

Trellix

24-26 OCTOBER 2023

EMEA Security Summit Rome, Italy



Trellix

Threat Intelligence as a Service

November 10, 2023



Speakers Intro

Who's that Guy



Siju Ramachandradasan

Professional Services Director - EMEA



Ralph Habets

Professional Services Manager - Germany

Trellix Platform

SecOps/Analysts
IT/Ops
MSSPs

XConsole

**Security
Solutions**

**Trellix
XDR**

**Advanced
Research
Center**


Services

Integration
Advisory
Staff Augmentation
Managed (partner)

 Endpoint Security

 Data Security


 Cloud Security


 Collaboration Security

 Network Security


 3rd Party Integrations

 Product Research

 Threat Intelligence

 Adversarial Resilience

 Data Science ML / AI

 Research Engineering

Articles / News

Trellix Discovers Major Cisco Networking Device Vulnerabilities

Nancy Liu | Editor
February 1, 2023 5:08 PM

Share this article:



Thread

BleepingComputer @BleepinComputer

Scoop: FBI seized \$2.2 million in bitcoin from a wallet owned by 'Lalartu,' a well-known REvil and GandCrab ransomware affiliate.



businessline

Companies / Markets / Portfolio / Opinion / Economy

Home » Info-tech


Job-themed emails have become prime target for cybercriminals: Trellix

March 02, 2023 - Updated 06:00 pm IST

Cybercriminals using phishing and malware campaigns to target job seekers in a bid to steal sensitive information

BY BL BENGALURU BUREAU


SHARE READ LATER



Tweet

Sean Lyngaas @snlyngaas

New --> Romanian authorities have arrested two people suspected of deploying REvil ransomware and netting half a million euros in ransom payments



Trellix

Government Support Contact

Platform Services Research Partners Resources About

THE CYBERTHREAT REPORT

June 2023

Insights, Global Perspectives, Global Network of Experts, Sensors,



WIRED

LONG READS BUSINESS CULTURE GEAR SCIENCE SECURITY WEBER

SECURITY

A New Kind of Bug Spells Trouble for iOS and macOS Security

Security researchers found a class of flaws that, if exploited, would allow an attacker to access people's messages, photos, and call history.

25 JUN 2023 01:00 PM

REUTERS

World Business Markets Legal Breakingviews Technology Investigations

United Kingdom

3 minute read · April 5, 2023 10:15 PM GMT+2 · Last Updated a month ago

'Operation Cookie Monster': International police action seizes dark web market

<https://www.trellix.com/en-us/about/newsroom/stories/research.html>



The Cyberthreat Report

June 2023

Nation-State Activity Q1 -2023

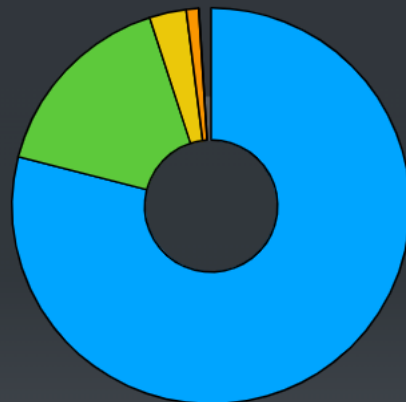
Most Prevalent Threat-Actor Countries Behind Nation-State Activity Q1 2023



79%

China accounted for a dominant majority of the nation-state-related activity in Q1 2023.

- China
- North Korea
- Russia
- Iran
- Pakistan



Most Prevalent Threat-Actor Groups Q1 2023

1. Mustang Panda	72%
2. Lazarus	17%
3. UNC4191	1%
4. Common Raven	1%
5. APT34	1%

Most Prevalent MITRE ATT&CK Techniques Used in Nation-State Activity Q1 2023

1. DLL Side-Loading	14%
2. Deobfuscate/Decode Files for Information	11%
3. Ingress Tool Transfer	10%
4. Data from Local System	10%
5. File and Directory Discovery	10%

Most Prevalent Malicious Tools Used in Nation-State Activity Q1 2023

38%

PlugX accounted for 38% of malicious nation-state activity in Q1 2023.

1. PlugX	38%
2. Cobalt Strike	35%
3. Raspberry Robin	14%
4. BLUEHAZE/DARKDEW/MISTCLOAK	3%
5. Mimikatz	3%

The Threat Intelligence Group

Part of the Advanced Research Center (ARC)

Motto: “Always Vigilant against Evil”



24/7 mission-critical insights on the evolving threat landscape

Valuable Intelligence based on:

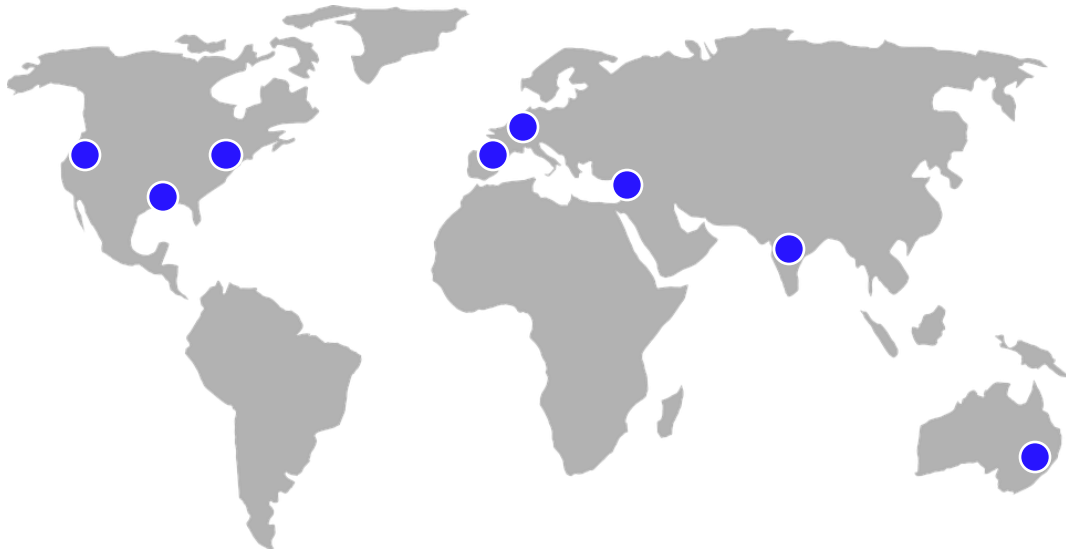
- Product integrations
- Custom intelligence collections
- In-depth research

History

- 2015 Support US Intelligence Community (IC)
- Expand service to IC agencies, defense orgs, Homeland Security, Federal law, commercial & financial orgs
- 2022 Trellix (McAfee & FireEye) ARC

