Navigating Cyber Threat Intelligence Requirements in the Evolving Threat Landscape

Robert Wortmann

About the speaker

Robert Wortmann
Principal Security Strategist

“It's both not as bad and much worse than you think”

Many ransomware attacks are not that sophisticated as people want you to believe

Most victims leave the front door open and are not targeted

Ransomware actors want to be seen, others don’t

Worry most about the things we don't see

Living in a changing world

New geopolitical layers

Criminals or state attackers?

Attacks on parties, the EU, armies and allies

Disinformation, AI and hybrid threats

Living in a changing world

	Hacktivists	Cyber Crime	Nation-State
Motivation	Political or ideological	Financial	Political with exceptions
Targets	Various, e.g. chemical or defence companies	Random	Governments with exceptions
Skill-level	Low-to-medium	Various	High

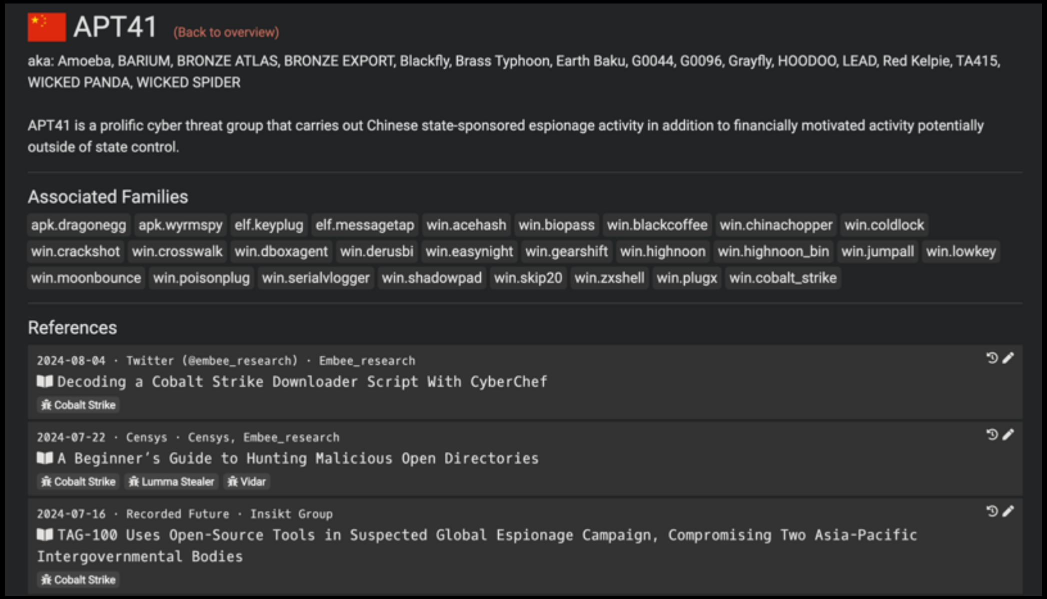
Crime groups getting ideological

Nation-state with financial motivations

Nation-state using cyber crime as proxy

Hacktivists getting sophisticated

Overlapping interests



APT41 (Back to overview)

aka: Amoeba, BARIUM, BRONZE ATLAS, BRONZE EXPORT, Blackfly, Brass Typhoon, Earth Baku, G0044, G0096, Grayfly, HOODOO, LEAD, Red Kelpie, TA415, WICKED PANDA, WICKED SPIDER

APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

Associated Families

apk.dragonegg apk.wyrmspy elf.keyplug elf.messagetap win.acehash win.biopass win.blackcoffee win.chinachopper win.coldlock win.crackshot win.crosswalk win.dboxagent win.derusbi win.easynight win.gearshift win.highnoon win.highnoon_bin win.jumpall win.lowkey win.moonbounce win.poisonplug win.serialvlogger win.shadowpad win.skip20 win.zxshell win.plugx win.cobalt_strike

References

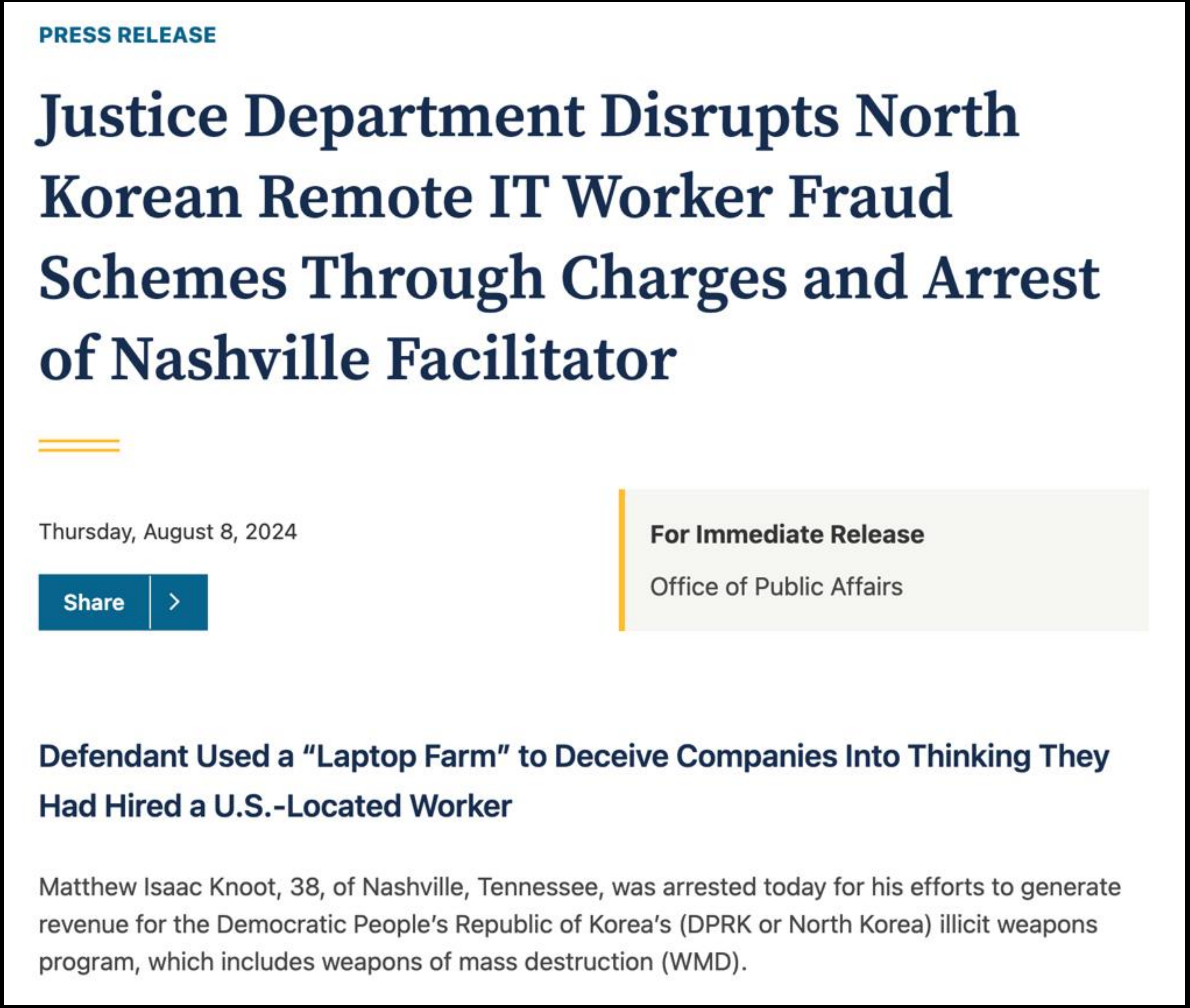
2024-08-04 · Twitter (@embee_research) · Embee_research
Decoding a Cobalt Strike Downloader Script With CyberChef
Cobalt Strike

2024-07-22 · Censys · Censys, Embee_research
A Beginner's Guide to Hunting Malicious Open Directories
Cobalt Strike · Lumma Stealer · Vidar

2024-07-16 · Recorded Future · Insikt Group
TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies
Cobalt Strike

