25.09.2025

INVISIBLE THREATS, VISIBLE PROTECTION – Powered by ESET TI

Mungunshagai.N

PRESALES SUPPORT ENGINEER

Digital Security
Progress. Protected.

AGENDA

1. About ESET and ESET THREAT INTELLIGENCE /ETI/
2. ETI DATA FEED
3. ETI APT REPORTS & NEWS
4. ESET ADVISE

About ESET

30+ years in the market

Private company, no debt

Always focused on technology

Biggest European Union vendor

Growing YoY since its inception

Owned by original founders

Strong values

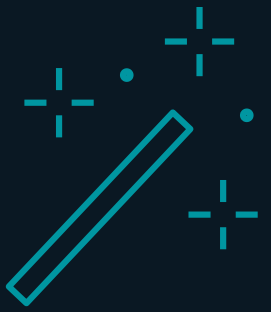
Progress. Protected.

OUR PRINCIPLES

Reliability

High Detection

Low Performance impact



Ease of use

ESET International Collaborations

ESET is one of the most actCKive MITRE ATT& contributors, and one of the most referenced sources

Long-standing and active cooperation with law enforcement agencies, such as the FBI, to crack down on cybercriminal gangs

Member of the Joint Cyber Defense Collaborative | CISA

Regular participant in NATO's Locked Shields military exercises

ESET THREAT INTELLIGENCE

1bn+
protected devices

400 000+
business customers

360° - 24/7
global coverage

750 000 suspicious samples received every day

2 500 000 000 URLs analyzed every day

500 000 unique URLs daily blocked

60 000 000 metadata records processed every day

Headquarters
Bratislava

Regional Centers
San Diego
Buenos Aires
Singapore

Research and Development Centers
Bratislava
San Diego
Buenos Aires
Singapore
Prague
Kosice
Krakow
Montreal
Zilina
Iași
Brno
Taunton

Offices
Prague
Jablonec and Nisou
Sao Paulo
Jena
Krakow
Sydney
Taunton
Bournemouth
Toronto
Montreal
Iași
Mexico City
Zilina
Brno
Tokyo
Milan

Why ESET Threat Intelligence

Highly curated
& actionable

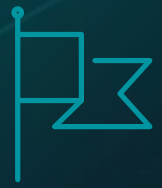
Unique geographical coverage from own telemetry