<https://www.trellix.com/en-us/platform/threat-intelligence.html>

Global Threat Intelligence Group

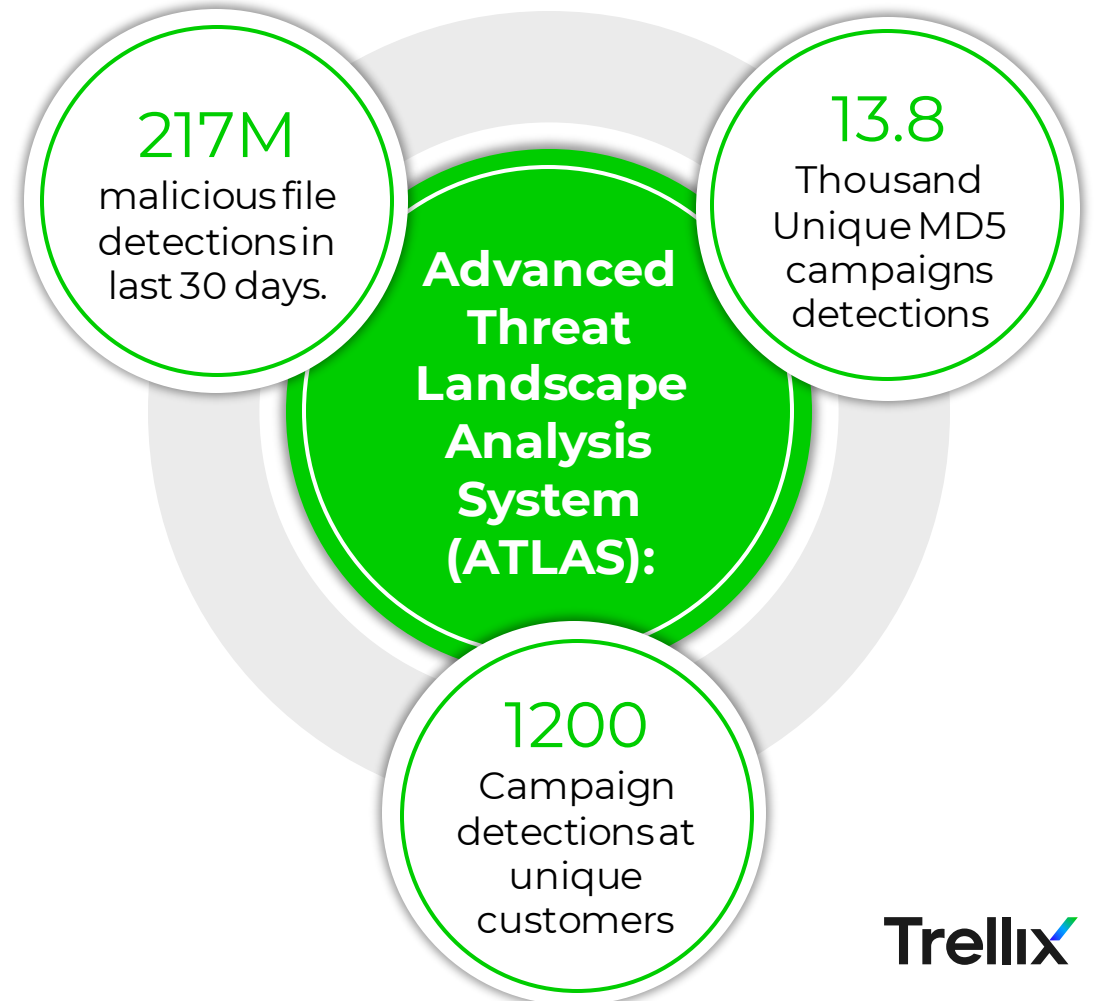
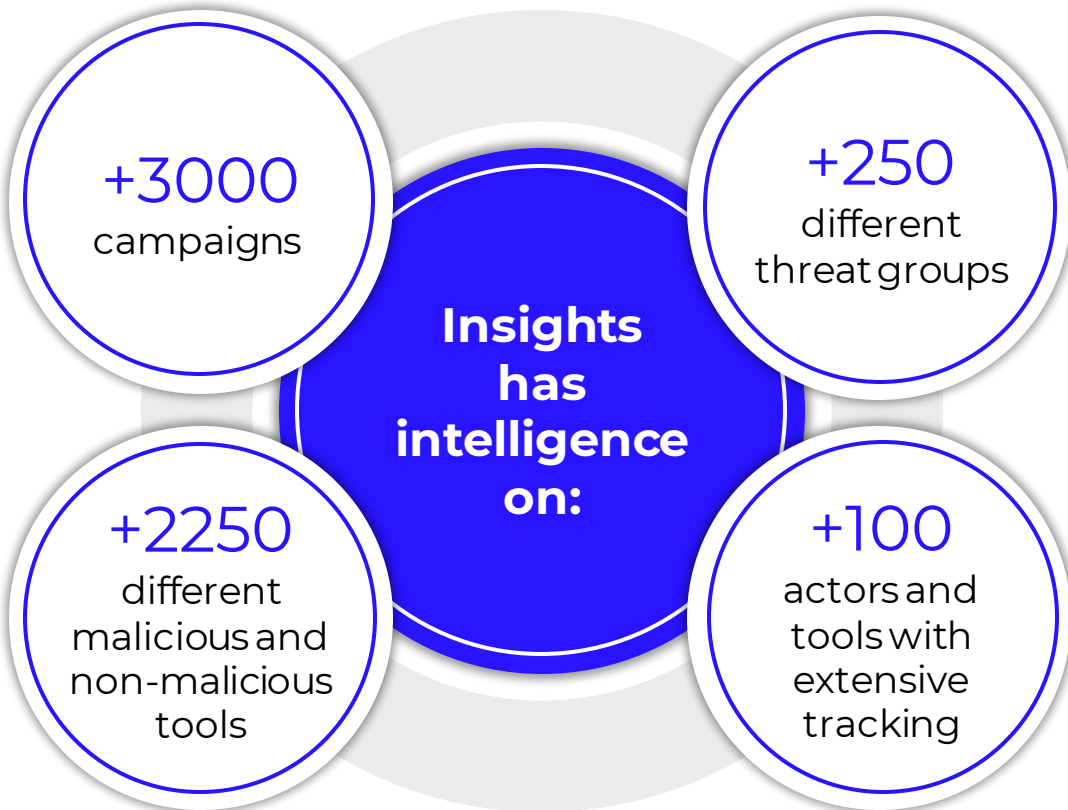


- Located in multiple time zones, 24/7 coverage
- Concentrated hubs in Europe and East Coast US
- Analysts remote and on-site with customers
- Native speakers in Russian, Chinese, Vietnamese, French, German, Spanish, Portuguese, Hebrew, Arabic and Dutch
- Skillset, from analyst to Vuln and Malware research
- Customers ranging from National CERTS, IC agencies, LE Agencies, Defense, and commercial orgs
- Top Publications
- Data-driven research from intel to products