Credits to Analyst1

The perks of remote work



PRESS RELEASE

Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator

Thursday, August 8, 2024

For Immediate Release

Office of Public Affairs

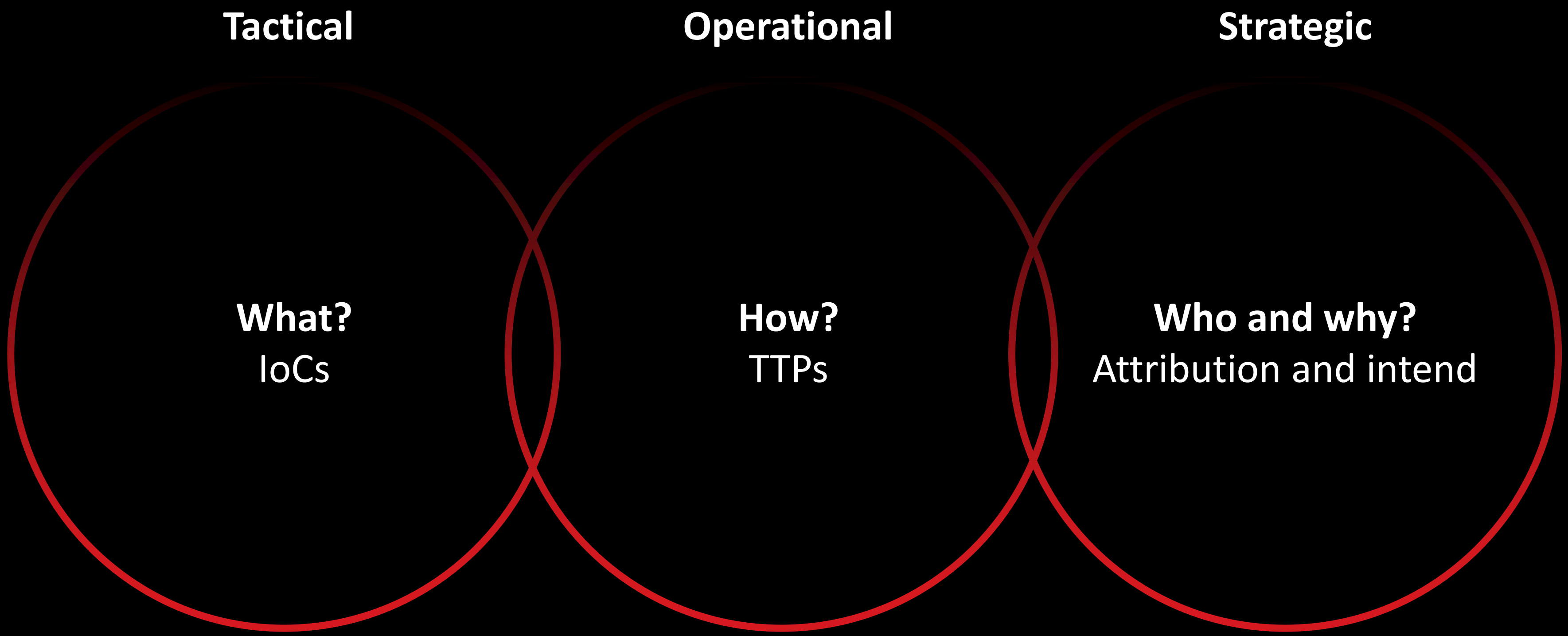
Defendant Used a "Laptop Farm" to Deceive Companies Into Thinking They Had Hired a U.S.-Located Worker

Matthew Isaac Knoot, 38, of Nashville, Tennessee, was arrested today for his efforts to generate revenue for the Democratic People's Republic of Korea's (DPRK or North Korea) illicit weapons program, which includes weapons of mass destruction (WMD).

Threat intelligence

“Threat Intelligence is not a feed!”

Threat intelligence



Tactical

What?
IoCs

Operational

How?
TTPs

Strategic

Who and why?
Attribution and intend

Understanding Risks

Is my organization being targeted right now?

Am I protected against the latest threats and exploits in the news?

What should I do next for this attack?

Is ransomware the only threat to us?

Did I catch everything about this attack?

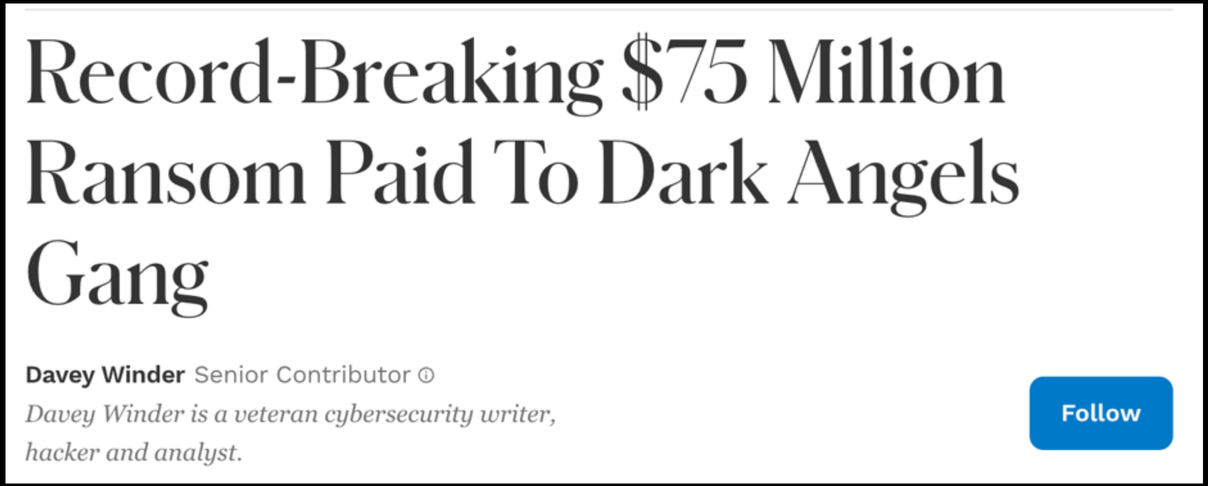
Who could be interested in us?

Breach Data

What does it really contain?

What does a breach mean besides the obvious?

Are there additional things to find?



Record-Breaking $75 Million Ransom Paid To Dark Angels Gang

Davey Winder Senior Contributor ⓘ

Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Growing attack surface

Standards versus Emerging Disruptive Technologies

Standards in data

Enables Automation

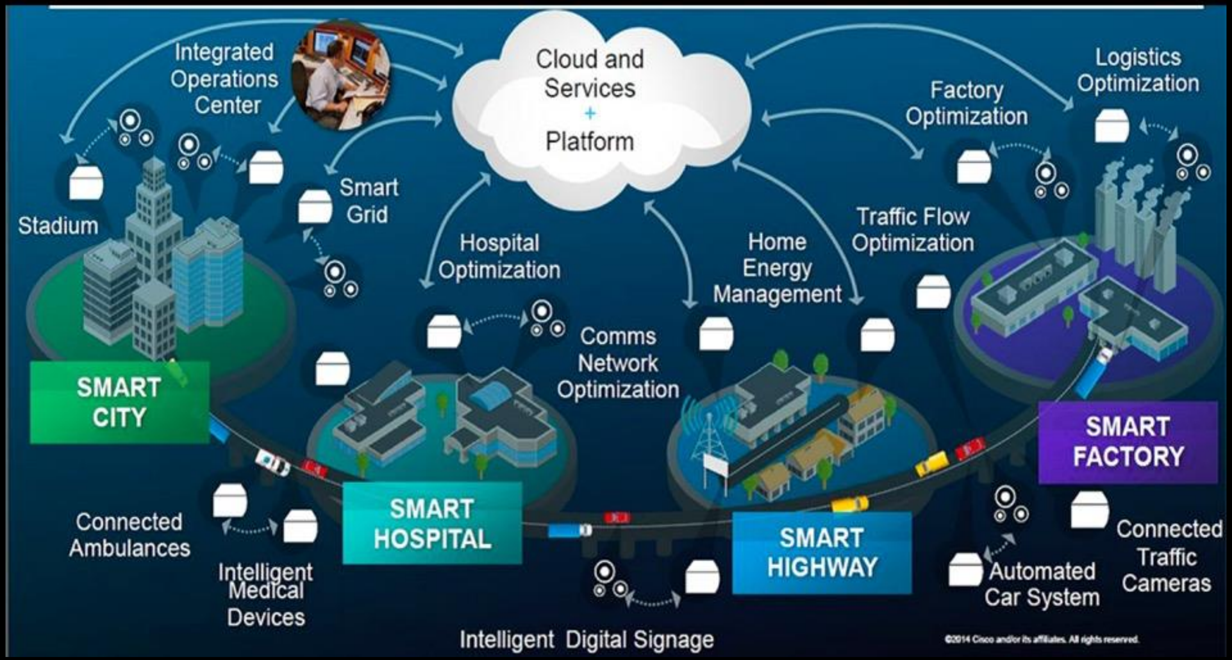
Repeatable Investigative Results

Emerging & Disruptive Technologies

Title says it all

Too new for standards

Product rush to market


Integrated Operations Center
Cloud and Services + Platform
Logistics Optimization
Factory Optimization
Smart Grid
Stadium
Hospital Optimization
Home Energy Management
Traffic Flow Optimization
Comms Network Optimization
SMART CITY
SMART HOSPITAL
SMART HIGHWAY
SMART FACTORY
Connected Ambulances
Intelligent Medical Devices
Intelligent Digital Signage
Automated Car System
Connected Traffic Cameras
©2014 Cisco and/or its affiliates. All rights reserved.

