.exe

MACHINE X | USER A

⚠ **SUSPICIOUS FILE DETECTED**

mkSandboxService.exe 1/72

MACHINE X | USER A

What was the distribution vector?

Is this an APT / 0-Day attack?

Who’s behind this cyberattack?

What are the C&C servers?

What malware family I’m facing?

SUSPICIOUS FILE DETECTED

mkSandboxService.exe ∑ 3/72

MACHINE X | USER A

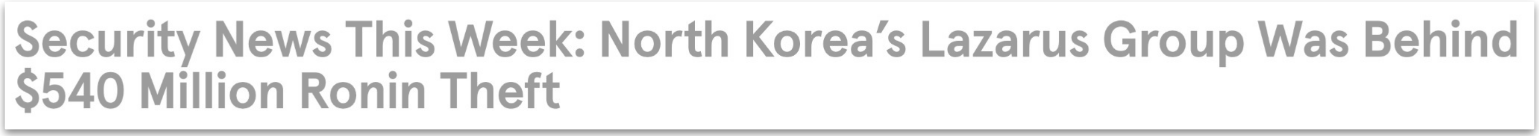
What techniques did the attackers use?

Are there any other indicators I should know about?

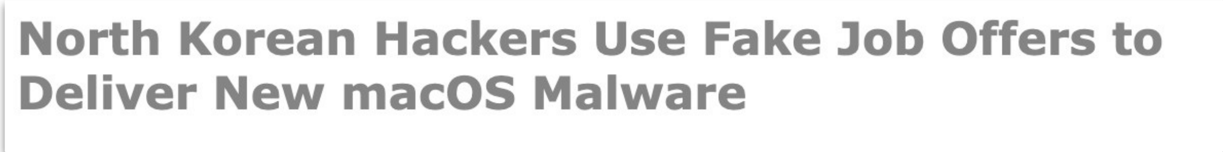
Can I do anything to detect future attacks??

What are the attackers motivations?

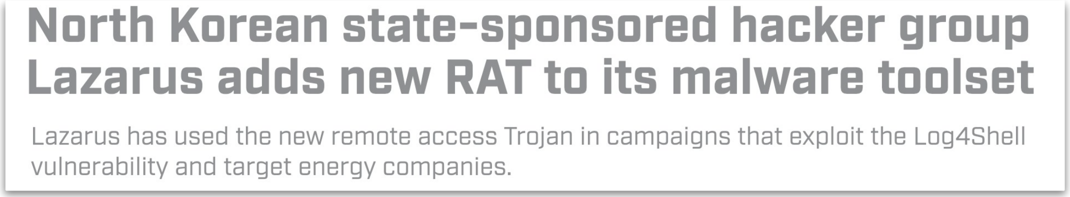
Could this be a false positive?



Security News This Week: North Korea’s Lazarus Group Was Behind $540 Million Ronin Theft



North Korean Hackers Use Fake Job Offers to Deliver New macOS Malware



North Korean state-sponsored hacker group Lazarus adds new RAT to its malware toolset

Lazarus has used the new remote access Trojan in campaigns that exploit the Log4Shell vulnerability and target energy companies.

LAZARUS GROUP

Lazarus Group is a cybercrime group made up of an unknown number of individuals run by the North Korean state.

1000+

56% of Large Companies Handle 1,000+ Security Alerts Each Day

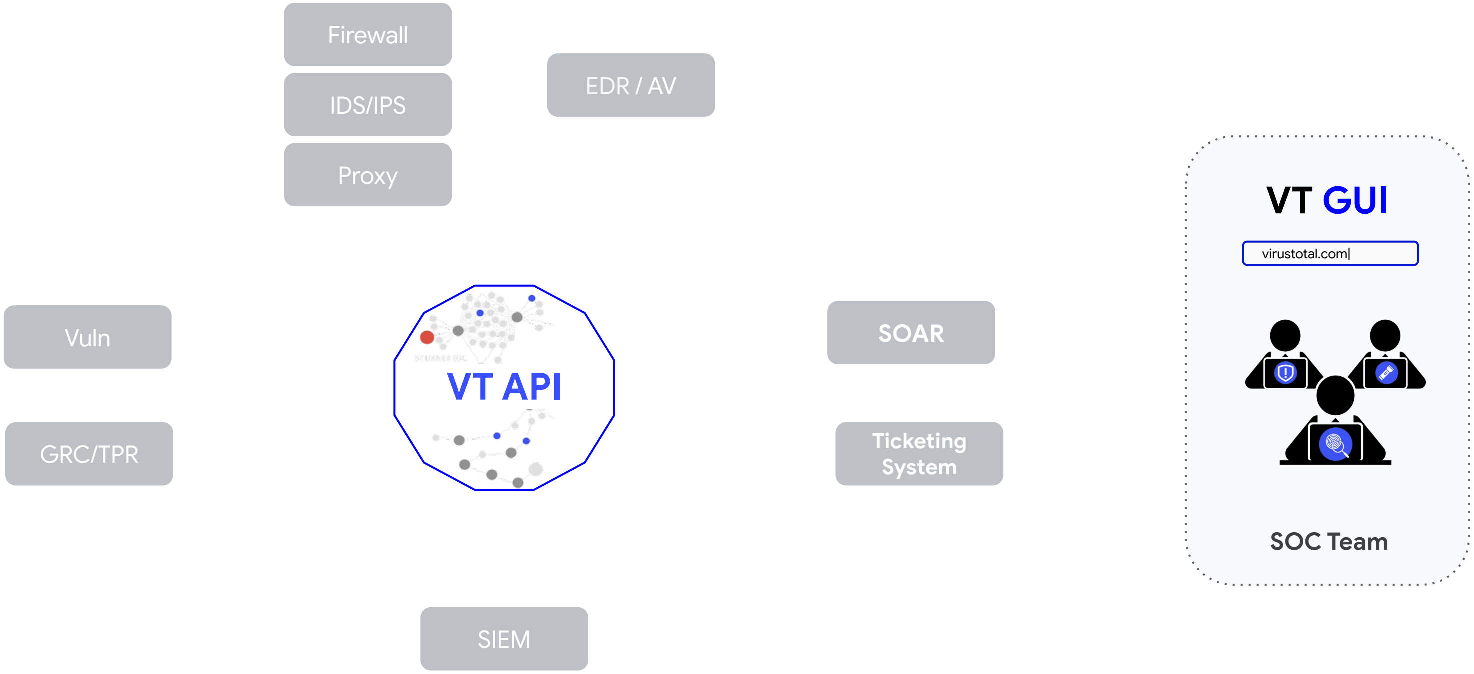
For 70% of IT security professionals, the volume of security alerts has doubled in the past five years.

Are we ready to deal with 2000 alerts per day in 5 years?