+50
TI Analysts

+200
researchers

Data-Driven Threat Intelligence

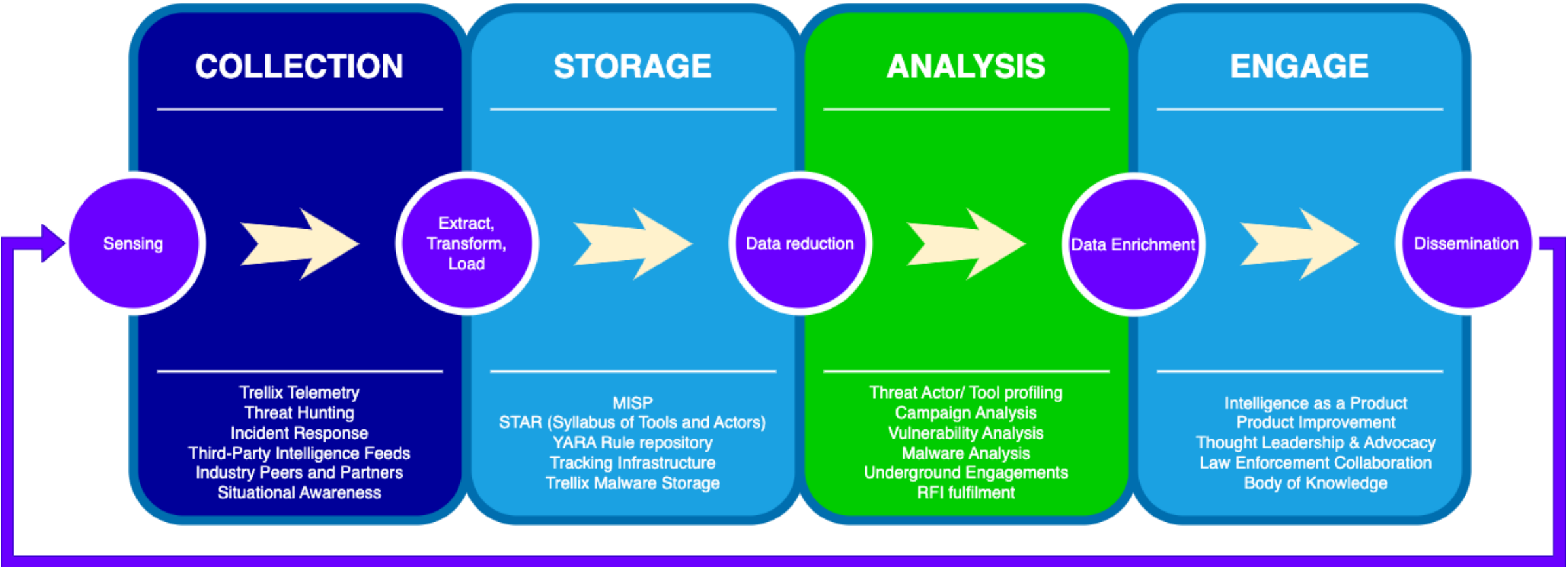




Defining Intelligence Requirements

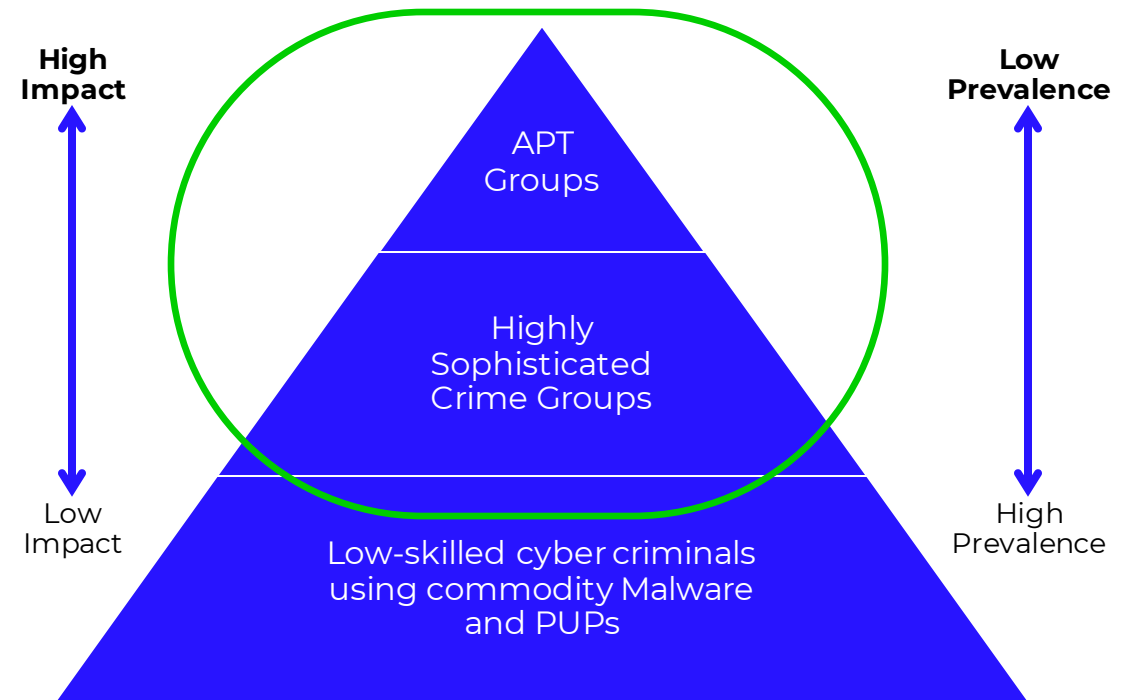
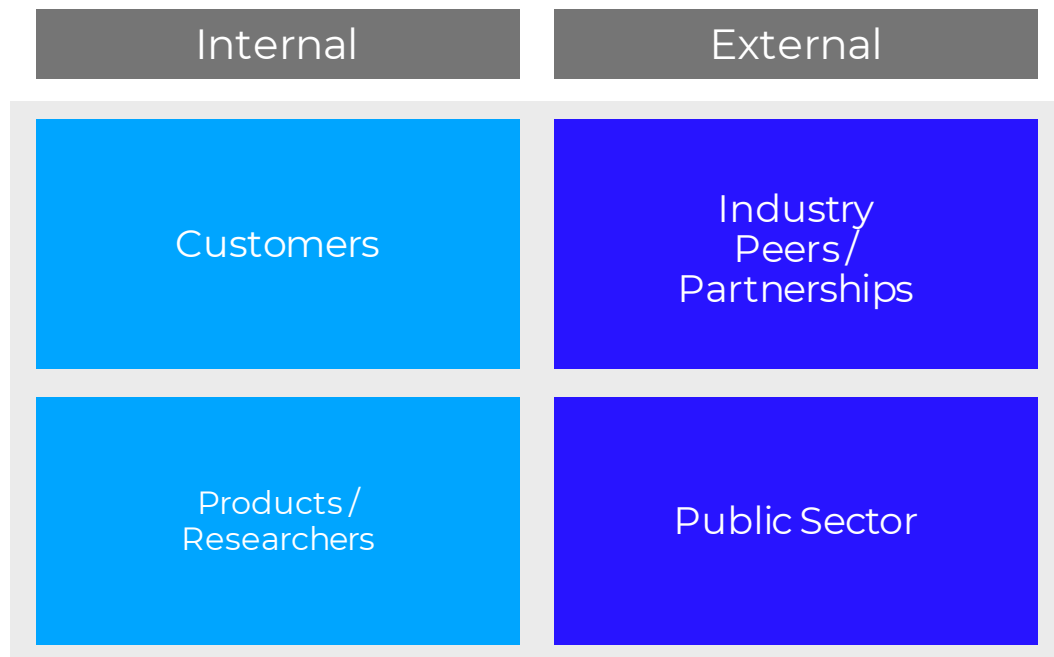
Trellix