Smart Automobiles, that seems interesting

Safety

Apps that alert drivers of impending accident(s)

Uses Geo-Location, velocity, direction, and machine learning

Pedestrian, Cyclists, Automobiles

Changing the view of Mobility

Autonomous Driving

Manufacturer, Rental Companies, Startups

Convenience

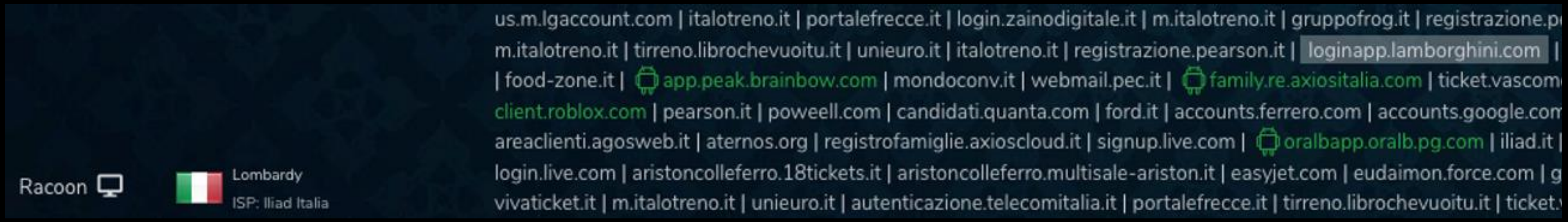
Manageable from a smart watch, phone, or laptop

Single Credential Dump

20,000+ car fleet credentials collected by stealers

5,000+ credentials for Volkswagen group, BMW

Almost all auto manufactures identified – including super-cars

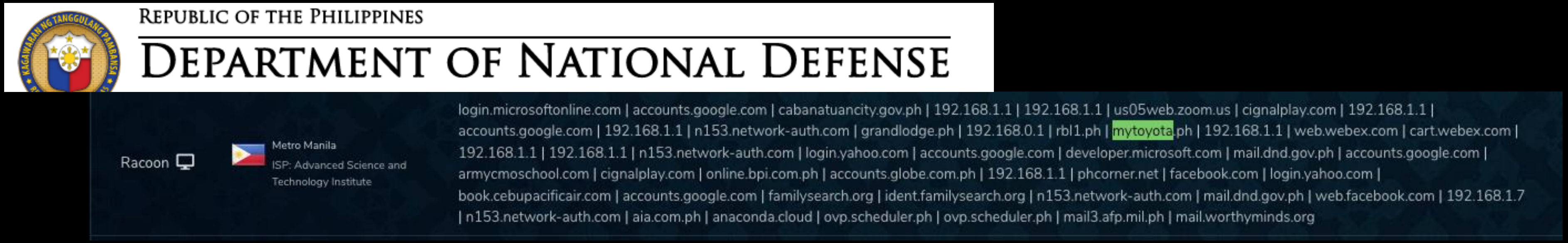


Racoon

Lombardy
ISP: Iliad Italia

```
us.m.lgaccount.com | italotreno.it | portalefrecce.it | login.zainodigitale.it | m.italotreno.it | gruppofrog.it | registrazione.p
m.italotreno.it | tirreno.librochevuoitu.it | unieuro.it | italotreno.it | registrazione.pearson.it | loginapp.lamborghini.com |
| food-zone.it | app.peak.brainbow.com | mondoconv.it | webmail.pec.it | family.re.axiositalia.com | ticket.vascom
client.roblox.com | pearson.it | poweell.com | candidati.quanta.com | ford.it | accounts.ferrero.com | accounts.google.com
areaclienti.agosweb.it | aternos.org | registrofamiglie.axioscloud.it | signup.live.com | oralbapp.oralb.pg.com | iliad.it |
login.live.com | aristoncolleferro.18tickets.it | aristoncolleferro.multisale-ariston.it | easyjet.com | eudaimon.force.com | g
vivaticket.it | m.italotreno.it | unieuro.it | autenticazione.telecomitalia.it | portalefrecce.it | tirreno.librochevuoitu.it | ticket.
```

Connecting Autos to Emails

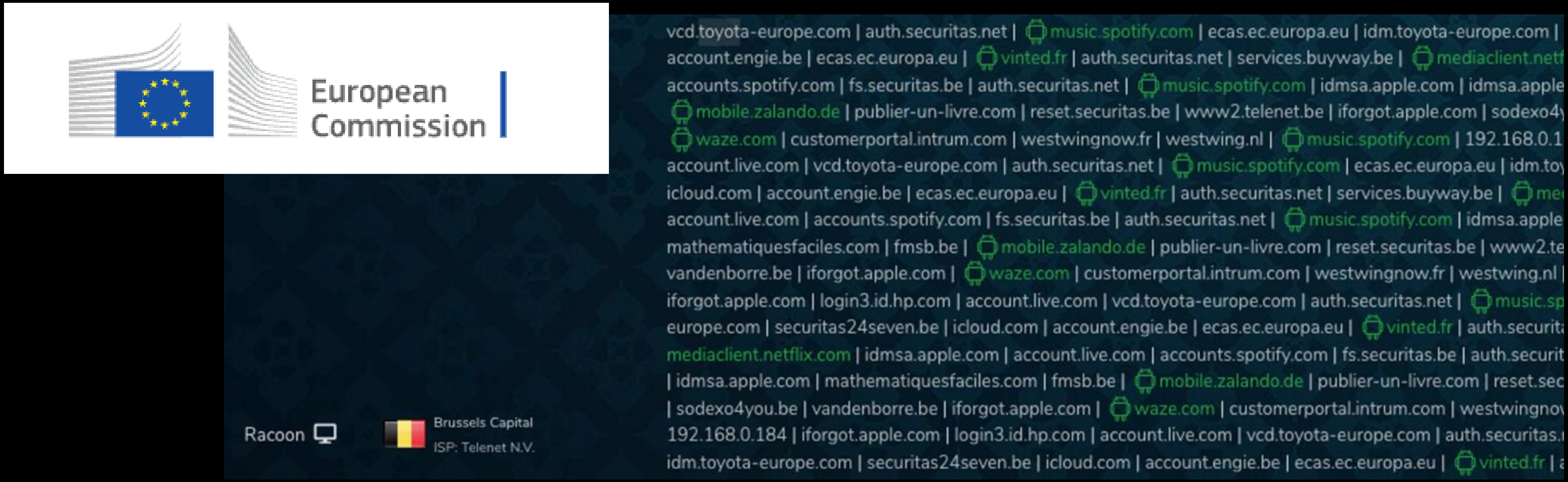


REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF NATIONAL DEFENSE

Racoon

Metro Manila
ISP: Advanced Science and Technology Institute

```
login.microsoftonline.com | accounts.google.com | cabanatuancity.gov.ph | 192.168.1.1 | 192.168.1.1 | us05web.zoom.us | cignalplay.com | 192.168.1.1 |
accounts.google.com | 192.168.1.1 | n153.network-auth.com | grandlodge.ph | 192.168.0.1 | rbl1.ph | mytoyota.ph | 192.168.1.1 | web.webex.com | cart.webex.com |
192.168.1.1 | 192.168.1.1 | n153.network-auth.com | login.yahoo.com | accounts.google.com | developer.microsoft.com | mail.dnd.gov.ph | accounts.google.com |
armycmoschool.com | cignalplay.com | online.bpi.com.ph | accounts.globe.com.ph | 192.168.1.1 | phcorner.net | facebook.com | login.yahoo.com |
book.cebupacificair.com | accounts.google.com | familysearch.org | ident.familysearch.org | n153.network-auth.com | mail.dnd.gov.ph | web.facebook.com | 192.168.1.7
| n153.network-auth.com | aia.com.ph | anaconda.cloud | ovp.scheduler.ph | ovp.scheduler.ph | mail3.afp.mil.ph | mail.worthyminds.org
```



European Commission

Racoon

Brussels Capital
ISP: Telenet N.V.

```
vcd.toyota-europe.com | auth.securitas.net | music.spotify.com | ecas.ec.europa.eu | idm.toyota-europe.com |
account.engie.be | ecas.ec.europa.eu | vinted.fr | auth.securitas.net | services.buyway.be | mediaclient.netf
accounts.spotify.com | fs.securitas.be | auth.securitas.net | music.spotify.com | idmsa.apple.com | idmsa.apple
mobile.zalando.de | publier-un-livre.com | reset.securitas.be | www2.telenet.be | iforgot.apple.com | sodexo4y
waze.com | customerportal.intrum.com | westwingnow.fr | westwing.nl | music.spotify.com | 192.168.0.1
account.live.com | vcd.toyota-europe.com | auth.securitas.net | music.spotify.com | ecas.ec.europa.eu | idm.toy
icloud.com | account.engie.be | ecas.ec.europa.eu | vinted.fr | auth.securitas.net | services.buyway.be | me
account.live.com | accounts.spotify.com | fs.securitas.be | auth.securitas.net | music.spotify.com | idmsa.apple
mathematiquesfaciles.com | fmsb.be | mobile.zalando.de | publier-un-livre.com | reset.securitas.be | www2.te
vandenborre.be | iforgot.apple.com | waze.com | customerportal.intrum.com | westwingnow.fr | westwing.nl |
iforgot.apple.com | login3.id.hp.com | account.live.com | vcd.toyota-europe.com | auth.securitas.net | music.sp
europe.com | securitas24seven.be | icloud.com | account.engie.be | ecas.ec.europa.eu | vinted.fr | auth.securit
mediaclient.netflix.com | idmsa.apple.com | account.live.com | accounts.spotify.com | fs.securitas.be | auth.securit
| idmsa.apple.com | mathematiquesfaciles.com | fmsb.be | mobile.zalando.de | publier-un-livre.com | reset.sec
| sodexo4you.be | vandenborre.be | iforgot.apple.com | waze.com | customerportal.intrum.com | westwingnov
192.168.0.184 | iforgot.apple.com | login3.id.hp.com | account.live.com | vcd.toyota-europe.com | auth.securitas.
idm.toyota-europe.com | securitas24seven.be | icloud.com | account.engie.be | ecas.ec.europa.eu | vinted.fr | a
```