Automation and enrichment for SOC

02

3rd Party Integrations



Firewall

IDS/IPS

Proxy

EDR / AV

Vuln

GRC/TPR

VT API

SOAR

Ticketing System

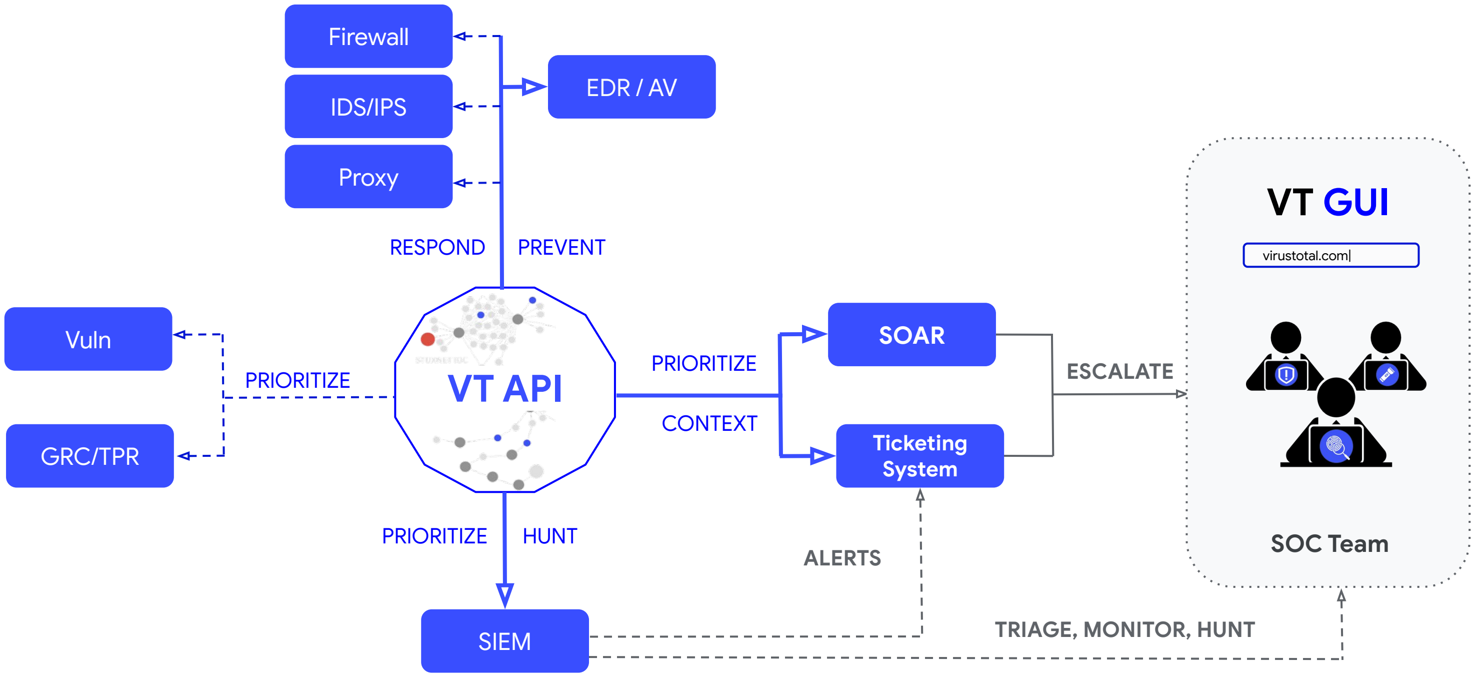
VT GUI

virustotal.com

SOC Team

SIEM

3rd Party Integrations

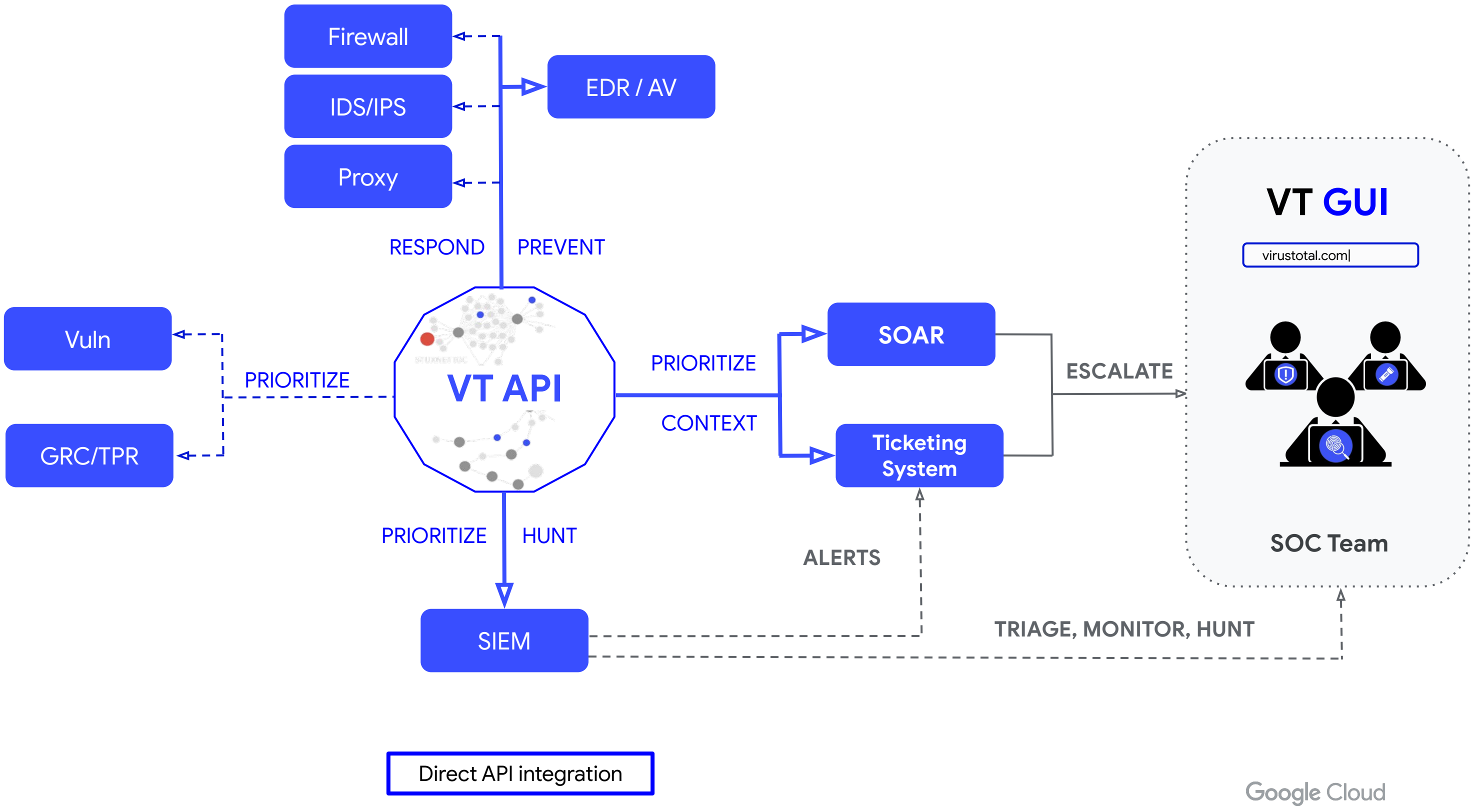


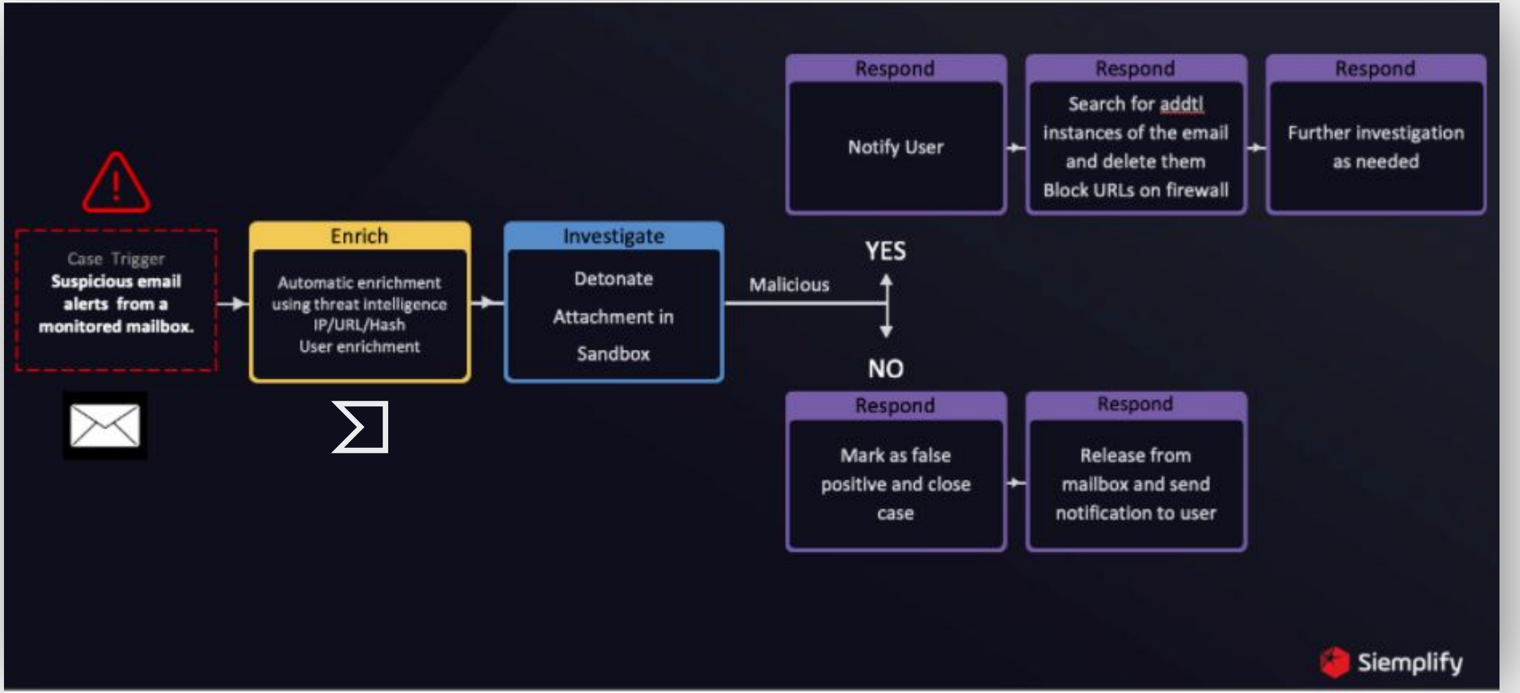
Direct API integration

Off the shelf plugins with...

- chronicle
- splunk>
- splunk> phantom
- CROWDSTRIKE
- CORTEX XSOAR BY PALO ALTO NETWORKS
- cisco SecureX
- IBM QRadar
- DEMISTO
- Carbon Black.
- McAfee ePolicy Orchestrator
- MALTEGO
- LogRhythm
- VERAMINE
- TANIUM.
- ANOMALI
- thycotic
- Cynet
- servicenow
- proofpoint
- paloalto NETWORKS
- WAZUH
- EnCase
- ayehu
- KnowBe4 Human error. Conquered.
- PhishER

...and most security products.





Case Trigger
Suspicious email alerts from a monitored mailbox.

Enrich
Automatic enrichment using threat intelligence IP/URL/Hash
User enrichment

Investigate
Detonate Attachment in Sandbox

Malicious

YES

Respond
Notify User

Respond
Search for addtl instances of the email and delete them
Block URLs on firewall