Trusted threat intelligence partner

Sectors

Government and governmental organizations

Defense sector



Diplomatic missions, diplomats

Energy sector & Critical Infrastructure

Finance, cryptocurrency sector

Sources

Threat telemetry

from sensors utilizing ESET multilayered protection

Threat tracking

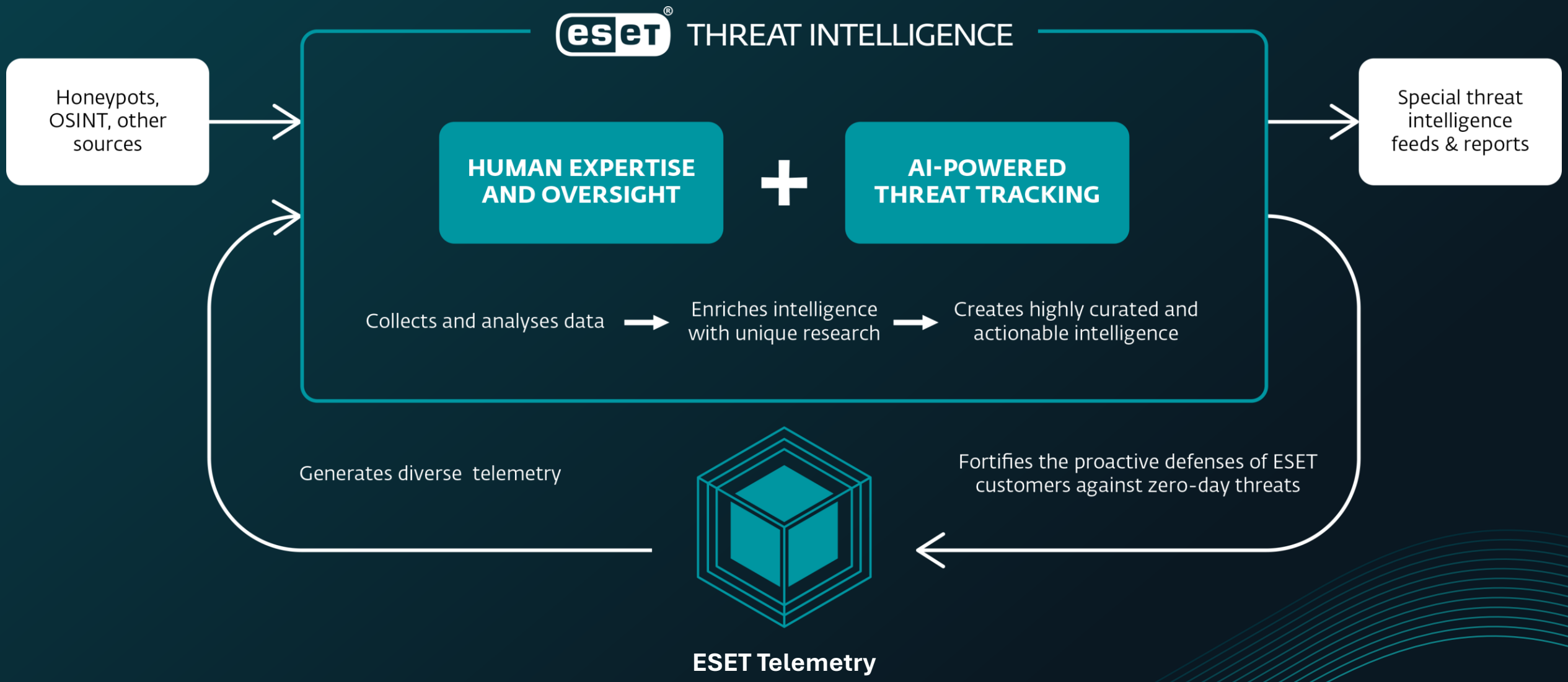
Many backend and detection systems

OSINT, honeypots and other data sources

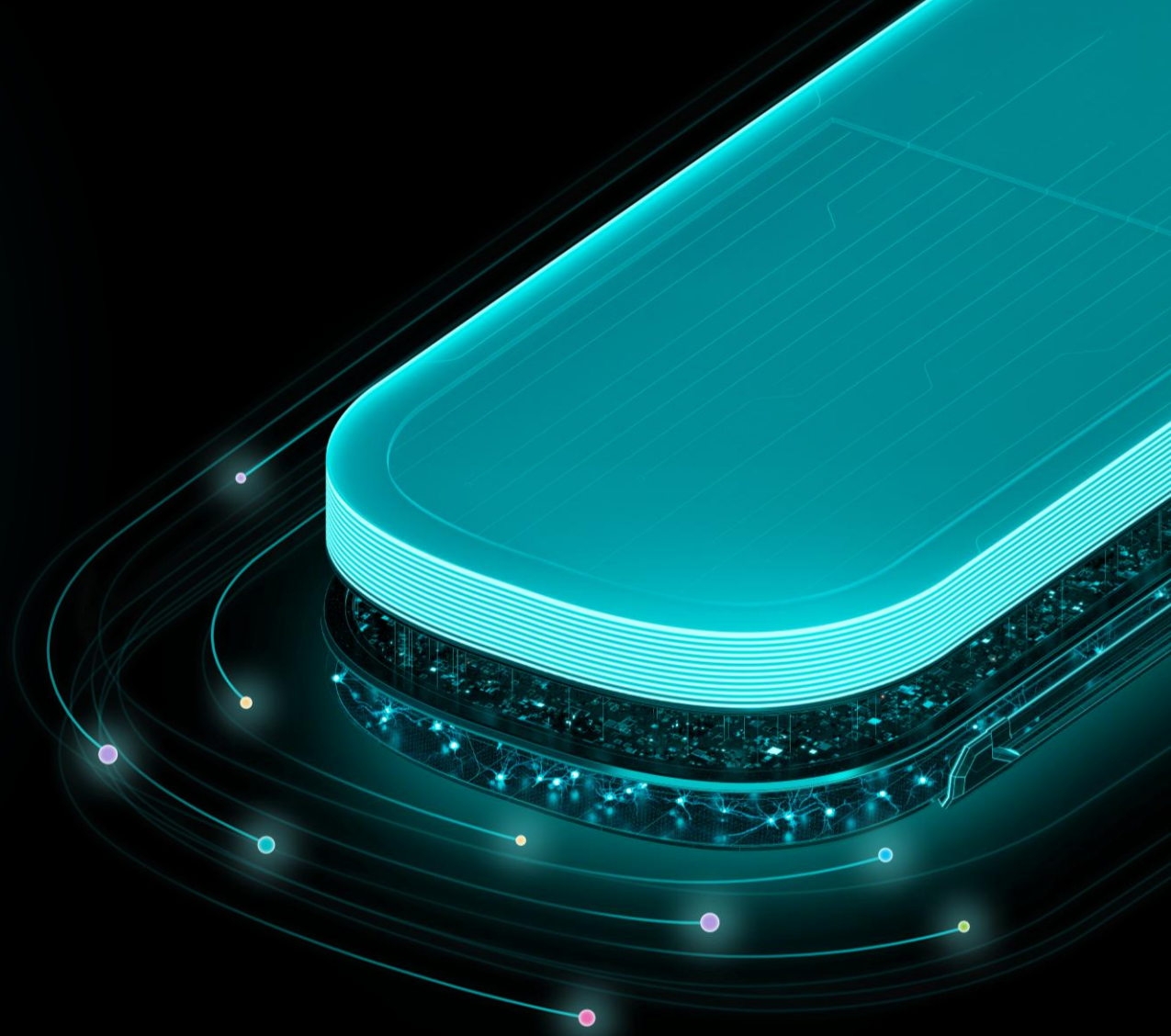
ESET TI Analysts & Researchers

Researchers study and analyze various threat actors, TTPs and tools.

ESET Threat Intelligence



Data Feeds



ESET THREAT INTELLIGENCE

Provides real-time global knowledge gathered by ESET experts on targeted attacks, advanced persistent threats, zero-days and botnet activities.

Shared in the form of **data feeds**:

JSON and STIX v2.0 formats	Via **TAXII** server, updated several times every hour	Indicators of Compromise (**IoCs**)	**Out-of-the-box integrations** with Threat Intelligence Platforms

- Botnet Feed
- Domain Feed
- URL Feed
- Malicious Files Feed
- IP Feed
- APT Feed
- Android infostealer feed
- Android threats feed
- Cryptoscam feed