Smart Car = Mobile 360 Surveillance Platform

- Supports physical crimes
- Assymetrical support during critical events
- State sponsored attacks (espionage)
- Target high profile figures
  - Politicians, C-Level executives, Media Influencers, etc.

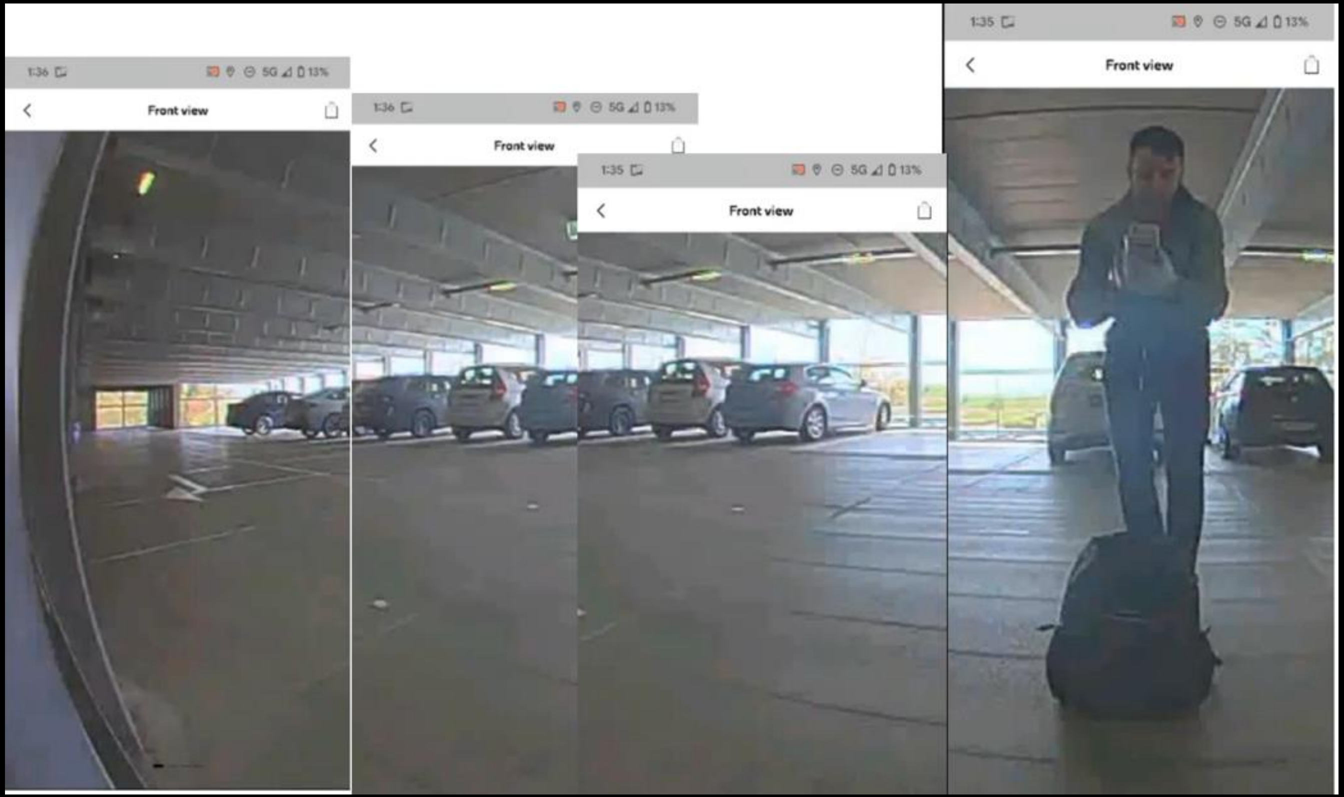
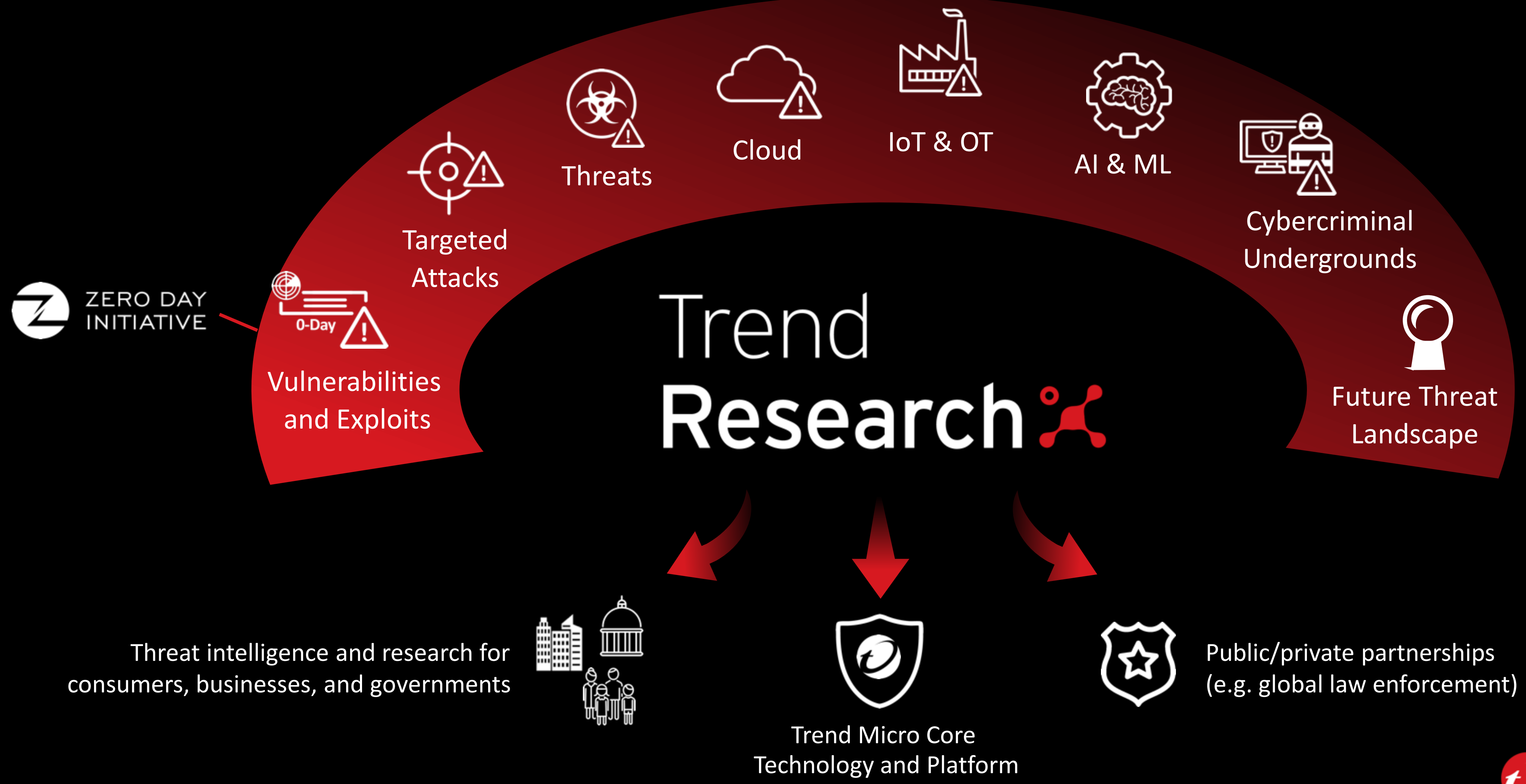


Image of researcher in Munich Germany, captured via the external cameras of a Car – by colleagues located in Taiwan, China, and France

Where Does Our Data Come From?