Respond
Further investigation as needed

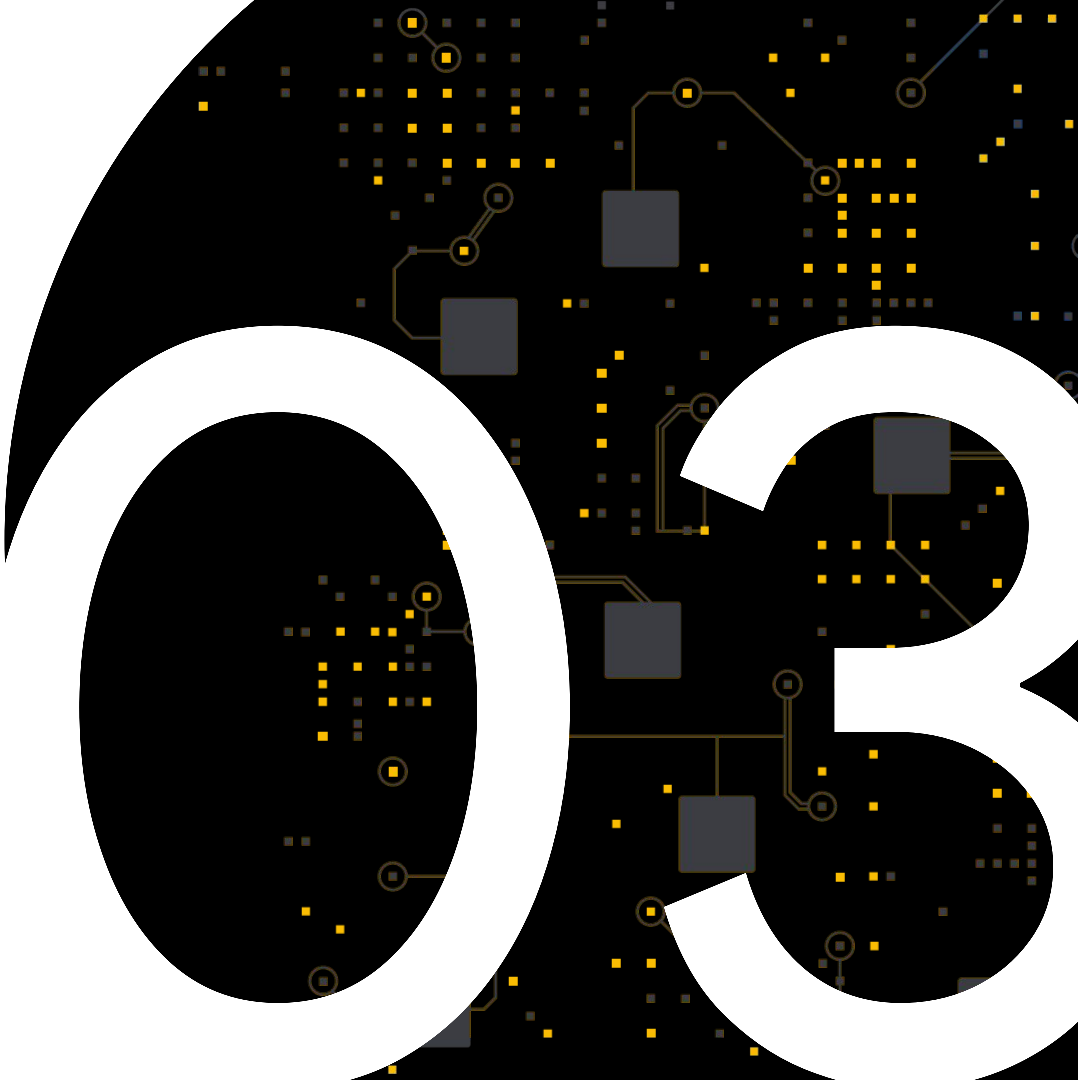
NO

Respond
Mark as false positive and close case

Respond
Release from mailbox and send notification to user

Siemplify

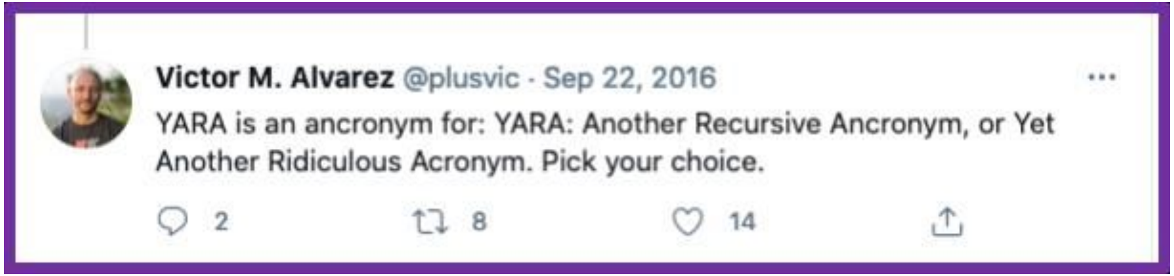
Threat Hunting



03

VirusTotal Hunting

VirusTotal is the proud home of YARA



Victor M. Alvarez @plusvic · Sep 22, 2016

YARA is an ancronym for: YARA: Another Recursive Ancronym, or Yet Another Ridiculous Acronym. Pick your choice.

2 8 14

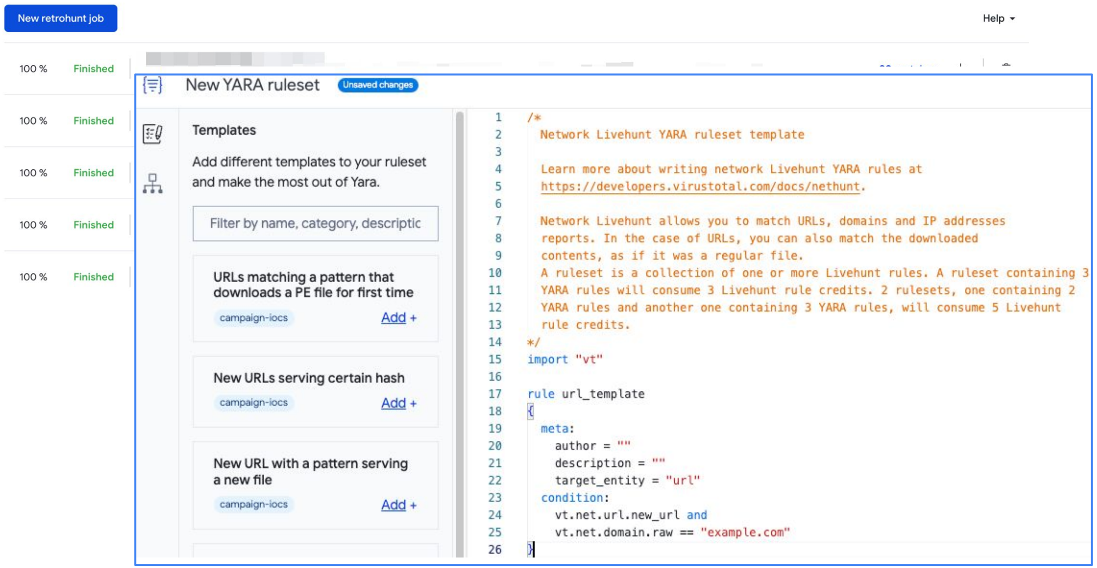
Created by **Victor Manuel Álvarez, VT engineer**

VTHUNTING

VirusTotal Hunting

Apply Yara rules (**Retrohunt**) to hunt back-in-time, across all submitted samples in VirusTotal

Create **LiveHunt** rules to get alerts on newly submitted samples. Hunt for not-yet-detected matches, or under-the-radar variants.



100 %	Finished
100 %	Finished
100 %	Finished
100 %	Finished
100 %	Finished

New YARA ruleset

Templates

Add different templates to your ruleset and make the most out of Yara.

Filter by name, category, descriptic

URLs matching a pattern that downloads a PE file for first time

campaign-iocs

New URLs serving certain hash

campaign-iocs

New URL with a pattern serving a new file

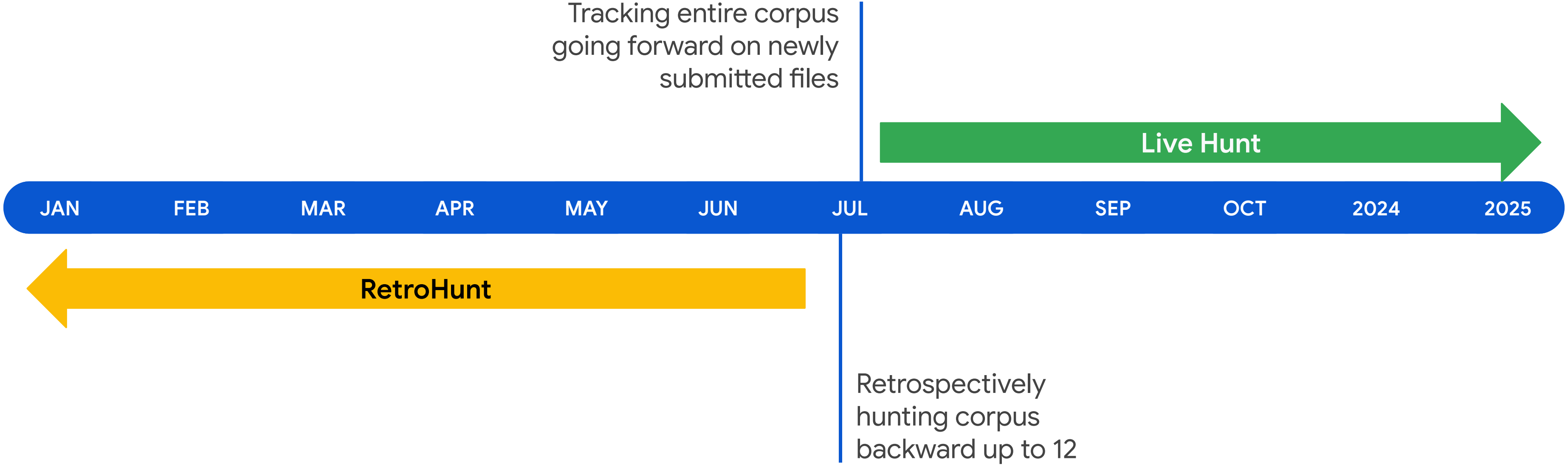
campaign-iocs

```
/*
  Network Livehunt YARA ruleset template

  Learn more about writing network Livehunt YARA rules at
  https://developers.virustotal.com/docs/nethunt.

  Network Livehunt allows you to match URLs, domains and IP addresses
  reports. In the case of URLs, you can also match the downloaded
  contents, as if it was a regular file.
  A ruleset is a collection of one or more Livehunt rules. A ruleset containing 3
  YARA rules will consume 3 Livehunt rule credits. 2 rulesets, one containing 2
  YARA rules and another one containing 3 YARA rules, will consume 5 Livehunt
  rule credits.
*/
import "vt"

rule url_template
{
  meta:
    author = ""
    description = ""
    target_entity = "url"
  condition:
    vt.net.url.new_url and
    vt.net.domain.raw == "example.com"
}
```