- Malicious email attachments feed
- Phishing URL feed
- Ransomware feed
- Scam URL feed
- Smishing feed
- SMS scam feed

Data Feeds

ESET feeds

- Metadata-rich and detailed, curated feeds with very low false positives
- Low size, high relevancy, deduplicated and confidence-scored data
- The result of advanced filtering, and insights from ESET researchers
- Market-leading, especially in botnet data
- Low maintenance requirements due to curated content
- Real-time feeds - only fresh and prevalent IoCs

Typical data feeds from competitors

- Just raw telemetry
- Unfiltered
- Unprocessed
- Outdated
- Requiring lots of processing on customer's side

ESET Threat Intelligence

REGIONS WITH ESET APT GROUPS REPORTS

China | Iran | Middle-East | Eastern Europe
North Korea | Russia | Central Asia | Pakistan
India | Unattributed | E-crime | East Asia

China-aligned

- EVASIVE PANDA
- GOBLIN PANDA
- KE3CHANG
- LUCKYMOUSE
- MIRRORFACE
- MUSTANG PANDA
- REDFOXTROT
- SNEAKYDRAGON
- SPARKLINGGOBLIN
- SPECCOM
- TA410
- TA428
- TICK
- WEBSIIC
- WEBWORM
- WINNTI GROUP
- WOROK
- StartupNation
- TheWizards
- FishMonger
- DigitalRecyclers
- GREF
- GALLIUM
- PerplexedGoblin
- CeranaKeeper