ZERO DAY INITIATIVE

0-Day

Vulnerabilities and Exploits

Targeted Attacks

Threats

Cloud

IoT & OT

AI & ML

Cybercriminal Undergrounds

Future Threat Landscape

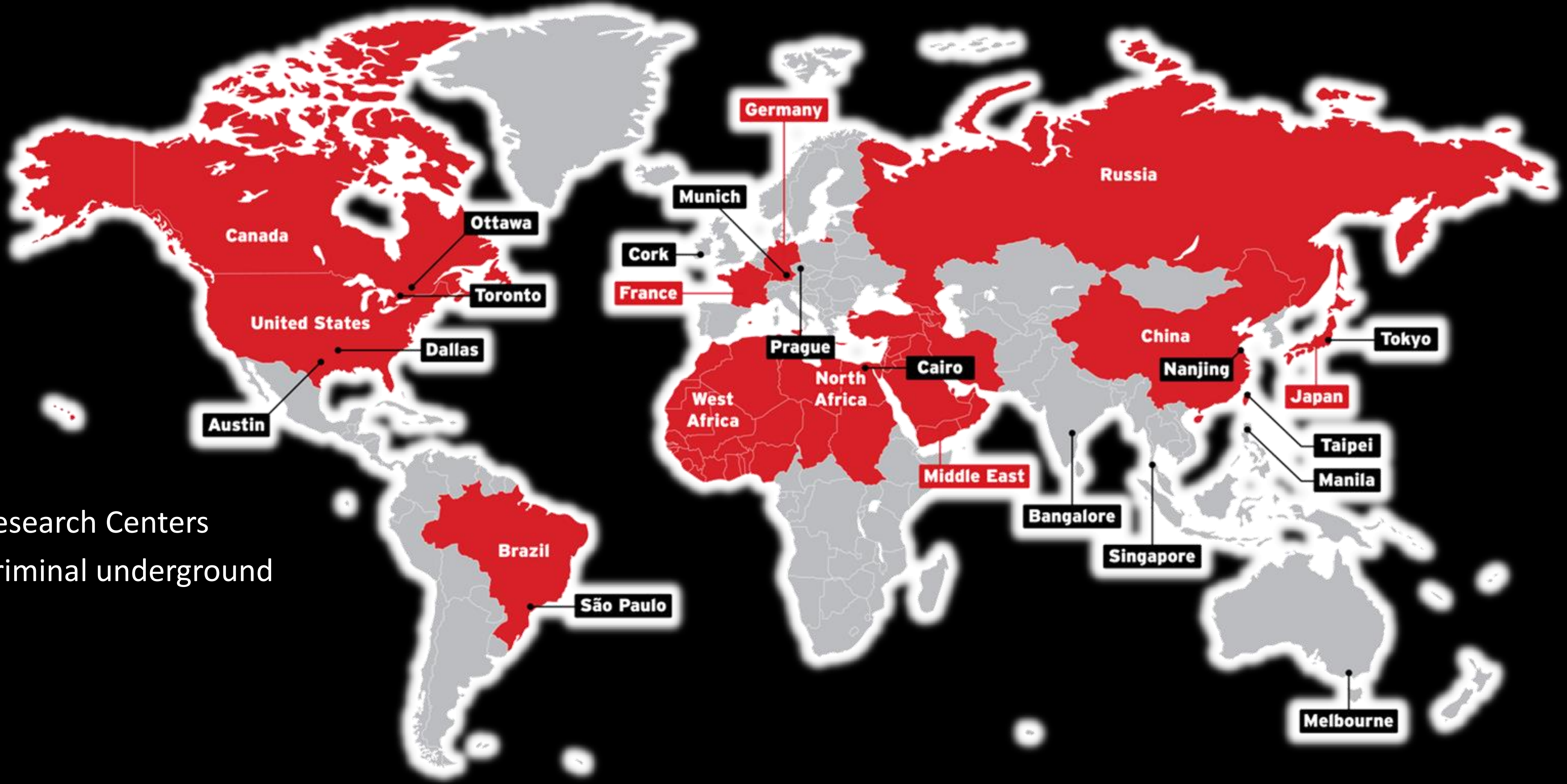
Trend Research

Threat intelligence and research for consumers, businesses, and governments

Trend Micro Core Technology and Platform

Public/private partnerships (e.g. global law enforcement)

Local Research Critical to Understanding Global Threats



- ⬛ Trend Micro Research Centers
- 🟥 Recent cybercriminal underground investigations

More is not Better!

88% of respondents strongly agree or agree that

it is hard to sort through noisy information to find what’s relevant to their organization.

69% of respondents strongly agree or agree that

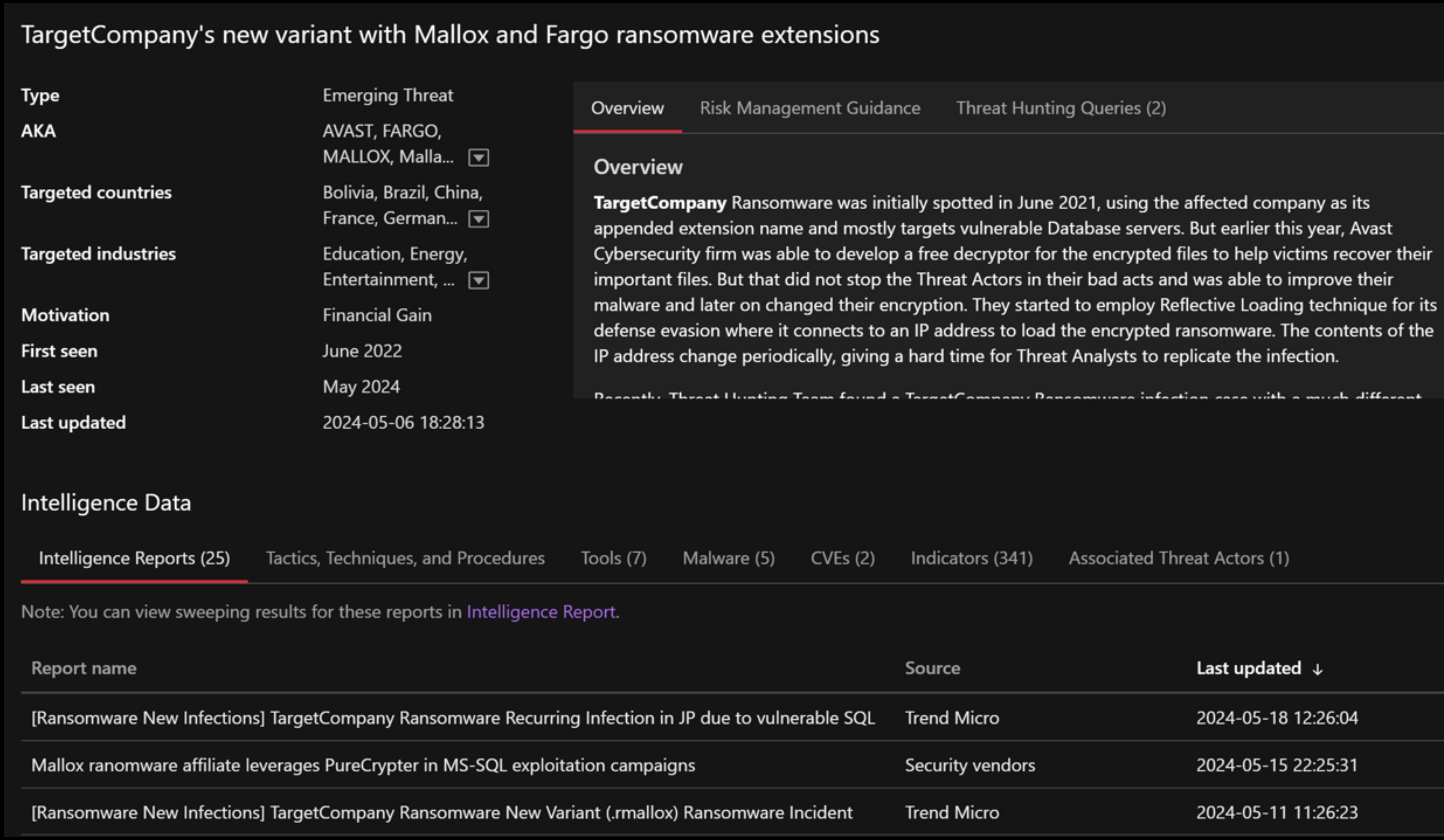
it is difficult to gauge the quality of different feeds/sources.

- “The Good, Bad, and Ugly of Enterprise Cyber-threat Intelligence Programs” by Enterprise Strategy Group, June 2023

Know what you’re up against

Deep insights on Emerging Threats and Threat Actors at your fingertips

Get to know your adversaries; who they are, what they want, and how they plan to get it.