Google Cloud

VirusTotal

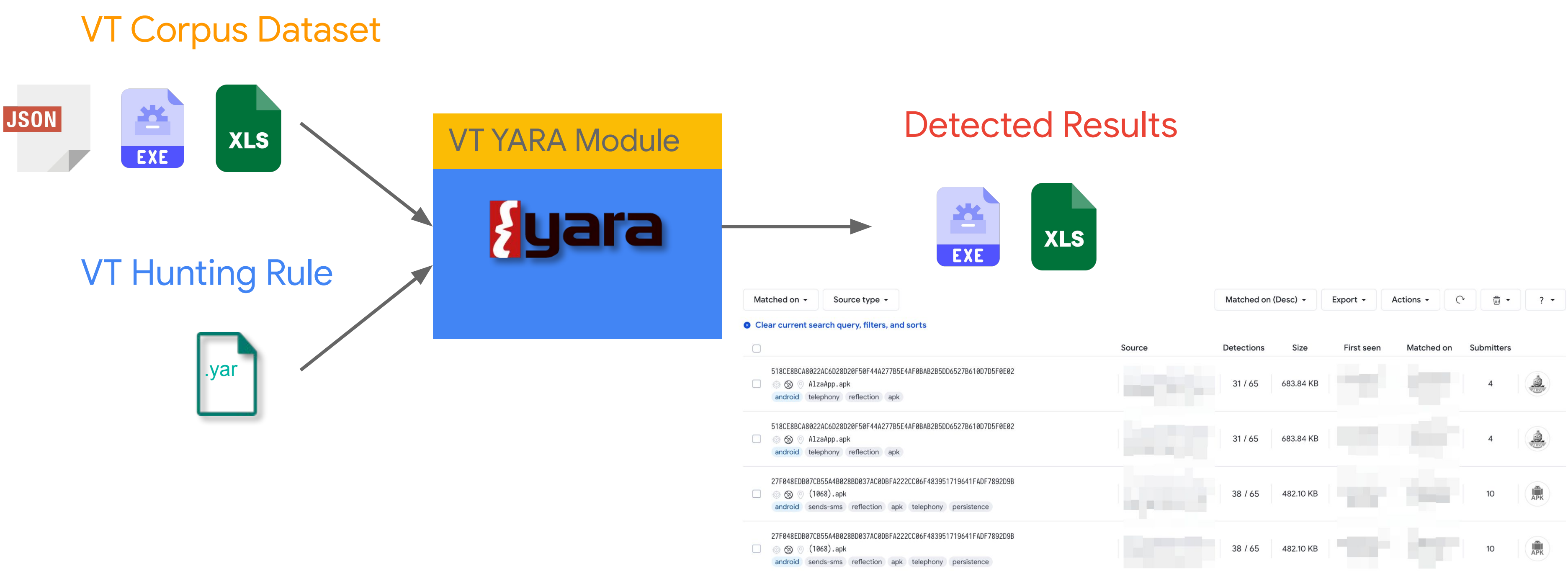
VirusTotal Hunting



Tracking entire corpus going forward on newly submitted files

Retrospectively hunting corpus backward up to 12 months

VirusTotal Hunting



Clear current search query, filters, and sorts

□		Source	Detections	Size	First seen	Matched on	Submitters	
□	518CE8BCA8022AC6D28D20F50F44A277B5E4AF0BAB2B5DD6527B610D7D5F0E02 AlzaApp.apk android telephony reflection apk	[redacted]	31 / 65	683.84 KB	[redacted]	[redacted]	4	ALZA
□	518CE8BCA8022AC6D28D20F50F44A277B5E4AF0BAB2B5DD6527B610D7D5F0E02 AlzaApp.apk android telephony reflection apk	[redacted]	31 / 65	683.84 KB	[redacted]	[redacted]	4	ALZA
□	27F048EDB07CB55A4B028BD037AC0DBFA222CC06F483951719641FADF7892D9B (1068).apk android sends-sms reflection apk telephony persistence	[redacted]	38 / 65	482.10 KB	[redacted]	[redacted]	10	APK
□	27F048EDB07CB55A4B028BD037AC0DBFA222CC06F483951719641FADF7892D9B (1068).apk android sends-sms reflection apk telephony persistence	[redacted]	38 / 65	482.10 KB	[redacted]	[redacted]	10	APK

VTHUNTING

VirusTotal Hunting : Use Case

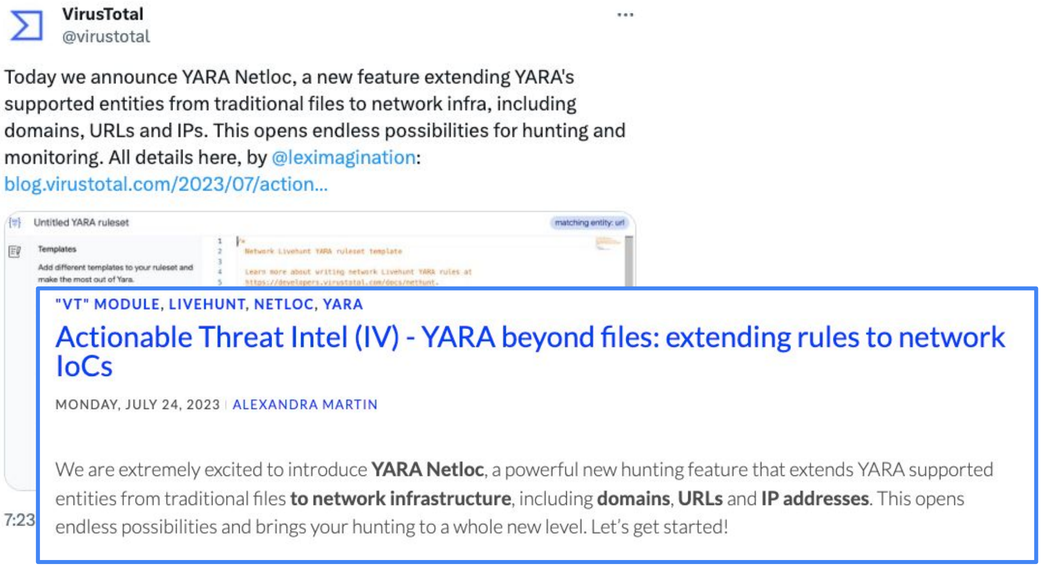
There are a number of use cases for using YARA with VT Hunting:

- **Identify** and classify malware
- **Find new samples** based on family-specific patterns
- **Incident Responders** can deploy YARA rules to identify samples and compromised devices
- **Proactive deployment of custom YARA rules** can increase an organization’s defenses

VTHUNTING

VirusTotal Hunting : Update

In July we have release YARA Netloc that extends YARA detection to network based IoCs (E.g. IP addresses, URLs, Domain, etc) in VT Corpus dataset.