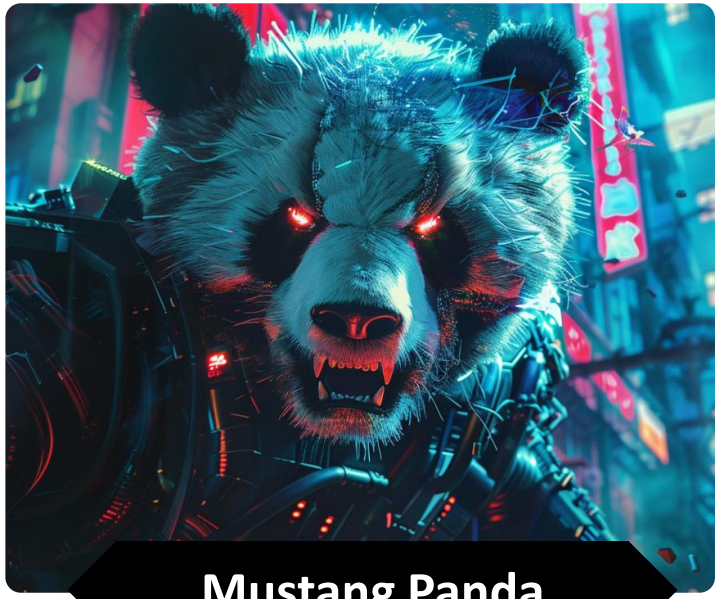

East Asia
• APT-C-60


Russia-aligned
BUHTRAP
GAMAREDON
INVISIMOLE
SAINTBEAR
SANDWORM
SEDNIT
THE DUKES
TURLA
CALLISTO
ATTOR

- KIMSUKY
- KONNI
- LAZARUS
- ANDARIEL
- SCARCRUFT
- DeceptiveDevelopment

North Korea-aligned

Mustang Panda

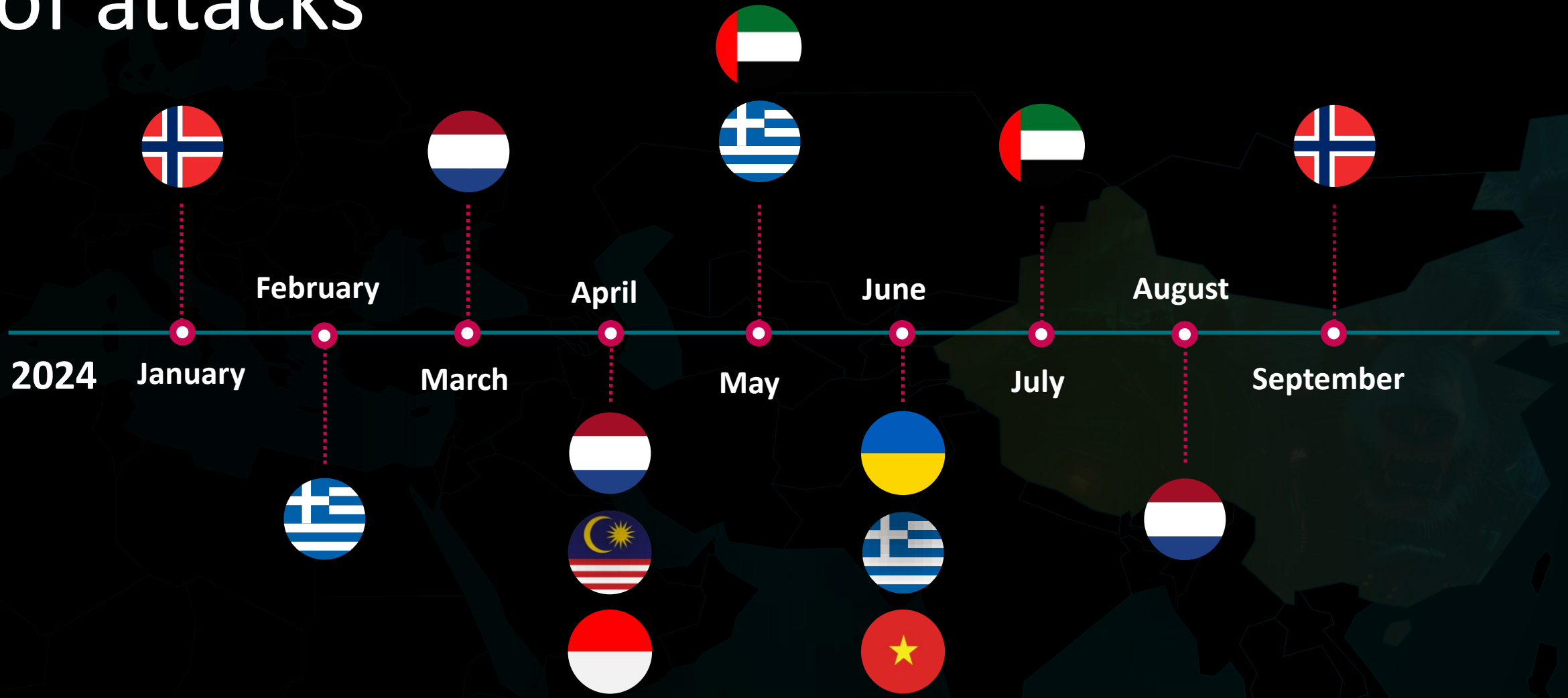


Mustang Panda

Mustang Panda is a China-based cyber espionage threat actor probably operating since at least 2014. It has targeted government entities, nonprofits, religious, and other non-governmental organizations. Mostly in East and Southeast Asia, big focus on **Mongolia.**
But also the U.S., Europe – notably attacked the Vatican in 2020