TargetCompany's new variant with Mallox and Fargo ransomware extensions

Type	Emerging Threat
AKA	AVAST, FARGO, MALLOX, Malla... ▾
Targeted countries	Bolivia, Brazil, China, France, German... ▾
Targeted industries	Education, Energy, Entertainment, ... ▾
Motivation	Financial Gain
First seen	June 2022
Last seen	May 2024
Last updated	2024-05-06 18:28:13

Overview

TargetCompany Ransomware was initially spotted in June 2021, using the affected company as its appended extension name and mostly targets vulnerable Database servers. But earlier this year, Avast Cybersecurity firm was able to develop a free decryptor for the encrypted files to help victims recover their important files. But that did not stop the Threat Actors in their bad acts and was able to improve their malware and later on changed their encryption. They started to employ Reflective Loading technique for its defense evasion where it connects to an IP address to load the encrypted ransomware. The contents of the IP address change periodically, giving a hard time for Threat Analysts to replicate the infection.

Recently, Threat Hunting Team found a TargetCompany Ransomware infection case with a much different

Intelligence Data

Intelligence Reports (25)
Tactics, Techniques, and Procedures
Tools (7)
Malware (5)
CVEs (2)
Indicators (341)
Associated Threat Actors (1)

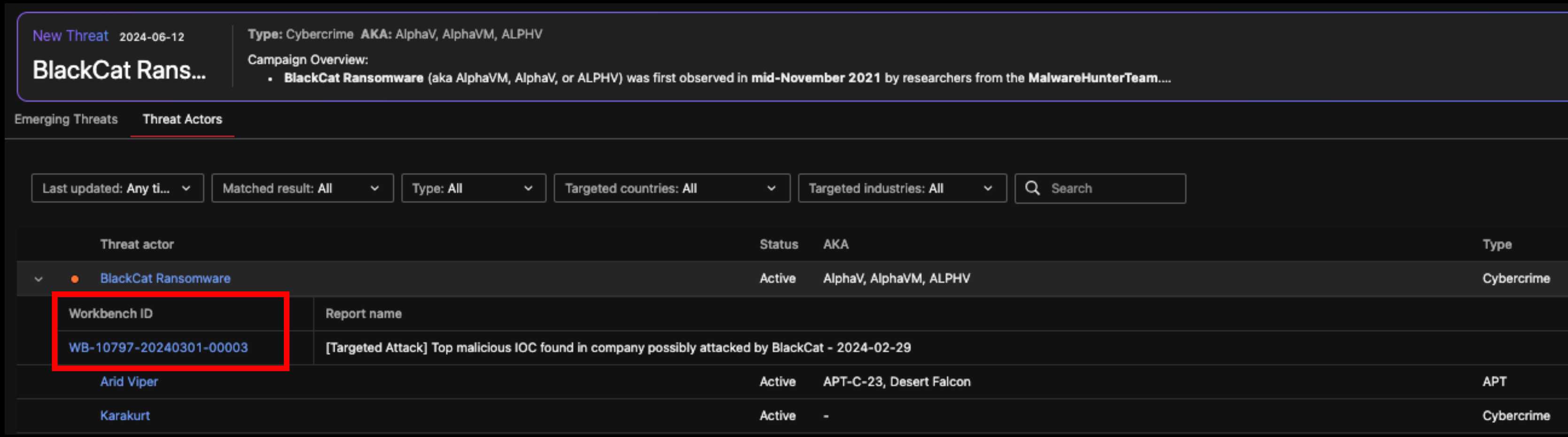
Note: You can view sweeping results for these reports in Intelligence Report.

Report name	Source	Last updated ↓
[Ransomware New Infections] TargetCompany Ransomware Recurring Infection in JP due to vulnerable SQL	Trend Micro	2024-05-18 12:26:04
Mallox ranomware affiliate leverages PureCrypter in MS-SQL exploitation campaigns	Security vendors	2024-05-15 22:25:31
[Ransomware New Infections] TargetCompany Ransomware New Variant (.rmallox) Ransomware Incident	Trend Micro	2024-05-11 11:26:23

Enrich XDR Alert Investigation

Enhance XDR workbench alerts with detailed threat intelligence

Know the "who, why and how" behind the attack



New Threat 2024-06-12

BlackCat Rans...

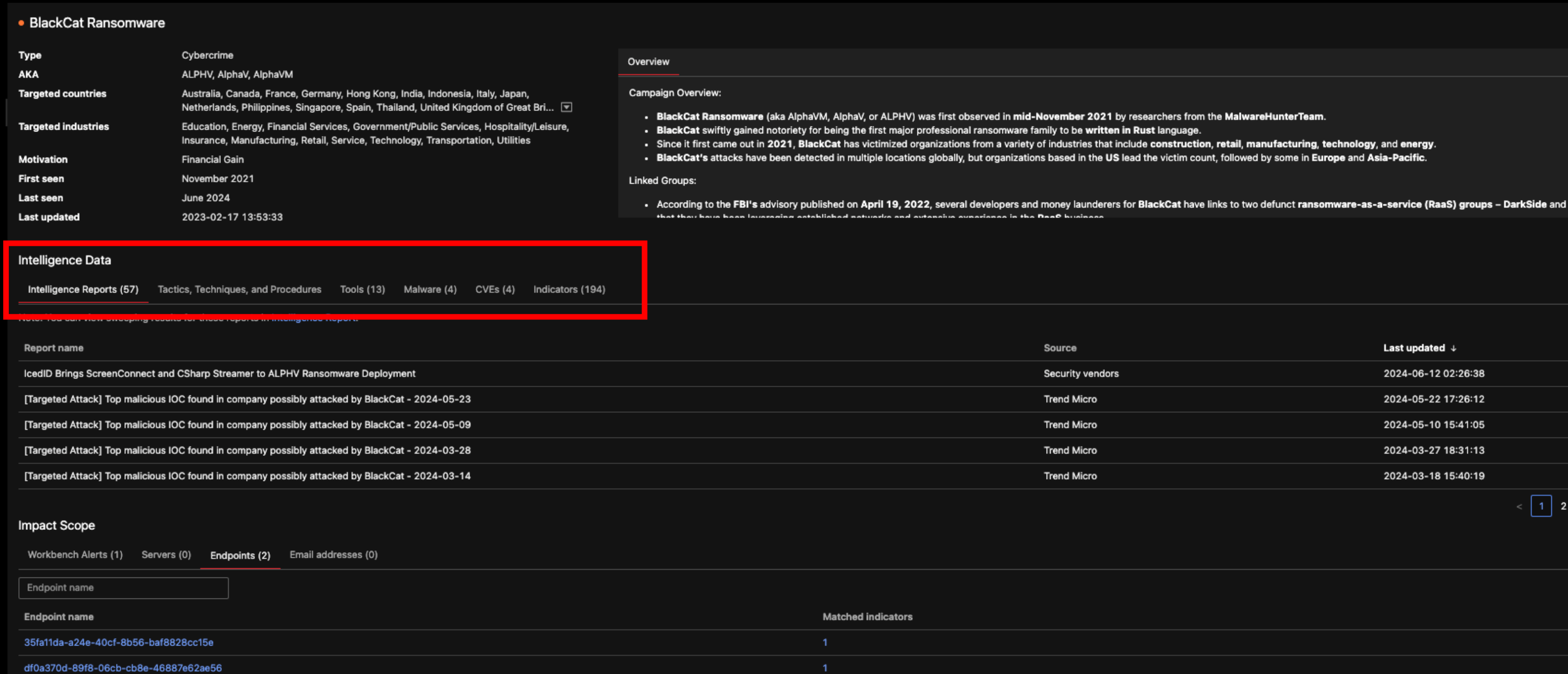
Type: Cybercrime **AKA:** AlphaV, AlphaVM, ALPHV

Campaign Overview:

- **BlackCat Ransomware** (aka AlphaVM, AlphaV, or ALPHV) was first observed in **mid-November 2021** by researchers from the **MalwareHunterTeam**....

Threat actor	Status	AKA	Type
BlackCat Ransomware	Active	AlphaV, AlphaVM, ALPHV	Cybercrime
Arid Viper	Active	APT-C-23, Desert Falcon	APT
Karakurt	Active	-	Cybercrime

Workbench ID	Report name
WB-10797-20240301-00003	[Targeted Attack] Top malicious IOC found in company possibly attacked by BlackCat - 2024-02-29



BlackCat Ransomware

Type	Cybercrime
AKA	ALPHV, AlphaV, AlphaVM
Targeted countries	Australia, Canada, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Netherlands, Philippines, Singapore, Spain, Thailand, United Kingdom of Great Bri...
Targeted industries	Education, Energy, Financial Services, Government/Public Services, Hospitality/Leisure, Insurance, Manufacturing, Retail, Service, Technology, Transportation, Utilities
Motivation	Financial Gain
First seen	November 2021
Last seen	June 2024
Last updated	2023-02-17 13:53:33

Campaign Overview:

- **BlackCat Ransomware** (aka AlphaVM, AlphaV, or ALPHV) was first observed in **mid-November 2021** by researchers from the **MalwareHunterTeam**.
- **BlackCat** swiftly gained notoriety for being the first major professional ransomware family to be **written in Rust** language.
- Since it first came out in **2021**, **BlackCat** has victimized organizations from a variety of industries that include **construction**, **retail**, **manufacturing**, **technology**, and **energy**.
- **BlackCat's** attacks have been detected in multiple locations globally, but organizations based in the **US** lead the victim count, followed by some in **Europe** and **Asia-Pacific**.