VirusTotal
@virustotal

Today we announce YARA Netloc, a new feature extending YARA's supported entities from traditional files to network infra, including domains, URLs and IPs. This opens endless possibilities for hunting and monitoring. All details here, by @leximagination: blog.virustotal.com/2023/07/action...

Untitled YARA ruleset

matching entity: url

Templates

Add different templates to your ruleset and make the most out of Yara.

```
/*
Network Livehunt YARA ruleset template

Learn more about writing network Livehunt YARA rules at
https://developers.virustotal.com/docs/nethunt.
```

7:23

"VT" MODULE, LIVEHUNT, NETLOC, YARA

Actionable Threat Intel (IV) - YARA beyond files: extending rules to network IoCs

MONDAY, JULY 24, 2023 | ALEXANDRA MARTIN

We are extremely excited to introduce **YARA Netloc**, a powerful new hunting feature that extends YARA supported entities from traditional files **to network infrastructure**, including **domains**, **URLs** and **IP addresses**. This opens endless possibilities and brings your hunting to a whole new level. Let's get started!

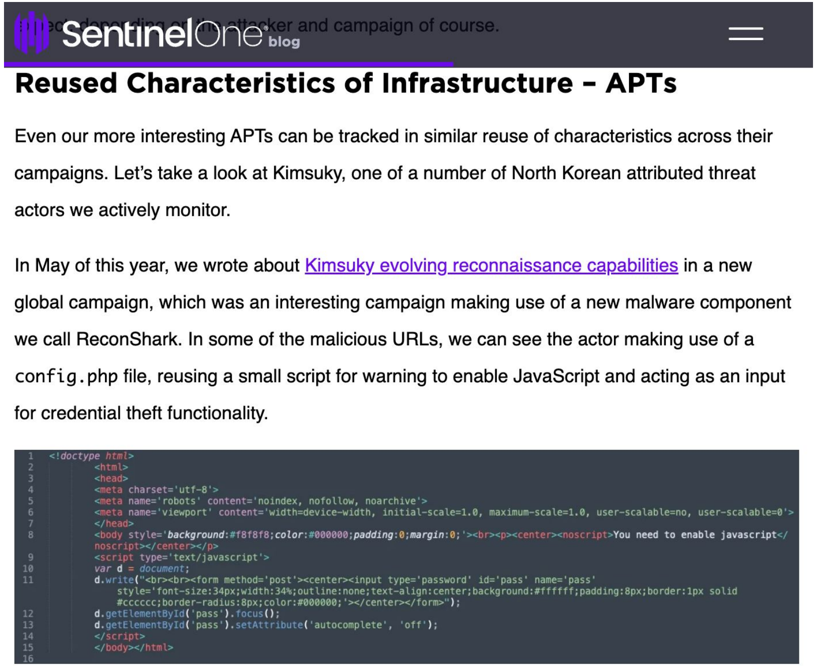
Google Cloud

VirusTotal

VTHUNTING

VT YARA Netloc : Kimsuky Behaviour

- Depending on the importance level of the campaign, threat actors may consider reusing their assets
- Example : Kimsuky's usage of config.php between different URLs
- Hash of config.php : 256fa5009e8e82258876325b7d36f41cc3e74e85627663206b042eec8736ce6a



Reused Characteristics of Infrastructure – APTs

Even our more interesting APTs can be tracked in similar reuse of characteristics across their campaigns. Let's take a look at Kimsuky, one of a number of North Korean attributed threat actors we actively monitor.

In May of this year, we wrote about Kimsuky evolving reconnaissance capabilities in a new global campaign, which was an interesting campaign making use of a new malware component we call ReconShark. In some of the malicious URLs, we can see the actor making use of a `config.php` file, reusing a small script for warning to enable JavaScript and acting as an input for credential theft functionality.

```
<!doctype html>
        <html>
        <head>
        <meta charset='utf-8'>
        <meta name='robots' content='noindex, nofollow, noarchive'>
        <meta name='viewport' content='width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no, user-scalable=0'>
        </head>
        <body style='background:#f8f8f8;color:#000000;padding:0;margin:0;'><br><p><center><noscript>You need to enable javascript</
        noscript></center></p>
        <script type='text/javascript'>
        var d = document;
        d.write("<br><br><form method='post'><center><input type='password' id='pass' name='pass'
            style='font-size:34px;width:34%;outline:none;text-align:center;background:#ffffff;padding:8px;border:1px solid
            #cccccc;border-radius:8px;color:#000000;'></center></form>");
        d.getElementById('pass').focus();
        d.getElementById('pass').setAttribute('autocomplete', 'off');
        </script>
        </body></html>
```

Kimsuky's *config.php*

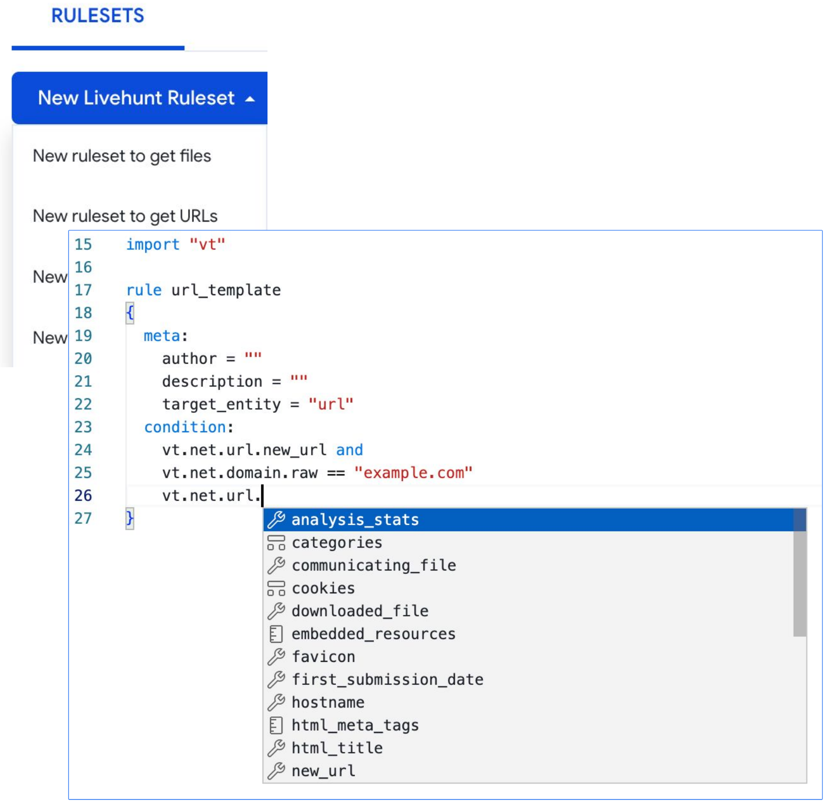
Reference : https://www.sentinelone.com/blog/illicit-brand-impersonation-a-threat-hunting-approach/