Trellix Intelligence Framework from 30K feet



Threat Intelligence outputs and by-products can serve as input for the collection

Determining Customer Requirements



TIG Intelligence Cycle

RFI - INTaaS

INTaaS
Intelligence
Cycle

Planning & Direction

- Can the customer consume Intelligence?
- Identify cyberattack/threat and determine course of action and requirements to illuminate the adversary
- Contract finalization

Utilization

- Provides the end user the ability to generate courses of action: update/enhance security protocols; LE response
- Identify new requirements and reattack

Dissemination

- Private release only / NDA
- Report with TLP-Level

Production

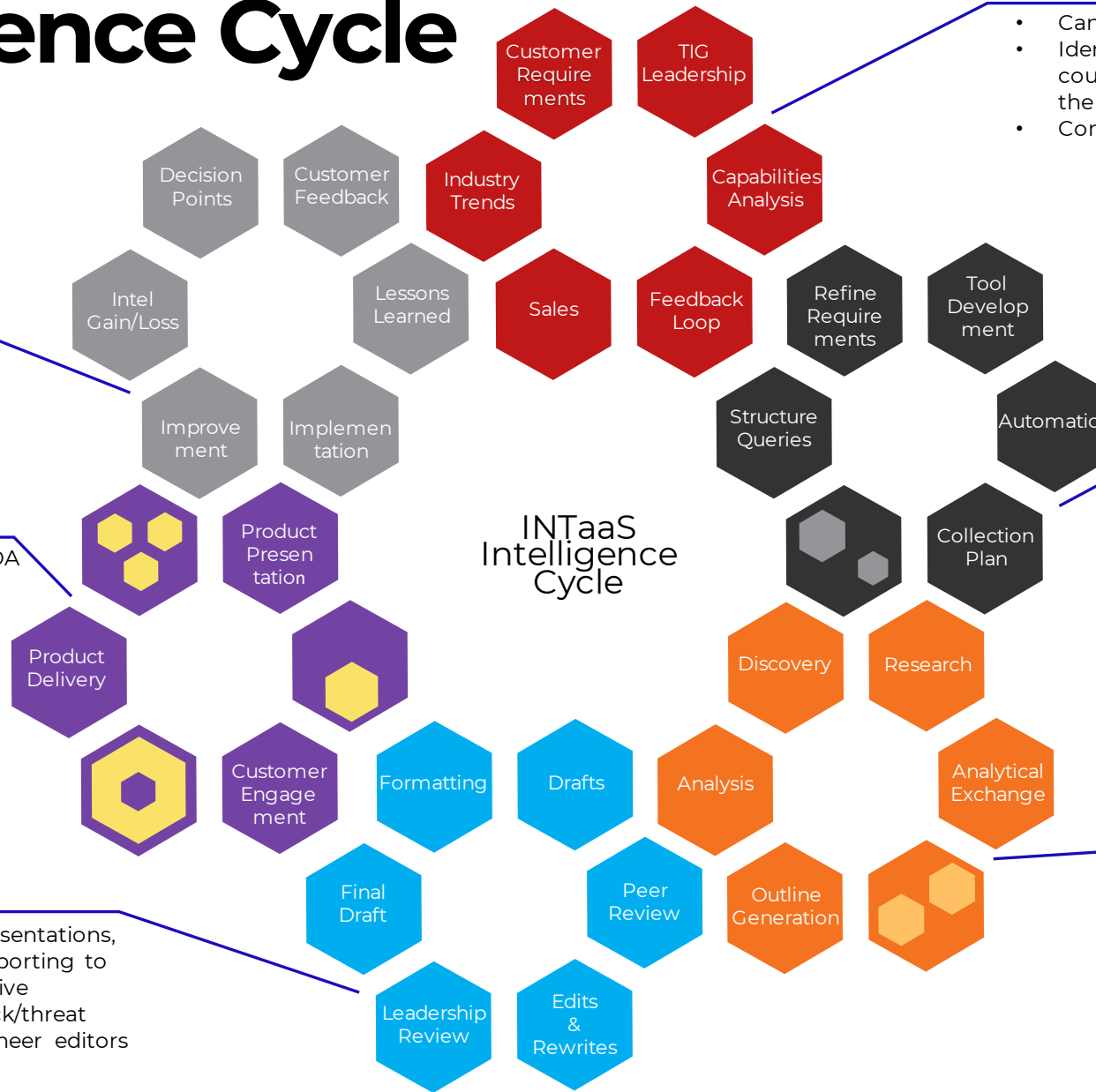
- Combine visual representations, data, and industry reporting to create a comprehensive response to the attack/threat
- PhD & Principal Engineer editors
- Written for Executive consumption

Collection

- Team build or leverage capabilities tailored to requirements
- Aggregate information from internal/external resources
- Team works to turn complex technical data into consumable information
- Constantly refining requirements and collection