Linked Groups:

- According to the **FBI's** advisory published on **April 19, 2022**, several developers and money launderers for **BlackCat** have links to two defunct **ransomware-as-a-service (RaaS) groups – DarkSide** and

Intelligence Data

Intelligence Reports (57)
Tactics, Techniques, and Procedures
Tools (13)
Malware (4)
CVEs (4)
Indicators (194)

Report name	Source	Last updated ↓
IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment	Security vendors	2024-06-12 02:26:38
[Targeted Attack] Top malicious IOC found in company possibly attacked by BlackCat - 2024-05-23	Trend Micro	2024-05-22 17:26:12
[Targeted Attack] Top malicious IOC found in company possibly attacked by BlackCat - 2024-05-09	Trend Micro	2024-05-10 15:41:05
[Targeted Attack] Top malicious IOC found in company possibly attacked by BlackCat - 2024-03-28	Trend Micro	2024-03-27 18:31:13
[Targeted Attack] Top malicious IOC found in company possibly attacked by BlackCat - 2024-03-14	Trend Micro	2024-03-18 15:40:19

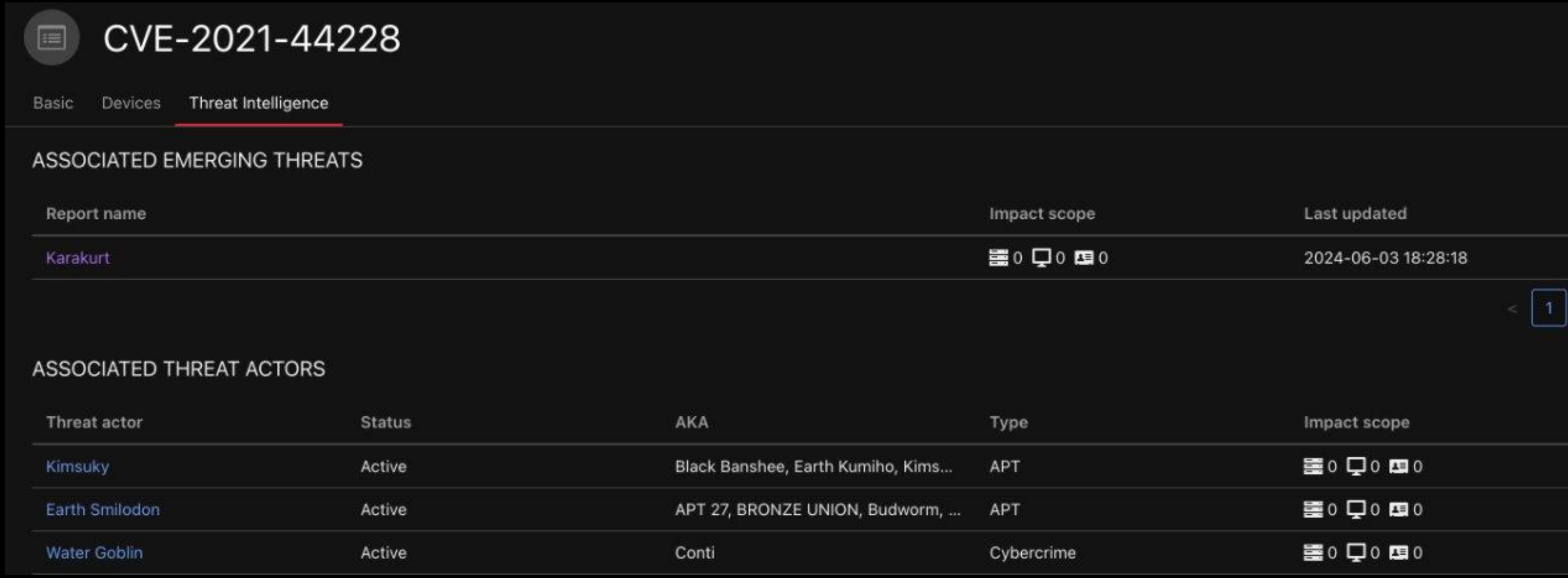
Impact Scope

Endpoint name	Matched indicators
35fa11da-a24e-40cf-8b56-baf8828cc15e	1
df0a370d-89f8-06cb-cb8e-46887e62ae56	1

Elevate ASRM vulnerability management

Get emerging threats, threat actors and hunting queries associated with the specific CVEs in your environment

Enables faster, better risk management decision



CVE-2021-44228

Basic | Devices | Threat Intelligence

ASSOCIATED EMERGING THREATS

Report name	Impact scope	Last updated
Karakurt	▤ 0 🖵 0 🪪 0	2024-06-03 18:28:18

< 1

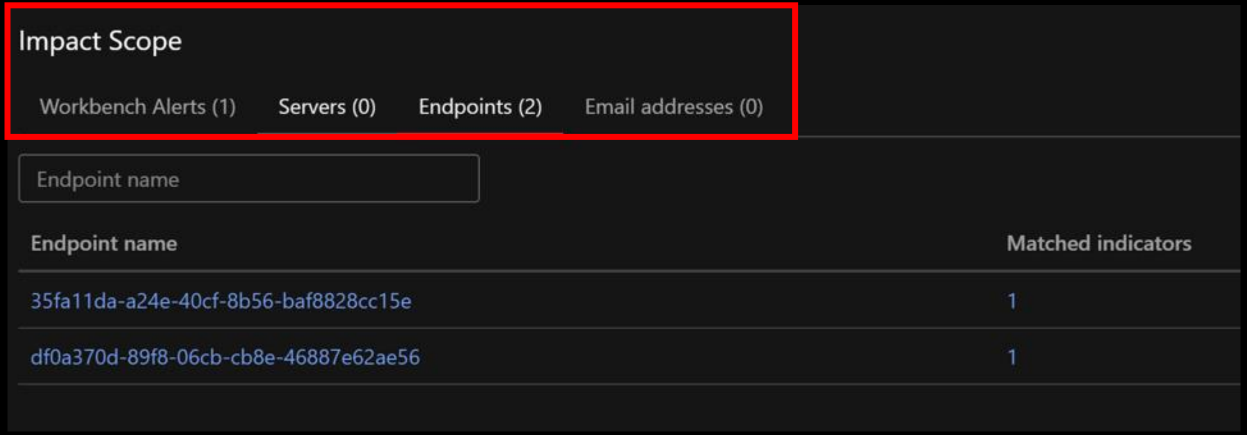
ASSOCIATED THREAT ACTORS

Threat actor	Status	AKA	Type	Impact scope
Kimsuky	Active	Black Banshee, Earth Kumiho, Kims...	APT	▤ 0 🖵 0 🪪 0
Earth Smilodon	Active	APT 27, BRONZE UNION, Budworm, ...	APT	▤ 0 🖵 0 🪪 0
Water Goblin	Active	Conti	Cybercrime	▤ 0 🖵 0 🪪 0

Take proactive action

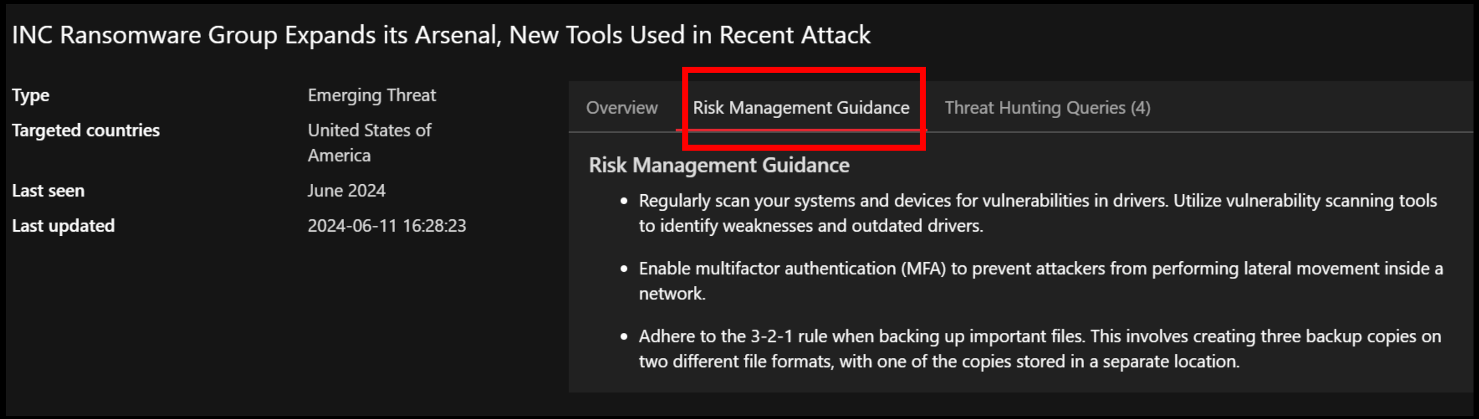
Plan your defenses

Understand where you’re most vulnerable and take action based on risk mitigation recommendations