Google Cloud

VirusTotal

VT YARA Netloc : Kimsuky Behaviour

- With the hash, we can now monitor if there is any new URLs that serve the same php file
- You can make use of Netloc functions in VT module when using YARA rule editor

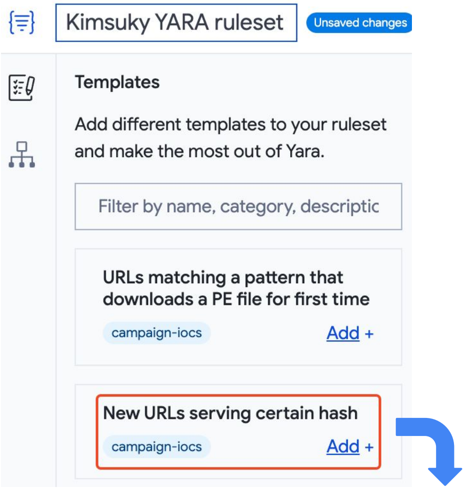


```
import "vt"

rule url_template
{
  meta:
    author = ""
    description = ""
    target_entity = "url"
  condition:
    vt.net.url.new_url and
    vt.net.domain.raw == "example.com"
    vt.net.url.
}
```

VTHUNTING

VT YARA Netloc : Kimsuky Behaviour

- You can also make use of templates within YARA rule editor
- This reduced time required when writing YARA rules or lookup of YARA rule format



Kimsuky YARA ruleset

Unsaved changes

Templates

Add different templates to your ruleset and make the most out of Yara.

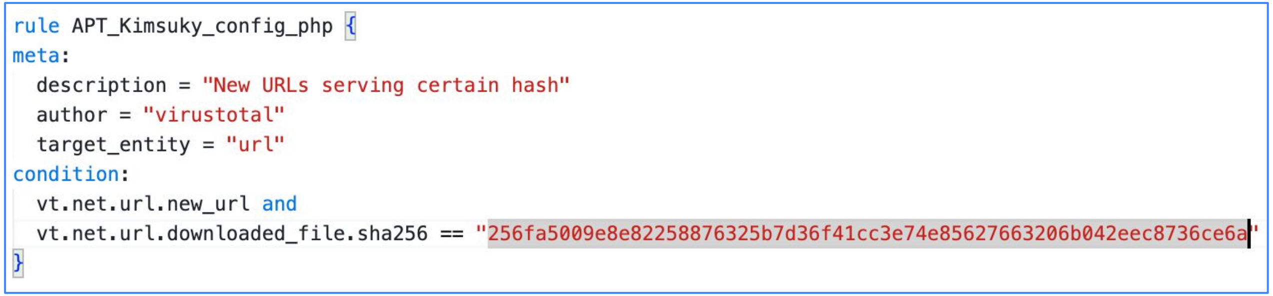
Filter by name, category, descriptic

URLs matching a pattern that downloads a PE file for first time

campaign-iocs Add +

New URLs serving certain hash

campaign-iocs Add +



```
rule APT_Kimsuky_config_php {
meta:
  description = "New URLs serving certain hash"
  author = "virustotal"
  target_entity = "url"
condition:
  vt.net.url.new_url and
  vt.net.url.downloaded_file.sha256 == "256fa5009e8e82258876325b7d36f41cc3e74e85627663206b042eec8736ce6a"
}
```

Google Cloud

VirusTotal

VT Reference from JPCERT

04

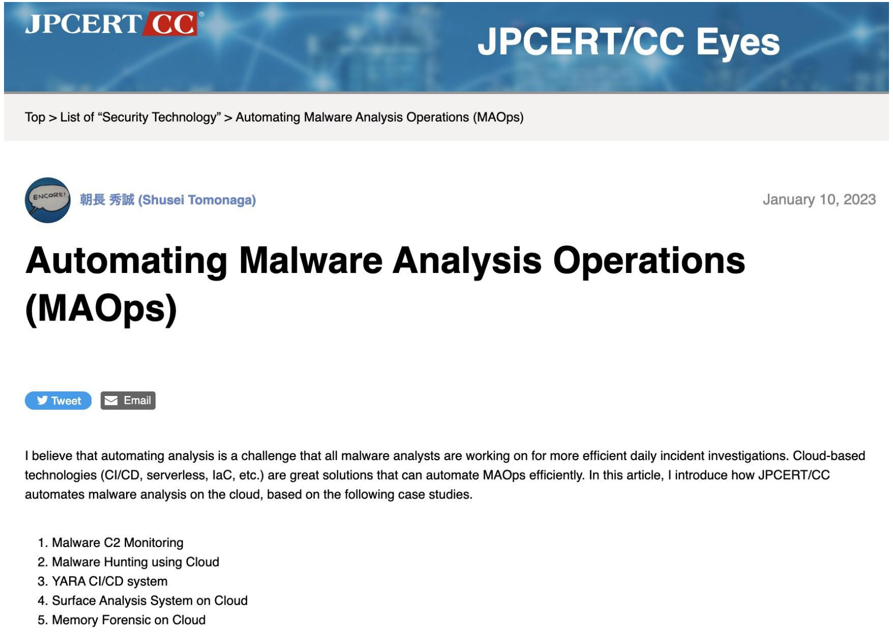
Google Cloud

JPCERT usage of VT for Malware Analysis Automation

- JPCERT setup an automated Malware Analysis Operations (**MAOps**)
- As part of the automation, VT API was used download IOCs for analysis

5 Use Cases

1. Malware C2 Monitoring
2. Malware Hunting
3. YARA CI/CD system
4. Surface Analysis System
5. Memory Forensic



JPCERT CC

JPCERT/CC Eyes

Top > List of “Security Technology” > Automating Malware Analysis Operations (MAOps)

朝長 秀誠 (Shusei Tomonaga)

January 10, 2023

Automating Malware Analysis Operations (MAOps)

I believe that automating analysis is a challenge that all malware analysts are working on for more efficient daily incident investigations. Cloud-based technologies (CI/CD, serverless, IaC, etc.) are great solutions that can automate MAOps efficiently. In this article, I introduce how JPCERT/CC automates malware analysis on the cloud, based on the following case studies.

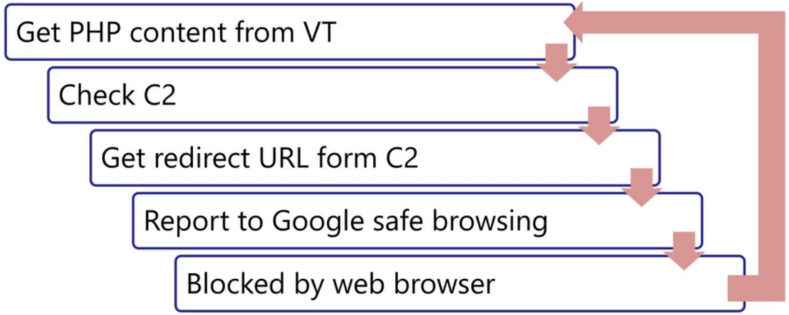
1. Malware C2 Monitoring
2. Malware Hunting using Cloud
3. YARA CI/CD system
4. Surface Analysis System on Cloud
5. Memory Forensic on Cloud

By Shusei Tomonaga

Reference : https://blogs.jpcert.or.jp/en/2023/01/cloud_malware_analysis.html

JPCERT: Malware Analysis Automation

- In one of their use case (C2 monitoring), JPCERT downloads IOCs from VT, performed an analysis and if determined to be malicious, reports to SafeBrowsing.
- This provides a positive feedback loop to all users (Future prevention)



Get PHP content from VT

Check C2

Get redirect URL form C2

Report to Google safe browsing

Blocked by web browser

Figure 1 — JPCERT/CC's lucky visitor scam C2 server monitoring flow.