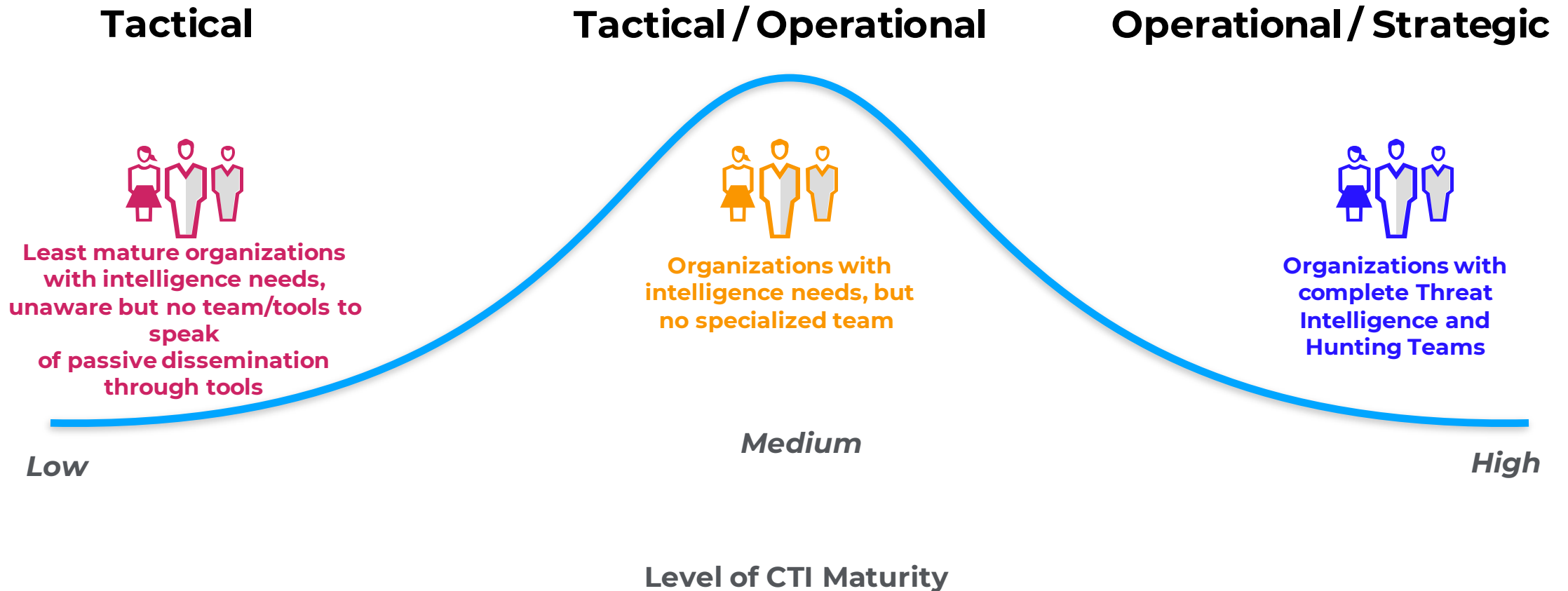
Processing & Exploitation

- Convert collected data into an understandable form: enriched, text-based data to a visual representation; attribution
- +35 years combined experienced in All-Source Analysis, Technical Analysis, Reverse Engineering, and Malware Analysis