2014 | **APT Group** | China

Timeline
of attacks



LNK

JS

NSIS

MSI

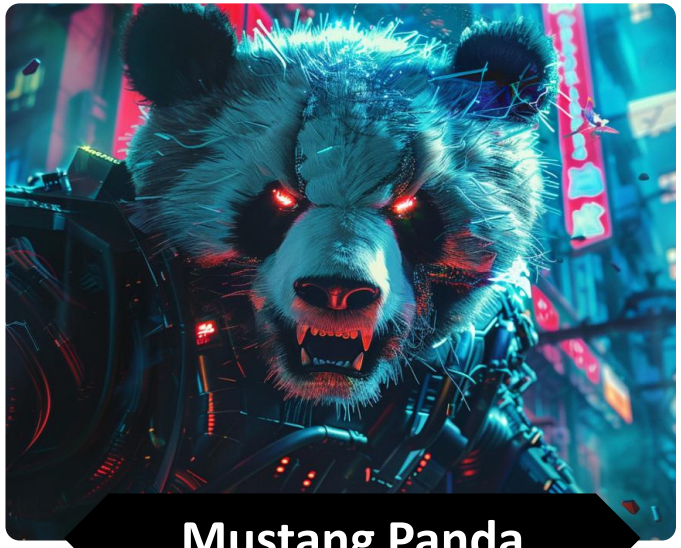
XLL

MSC

HTA

VBS

RAR



Mustang Panda

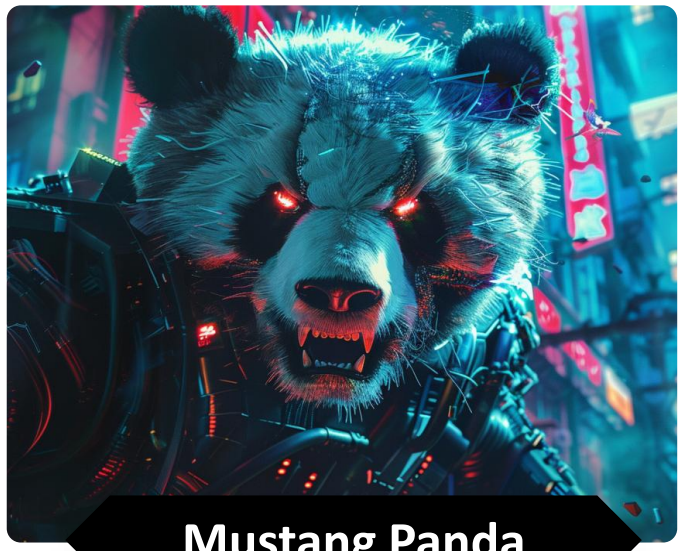
Mustang Panda is a China-based cyber espionage threat actor probably operating since at least 2014. It has targeted government entities, nonprofits, religious, and other non-governmental organizations. Mostly in East and Southeast Asia, big focus on **Mongolia**.

But also the U.S., Europe – notably attacked the Vatican in 2020

2014 | **APT Group** | China

Known TTPs

- **Spear Phishing:** Used to deliver malicious payloads, often leveraging current events as lures.
- **Custom Malware and Backdoors:** Deployment of custom loaders and backdoors like Korplug (PlugX) to maintain persistent access.
- **Exploitation of Vulnerabilities:** Targeting known vulnerabilities in software and systems.
- **Living off the Land:** Using legitimate tools and binaries to conduct operations stealthily.
- **Data Exfiltration:** Focused on exfiltrating sensitive data using encrypted channels.