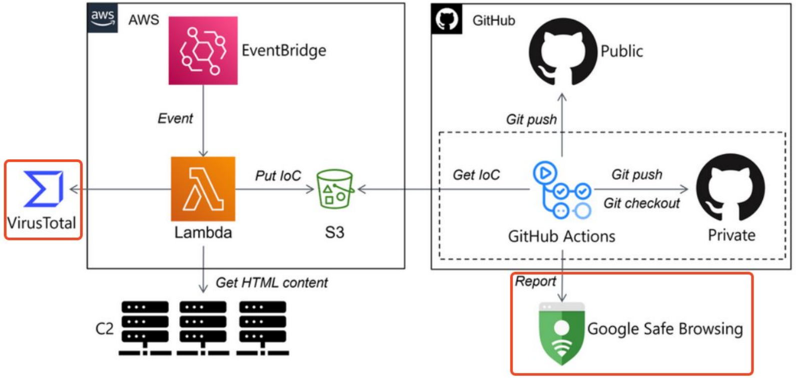


Figure 2 — JPCERT/CC's lucky visitor scam C2 server monitoring system.

Reference : https://blog.apnic.net/2023/09/13/how-jpcert-cc-automates-malware-analysis/

Use cases by Team

- Security Automation team -

- Automatic alert triage via API interaction or one-click integrations
- Security telemetry enrichment, continuously via feeds + API lookups
- Context-driven security orchestration, through your SOAR or custom via API

- Incident Response team -

- Root cause analysis and attack chain exploration
- Forensic analysis and breach containment
- IoC-driven SIEM threat hunting to understand breach breadth

- Anti-abuse team -

- Corporate infrastructure abuse detection & digital asset monitoring
- Brand impersonation detection - fake apps, online lures and others
- Scoring of IP addresses interacting with your services

- SOC/CERT -

- True positive confirmation and false positive discarding
- Contextualization of observables found in alerts
- Incident campaign IoC identification for preventive & remediative actions

- Malware Analysis team -

- Automatic dynamic analysis to understand unknown files
- Static dissection of weaponized documents to reveal final payloads
- Classification and attribution via genetic analysis with n-gram searches

- Red team / Pentesting team -

- Blackbox reconnaissance & passive fingerprinting
- Breach & attack simulation emulating adversary TTPs
- Security stack validation to identify blindspots and mistaken setups

- Threat Intelligence team -

- Discovery of unknown threats to complement existing defenses
- Campaign monitoring to preventively block malicious infrastructure
- Threat actor tracking for proactive TTP hunting & situational awareness

- Anti-fraud team -

- Identification of phishing campaigns & counterfeiting sites targeting your org
- Mitigation of banking and identity theft trojans against your company
- Interception and study of phishing kits and C2 panels for the above

- Vulnerability Management team -

- Vulnerability prioritization & smart risk-driven patching strategy
- In-the-wild vulnerability weaponization monitoring
- Threat landscape exploration from a vulnerability exploitation perspective

Google Cloud

Vision: Be Mongolia Cyber TI Sharing Platform

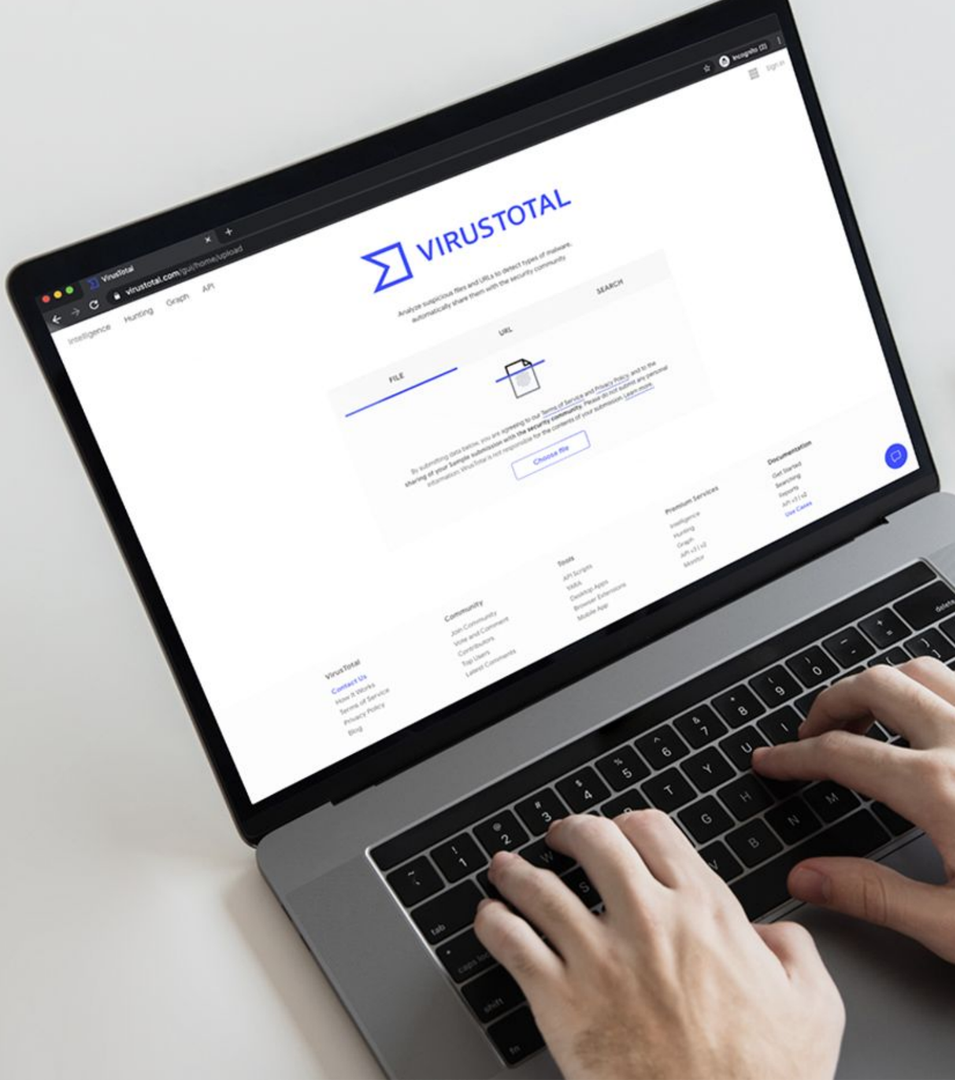
★ Welcome Mongolian own AV engine to be part of VT engines in the future

★ Welcome Mongolia different agencies to share Zero-Day with VT, like MBA

★ Welcome Mongolia Public and Private sector companies to share samples through VT

THANK YOU!

www.virustotal.com/contact



Steven Chen | Regional Lead VirusTotal - North Asia