Threat Intelligence Maturity

The demands differ from one organization to another

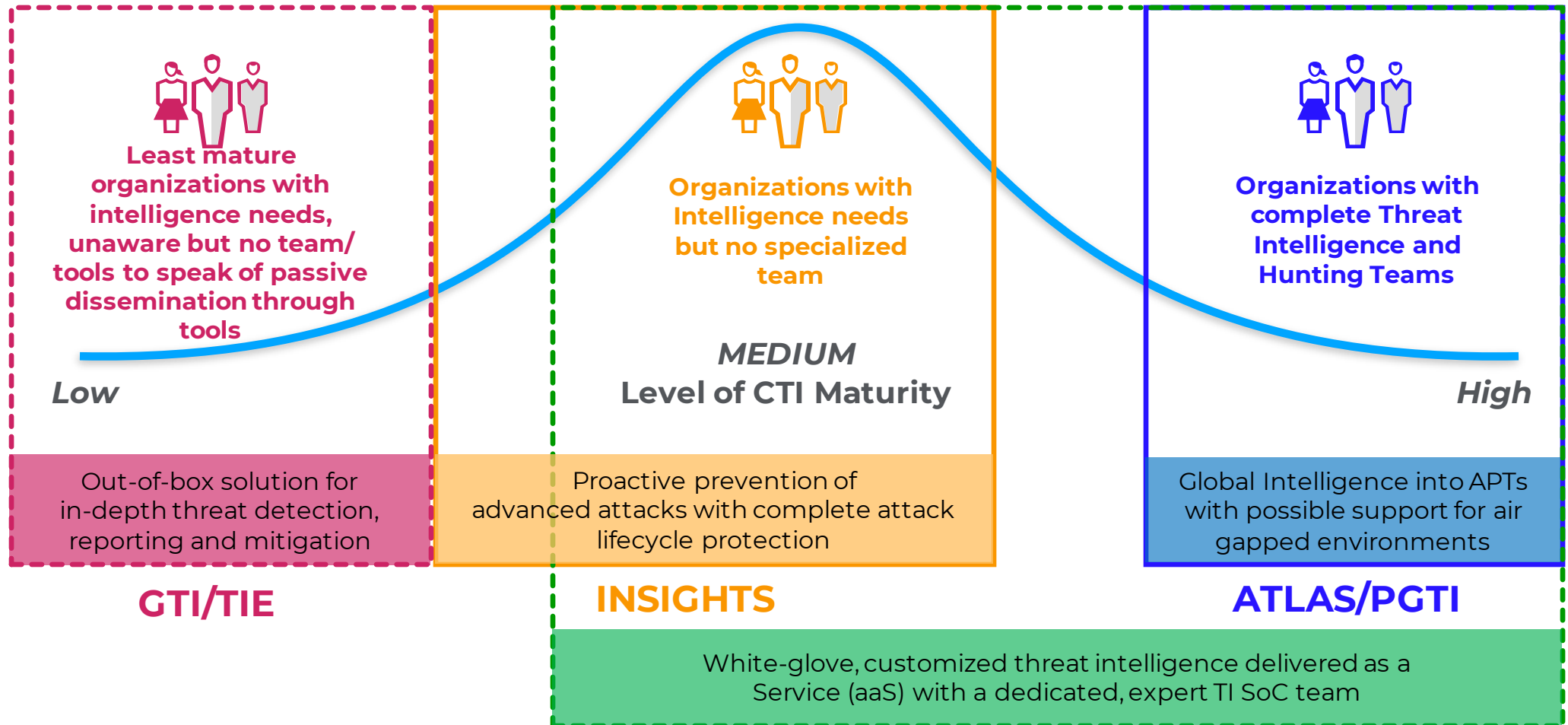


Customer-Centric Offerings to Meet Market Needs

Tactical

Tactical / Operational

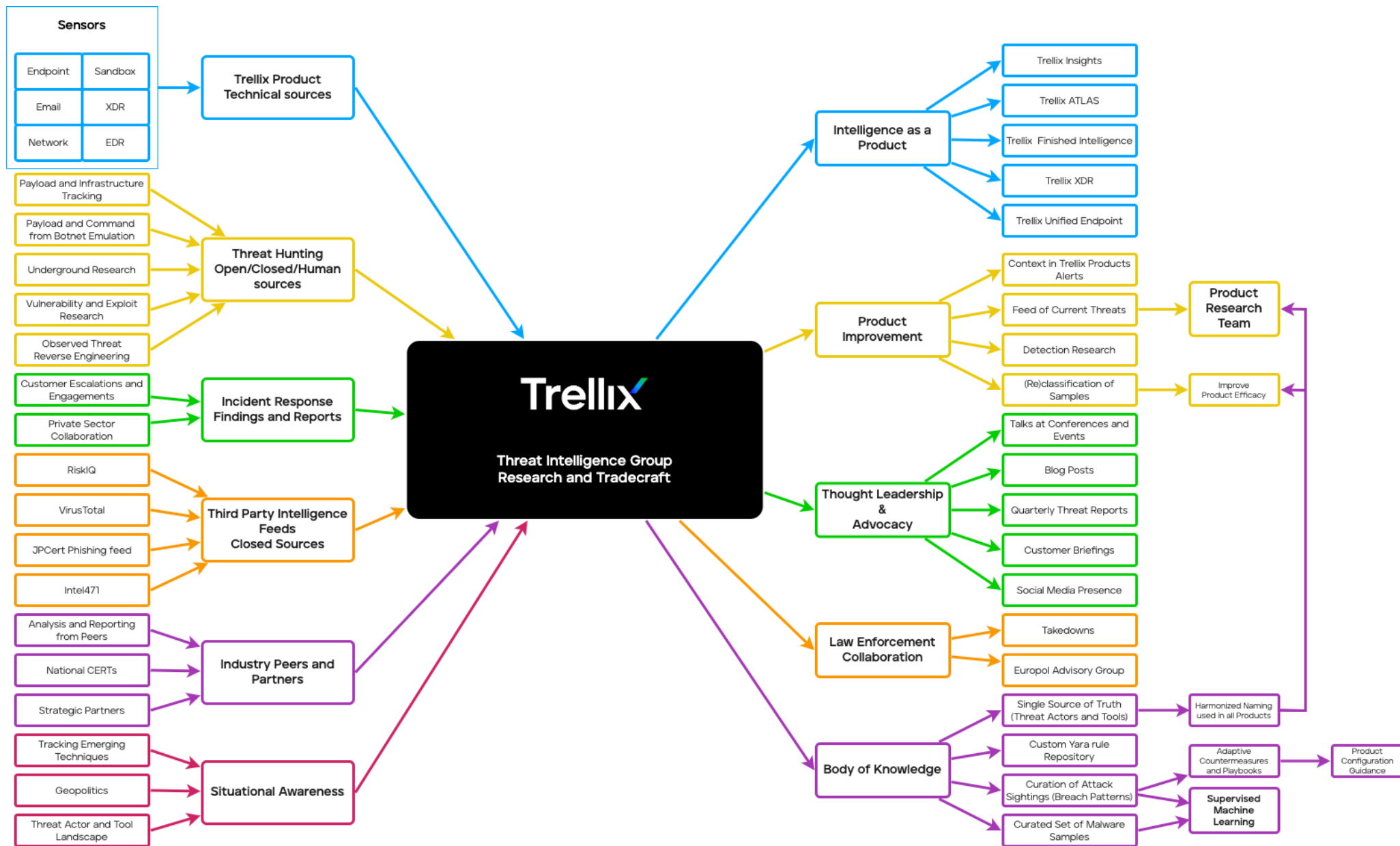
Operational / Strategic



INTaaS

Trellix

Collections and Deliverables overview



Frameworks supported

Internally:

- MITRE
- Diamond Model
- ACH (Analysis of Competing Hypotheses)
- CSAE

Externally:

- MITRE
- OODA loop (Countermeasures and playbooks)

The screenshot shows the Trellix ePO interface with the MITRE Explorer tool active. The main view displays a grid of MITRE techniques, categorized by phase. The selected technique is T1140, Defense Evasion: Deobfuscate/Decode Files or Information. The sidebar on the right provides details for this technique, including a description, tactical information, and associated campaigns.

MITRE Explorer

Technique : Deobfuscate/Decode Files or Information

Adversaries may use **Obfuscated Files or Information** to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

One such example is use of **certutil** to decode a remote access tool portable executable file that has been hidden inside a certificate file. (Citation: **Malwarebytes Targeted Attack against Saudi Arabia**) Another example is using the Windows **copy /b** command to reassemble binary fragments into a malicious payload. (Citation: **Carbon Black Obfuscation Sept 2016**)

Sometimes a user's action may be required to open it for deobfuscation or decryption part of the process. The user's action may be required to open it for deobfuscation or decryption part of the process. The user's action may be required to open it for deobfuscation or decryption part of the process.

Tactic Defense Evasion

Technique Id T1140

Associated Campaigns

- BItxor20 Backdoor Spreading Via...
- PcShare backdoor attacks
- Matanbuchus Loader Leads To C...

+ 1042 more

Vision

Current

- Meet customers where they are as the “go-to threat intelligence solutions”
- Sold as an individual solution or bundled with the Trellix portfolio
- Actionable and contextual write-ups for the CxO to analyst
- Accessible & transparent threat database
- Network effect on immediate detection

Future

- Create a microservice, composable solution
- Deployed within any console, either Trellix or external provider
- Apply AI to correlate “what we think it is on a probability %” vs “wait until the analyst is finished writing it up”
- Remediation steps that embeds Trellix solutions and SOAR Playbooks

Key Differentiators

- Sensor diversity with the largest footprint
- Composable application with on-demand Trellix deployments
- Bridging Threat Intelligence and Security Posture
- Threat Intelligence Group and Advanced Research Center

Partnerships and Relationships

Intelligence-sharing partnerships:

- MISP CIRCL
- JCDC CISA
- Mandiant (RPP)
- CyberVeilig Nederland
- Intel471
- JPCert
- AIS CISA (under development)

Public Sector relationships:

- Europol EC3 Advisory Group
- NSTAC
- JCDC
- NSA CCC
- FBI
- NCA
- NHTCU



Key Integrations SIA Partnerships

Existing TIP Integrations



Planned Integrations





Commercial Threat Intelligence Offerings

<https://www.trellix.com/en-us/platform/threat-intelligence.html>

Trellix

Trellix Threat Intelligence Portfolio

Build a Strong Defense with Global Intelligence and Local Visibility

- Mission-critical insights 24/7
- Millions of sensors distinctly across key vectors (endpoint, email, web, & network)
- One of the broadest and deepest intelligence offerings on the market
- Critical context to prioritize and drive better comprehensive protection

<https://www.trellix.com/en-us/platform/threat-intelligence.htm>

Global Threat Intelligence (GTI)

Private GTI

Trellix Intelligence Exchange (TIE)

Trellix Insights

Advanced Threat Landscape Analysis System (ATLAS)

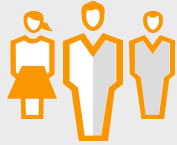
Intelligence as-a-Service (INTaaS)



Most Innovative -
Threat Intelligence

Trellix Insights

Real-time intelligence that identifies and prioritizes the threats most likely to target your organization



Customers with
intelligence needs but
no specialized team

MEDIUM

Level of CTI Maturity

CUSTOMER PROBLEMS:

1. The organization is under constant threat of advanced cyberattacks.
2. The team has the tools to mitigate most malicious threats but requires greater insight into the attack landscape to mitigate advanced, zero-day threats.
3. Broad best-of-breed security portfolio with disjointed analysis and reporting.

KEY BENEFITS:

- Proactively identifies and prioritizes threats most likely to hit your organization.
- Reduces mean time to detect and resolve from months to hours.
- Streamlines workflows with rich, actionable context and analysis.
- Intuitively guides security teams with various levels of experience to easily identify relevant threats.

Description

The Conti ransomware family was discovered using multiple techniques to find files to attack and how the encryption process is carried out. The malware uses multiple threads to encrypt files at a faster rate compared to other ransomware families and contains command-line options to scan for local files as well as remote files over SMB shares. Conti also uses the Windows Restart Manager to free up files that are open by various applications. The ransomware uses AES-256 encryption and requires the victim to email the threat actor for the decryption key. Variants of the malware post stolen data from entities who refuse to pay the ransom. Jabber IDs of the Threat-actors involved: it_work_support(@)xmpp.jp cicada3301(@)strong.pm

Trellix's Advanced Threat Research team will continue to monitor and update events related to the Conti ransomware family and disseminate information that is deemed appropriate regarding Conti and potential victims.