Mustang Panda

Mustang Panda is a China-based cyber espionage threat actor probably operating since at least 2014. It has targeted government entities, nonprofits, religious, and other non-governmental organizations. Mostly in East and Southeast Asia, big focus on **Mongolia**.
But also the U.S., Europe – notably attacked the Vatican in 2020

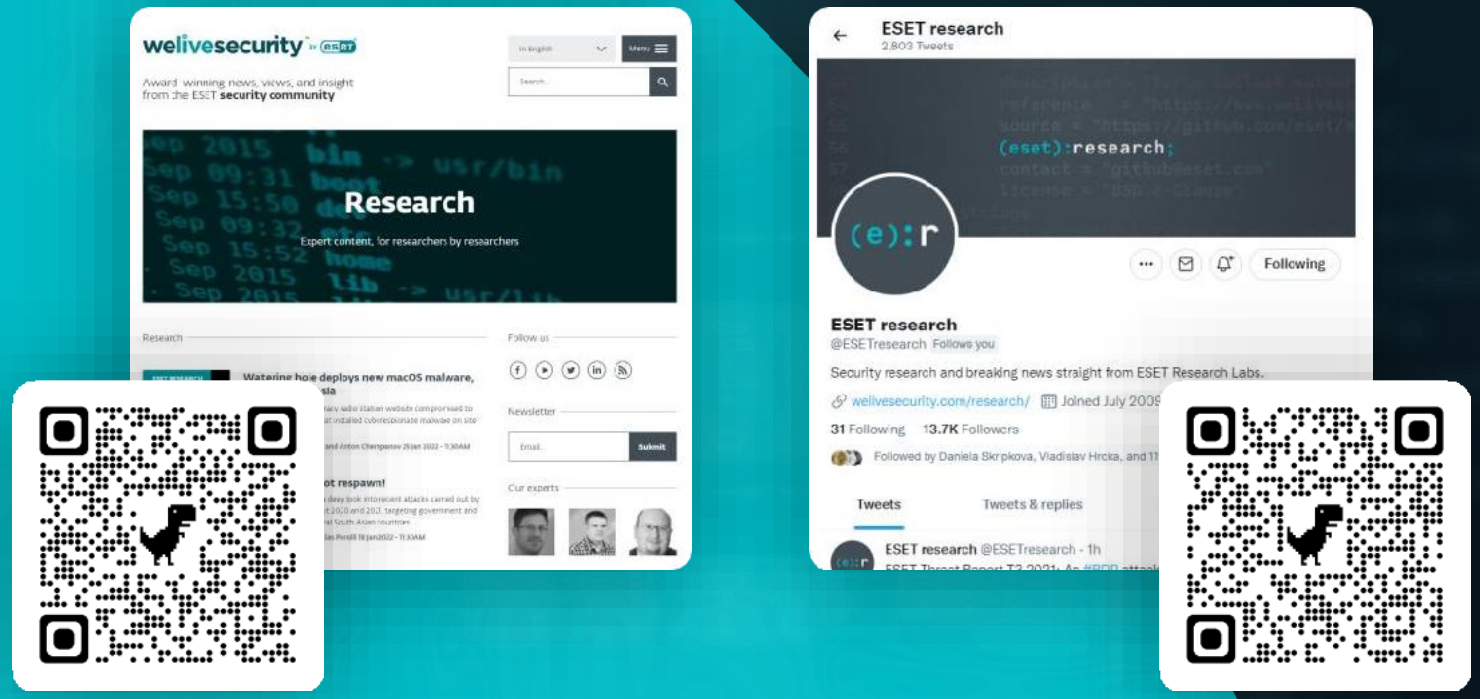
2014 | **APT Group** | China

Our Advise

- **Email Security:** Implement robust email security solutions to detect and block spear phishing attempts.
- **Patch Management:** Regularly update and patch software and systems to protect against known vulnerabilities.
- **Endpoint Protection:** Deploy comprehensive endpoint protection solutions to detect and block malware and unauthorized access attempts.
- **Incident Response Plan:** Develop and regularly update an incident response plan to quickly address and mitigate any security breaches.

Contact ESET to develop a holistic cybersecurity Defense Strategies.

Thank you!


welivesecurity
Award winning news, views, and insight from the ESET security community
Research
Expert content, for researchers by researchers
ESET research
2,803 Tweets
(eset):research;
(e):r
Following
ESET research
@ESETresearch Follows you
Security research and breaking news straight from ESET Research Labs.
welivesecurity.com/research/
31 Following
13.7K Followers
Tweets
Tweets & replies