Impact Scope

Endpoint name	Matched indicators
35fa11da-a24e-40cf-8b56-baf8828cc15e	1
df0a370d-89f8-06cb-cb8e-46887e62ae56	1



INC Ransomware Group Expands its Arsenal, New Tools Used in Recent Attack

Type	Emerging Threat
Targeted countries	United States of America
Last seen	June 2024
Last updated	2024-06-11 16:28:23

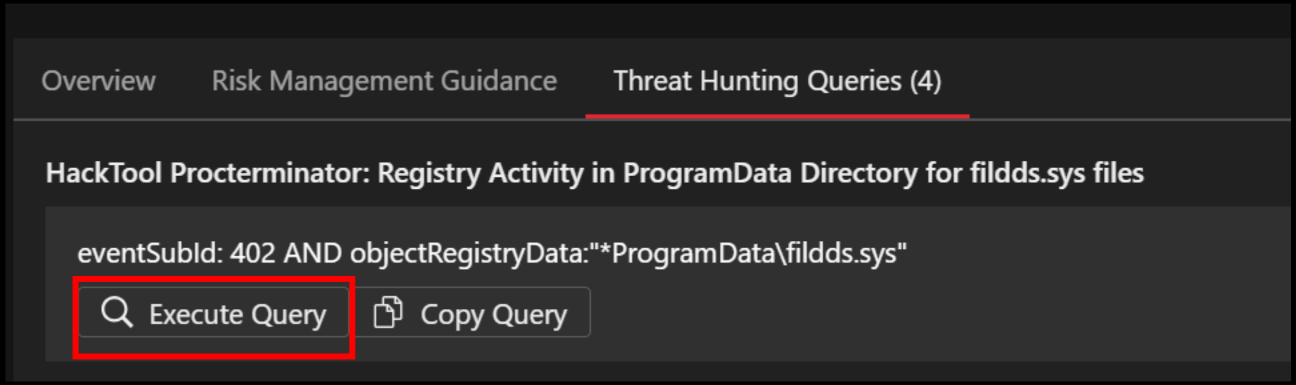
Risk Management Guidance

- Regularly scan your systems and devices for vulnerabilities in drivers. Utilize vulnerability scanning tools to identify weaknesses and outdated drivers.
- Enable multifactor authentication (MFA) to prevent attackers from performing lateral movement inside a network.
- Adhere to the 3-2-1 rule when backing up important files. This involves creating three backup copies on two different file formats, with one of the copies stored in a separate location.

Hunt them down

Get threat hunting queries and results instantly

Leave no stone unturned with threat hunting queries to track down specific indicators



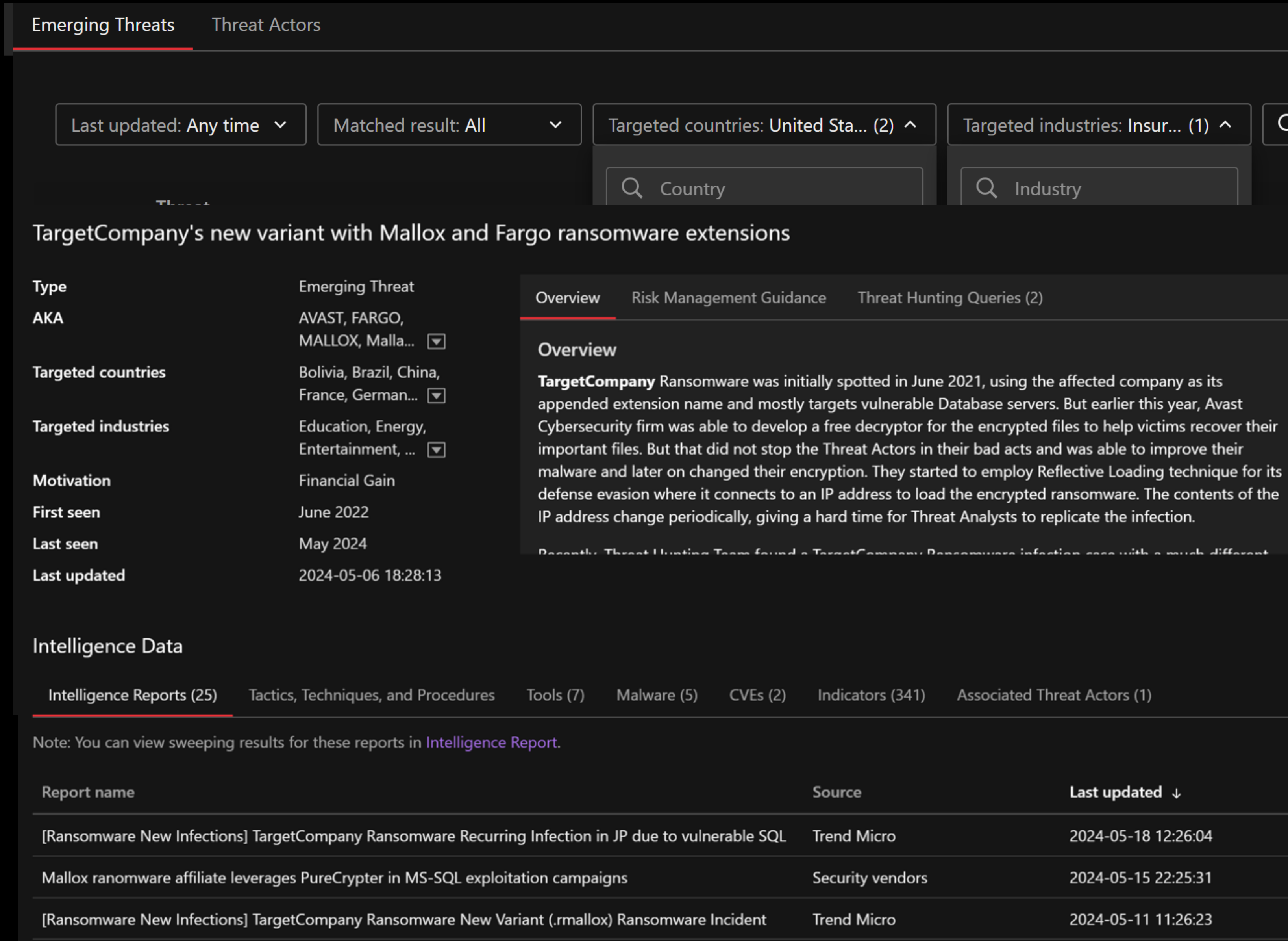
HackTool Procterminator: Registry Activity in ProgramData Directory for fildds.sys files

```
eventSubId: 402 AND objectRegistryData:"*ProgramData\fildds.sys"
```

See Threats Coming

Filter emerging threats and actors in your region and industry

Take actions ahead of upcoming threats



Last updated: Any time

Matched result: All

Targeted countries: United Sta... (2)

Targeted industries: Insur... (1)

TargetCompany's new variant with Mallox and Fargo ransomware extensions

Type	Emerging Threat
AKA	AVAST, FARGO, MALLOX, Malla...
Targeted countries	Bolivia, Brazil, China, France, German...
Targeted industries	Education, Energy, Entertainment, ...
Motivation	Financial Gain
First seen	June 2022
Last seen	May 2024
Last updated	2024-05-06 18:28:13

Overview

TargetCompany Ransomware was initially spotted in June 2021, using the affected company as its appended extension name and mostly targets vulnerable Database servers. But earlier this year, Avast Cybersecurity firm was able to develop a free decryptor for the encrypted files to help victims recover their important files. But that did not stop the Threat Actors in their bad acts and was able to improve their malware and later on changed their encryption. They started to employ Reflective Loading technique for its defense evasion where it connects to an IP address to load the encrypted ransomware. The contents of the IP address change periodically, giving a hard time for Threat Analysts to replicate the infection.

Recently, Threat Hunting Team found a TargetCompany Ransomware infection case with a much different

Intelligence Data

Intelligence Reports (25)
Tactics, Techniques, and Procedures
Tools (7)
Malware (5)
CVEs (2)
Indicators (341)
Associated Threat Actors (1)

Note: You can view sweeping results for these reports in Intelligence Report.

Report name	Source	Last updated ↓
[Ransomware New Infections] TargetCompany Ransomware Recurring Infection in JP due to vulnerable SQL	Trend Micro	2024-05-18 12:26:04
Mallox ranomware affiliate leverages PureCrypter in MS-SQL exploitation campaigns	Security vendors	2024-05-15 22:25:31
[Ransomware New Infections] TargetCompany Ransomware New Variant (.rmallox) Ransomware Incident	Trend Micro	2024-05-11 11:26:23

TREND MICRO™ | Global Leader in Cybersecurity

Robert Wortmann