Severity

High

Knowledge Base

https://kc.mcafee.com/corporate/index?page=content&id=KB93317

Labels

- Internet of Things (IoT) Ransomware Russo-Ukrainian Crisis Vulnerability

Common Vulnerabilities and Exposures

- CVE-2021-1675 CVE-2021-34473 CVE-2021-34523 CVE-2018-13379

Threat Behavior

MITRE Techniques Observed (80)

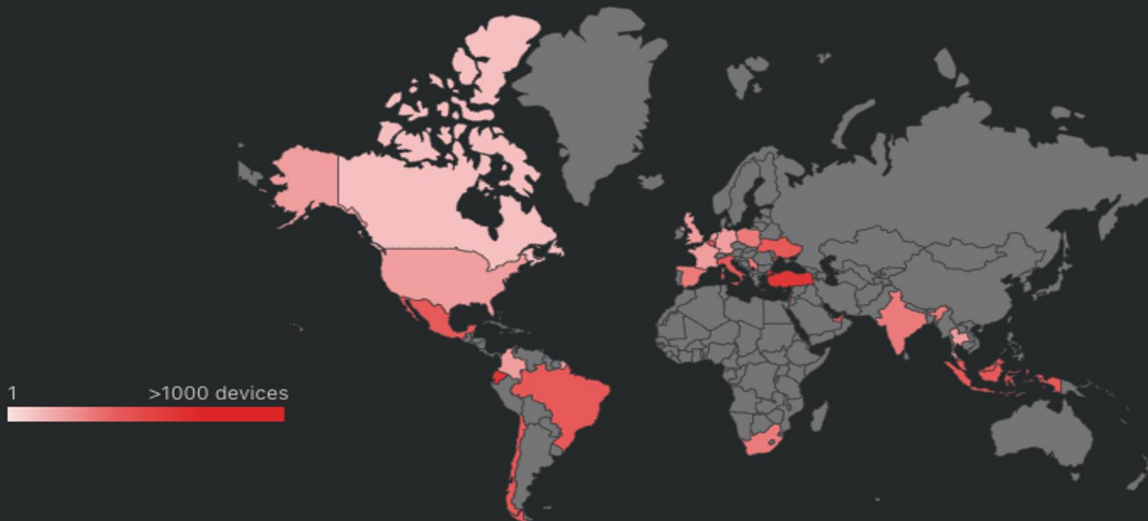
- Network Share Discovery - T1135 (Discovery)
Network Service Scanning - T1046
Dynamic-link Library Injection - T1055.001 (Privilege Escalation, ...)

Details

Observables

```
rclone.exe copy "\\<Server 3>\<Folder path>" remote:<victim name> -q --ignore-
%USERPROFILE%\ .config\rclone\rclone.conf
```

Global Prevalence



Observed Countries (27)

- Israel Turkey Ecuador Luxembourg Ukraine Mexico Italy United Arab Emirates Belgium Malaysia Indonesia Chile
Brazil Poland India Singapore Spain Serbia South Africa Colombia Netherlands United States United Kingdom

Other Information

Trellix Threat Actor

Conti Group

Trellix Tool

- IcedID PowerShell Invoke-SMBExec
Metasploit AdFind RCLONE



Selected Campaigns: Mallox Ransomware Increases Ac... | Sirattacker And ALC Ransomware... | CISA-FBI Joint Cybersecurity Adv... | More filters: 269

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Active Scanning T1595 (4)	Acquire Infrastructure T1583 (4)	Drive-by Compromise T1189 (2)	Command and Scripting Inte... T1059 (2)	Account Manipulation T1088 (6)	Abuse Elevation Control Mec... T1548 (3)	Abuse Elevation Control Mec... T1548 (3)	Credentials from Password S... T1555 (4)	Account Discovery T1087 (3)	Exploitation of Remote Servi... T1210 (3)	Archive Collected Data T1580 (2)
Gather Victim Network Infor... T1590 (3)	Compromise Accounts T1586 (1)	Exploit Public-Facing Appli... T1190 (2)	Exploitation for Client Execut... T1203 (5)	BITS Jobs T1197 (3)	Access Token Manipulation T1134 (1)	Access Token Manipulation T1134 (1)	Exploitation for Credential A... T1212 (1)	Application Window Discovery T1010 (3)	Internal Spearphishing T1534 (1)	Automated Collection T1119 (1)
	Develop Capabilities T1587 (3)	External Remote Services T1133 (2)	Native API T1108 (2)	Boot or Logon Autostart Exa... T1547 (3)	Boot or Logon Autostart Exa... T1547 (3)	BITS Jobs T1197 (3)	Input Capture T1058 (2)	Browser Bookmark Discovery T1217 (1)	Lateral Tool Transfer T1570 (2)	Browser Session Hijacking T1185 (1)
	Obtain Capabilities T1588 (3)	Phishing T1568 (2)	Scheduled Task/Job T1053 (2)	Browser Extensions T1176 (2)	Create or Modify System Pro... T1543 (2)	Debugger Evasion T1622 (2)	Multi-Factor Authentication ... T1621 (1)	Debugger Evasion T1622 (2)	Remote Services T1021 (1)	Clipboard Data T1115 (2)
	Stage Capabilities T1608	Replication Through Remova... T1091 (1)	Shared Modules T1129 (2)	Compromise Client Software... T1554 (1)	Domain Policy Modification T1484 (3)	Deobfuscate/Decode Files or ... T1480 (2)	Network Sniffing T1040 (3)	Domain Trust Discovery T1482 (2)	Replication Through Remova... T1091 (3)	Data Staged T1074 (2)
		Trusted Relationship T1199 (1)	Software Deployment Tools T1072 (4)	Create Account T1136 (3)	Exploitation for Privilege Esc... T1068 (2)	Domain Policy Modification T1484 (3)	OS Credential Dumping T1003 (2)	File and Directory Discovery T1083 (1)	Software Deployment Tools T1072 (4)	Data from Cloud Storage T1530 (2)
		Valid Accounts T1078 (2)	System Services T1569 (5)	Create or Modify System Pro... T1543 (2)	Hijack Execution Flow T1574 (1)	Execution Guardrails T1480 (2)	Steal Application Access Tok... T1528 (2)	Group Policy Discovery T1616 (2)	Taint Shared Content T1080 (1)	Data from Information Repos... T1213 (3)
			User Execution T1204 (2)	External Remote Services T1133 (2)	Process Injection T1055 (2)	Exploitation for Defense Eva... T1211 (4)	Steal or Forge Kerberos Tick... T1558 (3)	Network Service Discovery T1046 (2)		Data from Local System T1095 (2)
			Windows Management Instr... T1047 (4)	Hijack Execution Flow T1574 (1)	Scheduled Task/Job T1053 (2)	File and Directory Permissio... T1222 (3)	Unsecured Credentials T1552 (1)	Network Share Discovery T1135 (2)		Data from Network Shared D... T1039 (3)
				Scheduled Task/Job T1053 (2)	Valid Accounts T1078 (2)	Hide Artifacts T1564 (1)		Network Sniffing T1040 (3)		Data from Removable Media T1025 (1)
				Server Software Component T1505 (1)		Hijack Execution Flow T1574 (1)		Peripheral Device Discovery T1120 (1)		Email Collection T1114 (2)
				Traffic Signaling T1205 (1)		Impair Defenses T1562 (1)		Permission Groups Discovery T1069 (1)		Input Capture T1056 (2)
				Valid Accounts T1078 (2)		Indicator Removal T1070 (2)		Process Discovery T1057 (2)		Screen Capture T1113 (1)
						Indirect Command Execution T1202 (1)		Query Registry T1012 (1)		
						Masquerading T1036 (2)		Remote System Discovery T1018 (2)		
						Modify Registry T1112 (2)		Software Discovery T1518 (1)		
						Obfuscated Files or Informat... T1827 (2)		System Information Discovery T1082 (1)		
						Process Injection T1055 (2)		System Location Discovery T1614 (2)		
						Reflective Code Loading		System Network Configurati...		

