

Implement Threat Intelligence Principles

Indicators of Compromise (IoCs) and Detection Methods

1. Suspicious IP Addresses

- Detection Methods:
 - Network traffic monitoring tools (e.g., Wireshark, Snort) can flag and analyze incoming/outgoing packets for connections with blacklisted or unusual IPs.
 - Threat intelligence feeds maintain databases of malicious IPs, which security software cross-references in real-time.
- How It Indicates Threats:
 - Frequent connections to a known malicious IP address could indicate botnet activity, data exfiltration, or unauthorized remote control by attackers.
 - Unusual spikes in traffic to obscure regions suggest potential communication with command-and-control servers.

2. Abnormal File Hashes (Malicious Executables)

- Detection Methods:
 - Endpoint security solutions like antivirus and EDR systems scan files for signature-based matches against known malware hashes
 - Tools such as VirusTotal and SHA256 checks help validate the integrity of files.
- How It Indicates Threats:
 - If a file's hash matches that of a known malicious payload, it may point to ransomware, trojans, or backdoors on the system.
 - Files with uncommon hashes may indicate polymorphic malware that changes slightly to evade signature-based detection.

localhost

Online UUID Generator ToolopenCTI | FREE Cyber Threat IntelligenceOpenCTI - Cyber Threat Intelligenceconnectors/external-import at...VirusTotal - API Key - undefinedOnline UUID Generator Tool

Search the platform...

🔍

🔍

🔔

🔄

🗖

👤

Threats / Campaigns

Search these results...

Add filter

Sort by

Name

↓

37 entitie(s)

🗖

🗖

📄

🔥

2015 Ukraine Electric Power Attack

January 29, 2025

2015 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used BlackEnergy (specifically...

KNOWN AS

USED MALWARE

-

BlackEnergy, KillDisk

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

2016 Ukraine Electric Power Attack

January 29, 2025

2016 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used Industroyer malware to target...

KNOWN AS

USED MALWARE

-

Industroyer

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

2022 Ukraine Electric Power Attack

January 29, 2025

The 2022 Ukraine Electric Power Attack was a Sandworm Team campaign that used a combination of GOGETTER, Neo...

KNOWN AS

USED MALWARE

-

CaddyWiper

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

APT41 DUST

January 29, 2025

APT41 DUST was conducted by APT41 from 2023 to July 2024 against entities in Europe, Asia, and the Middle East. APT41...

KNOWN AS

USED MALWARE

-

DUSTPAN, Cobalt Strike, DUSTTRAP

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

C0010

January 29, 2025

C0010 was a cyber espionage campaign conducted by UNC3890 that targeted Israeli shipping, government, aviation...

KNOWN AS

USED MALWARE

-

SUGARUSH, SUGARDUMP

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

C0011

January 29, 2025

C0011 was a suspected cyber espionage campaign conducted by Transparent Tribe that targeted students at universities and...

KNOWN AS

USED MALWARE

-

Crimson

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

C0015

January 29, 2025

C0015 was a ransomware intrusion during which the unidentified attackers used Bazar, Cobalt Strike, and...

KNOWN AS

USED MALWARE

-

Bazar, Conti, Cobalt Strike

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

C0017

January 29, 2025

C0017 was an APT41 campaign conducted between May 2021 and February 2022 that successfully compromised at least six U.S...

KNOWN AS

USED MALWARE

-

DEADEYE, KEYPLUG, Cobalt Strike

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

+

localhost

Online UUID Generator ToolopenCTI | FREE Cyber Threat IntelligenceOpenCTI - Cyber Threat Intelligenceconnectors/external-import at...VirusTotal - API Key - undefinedOnline UUID Generator Tool

Search the platform...

🔍

🔍

🔔

🔄

🗖

👤

Threats / Intrusion sets

Search these results...

Add filter

Sort by

Name

↓

171 entitie(s)

🗖

🗖

📄

🔥

admin@338

January 29, 2025

admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and ha...

KNOWN AS

USED MALWARE

-

PoisonIvy, LOWBALL, BUBBLEWRAP

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

Agrius

January 29, 2025

Agrius is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East,...

KNOWN AS

USED MALWARE

-

Pink Sandstorm, AMERICIUM,...

Apostle, ASPXSpy, BFG Agonizer,...

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

Ajax Security Team

January 29, 2025

Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax...

KNOWN AS

USED MALWARE

-

Operation Woolen-Goldfish, AjaxTM,...

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

Akira

January 29, 2025

Akira is a ransomware variant and ransomware deployment entity active since at least March 2023.(Citation: Arctic Wolf...

KNOWN AS

USED MALWARE

-

GOLD SAHARA, PUNK SPIDER

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

ALLANITE

January 29, 2025

ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within t...

KNOWN AS

USED MALWARE

-

Palmetto Fusion

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

Andariel

January 29, 2025

Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focuse...

KNOWN AS

USED MALWARE

-

Silent Chollima, PLUTONIUM, Onyx...

gh0st RAT, Rldoor

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

Aoqin Dragon

January 29, 2025

Aoqin Dragon is a suspected Chinese cyber espionage threat group that has been active since at least 2013. Aoqin Dragon has...

KNOWN AS

USED MALWARE

-

Heyoka Backdoor, Mongall

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

🔥

APT-C-23

January 29, 2025

APT-C-23 is a threat group that has been active since at least 2014.(Citation: symantec_mantis) APT-C-23 has primaril...

KNOWN AS

USED MALWARE

-

Mantis, Arid Viper, Desert Falcon, TAG...

FrozenCell, Desert Scorpion, Phenakite,...

TARGETED COUNTRIES

TARGETED SECTORS

-

-

No label

+