Number of Match... ? ^

- >5
- 4
- 3
- 2
- 1

MITRE Explorer

Technique : Deobfuscate/Decode Information

Adversaries may use **Obfuscated Files or Information** as a technique to decode or deobfuscate the artifacts of an intrusion from analysis. They may use various mechanisms to decode or deobfuscate the artifacts, including built-in functionality of malware or binaries present on the system.

One such example is use of **certutil** to decode a portable executable file that has been encoded as a certificate file. (Citation: Malwarebytes Targeted Ransomware in Saudi Arabia) Another example is using the **Winternl** command to reassemble binary fragments in a ransomware payload. (Citation: Carbon Black Obfuscation Separates)

Sometimes a user's action may be required to complete the deobfuscation process of the file.

Tactic Defense Evasion

Technique Id T1140

Associated Campaigns

- B1txor20 Backdoor Spreading Via...
- PcShare backdoor attacks
- Matanbuchus Loader Leads To C...

+ 1042 more

Country - Ukraine x Country - Sweden x Country - Finland x More filters: 2

Search and add

Show only common campaigns across categories

Profiled (Actors / Tools) ^

Threat Actor

- APT19
- APT27
- APT27_Attack
- APT28

Tool

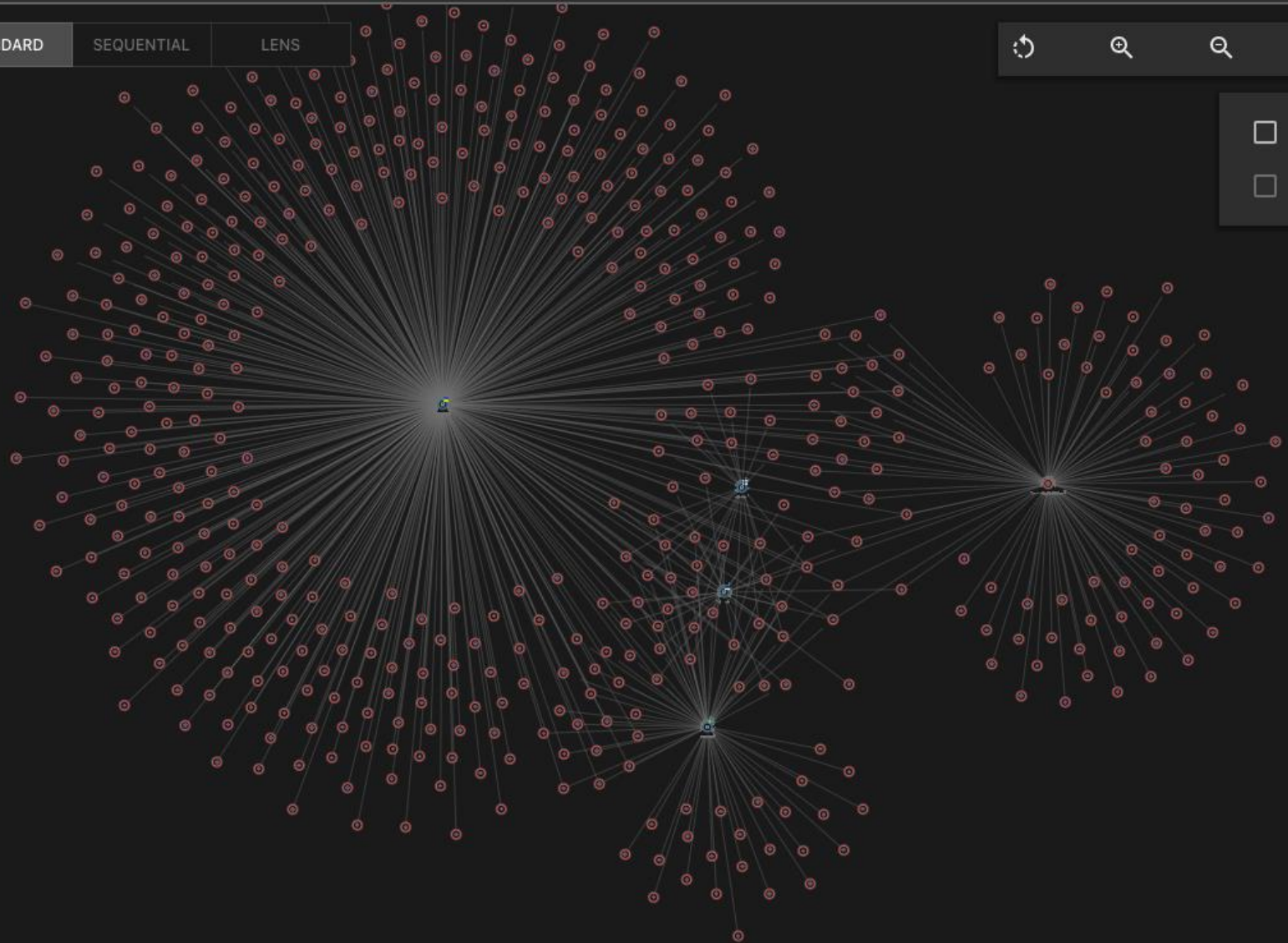
- 7Logger
- 7z SFX Constructor
- 7zr
- 8.t Dropper

Labels ^

- Russo-Ukrainian Crisis
- Scareware
- Spyware
- Supply chain attack
- Tool

STANDARD SEQUENTIAL LENS

Include Detections
 Include TTPs



Type	Countermeasure Outcome	Tools	Techniques	Enablers
✓	Maximum native logging for PowerShell Script Block execution.	PowerShell	T1059.001 - Powe...	Windows Active Directory GPO
🛡️	Prevention from Campaign GandCrab Ransomware Puts the Pinch on Victims	Not Available	Not Available	ENS
🛡️	Prevention from Campaign GandCrab Malspam	Not Available	Not Available	ENS
🛡️	Prevention from Campaign GandCrab 5.0.4	Not Available	Not Available	ENS
🛡️	Prevention from Campaign Lazarus Group Targets More Cryptocurrency Exchanges and FinTech Companies	Not Available	Not Available	ENS
🛡️	Prevention from Campaign GandCrab Ransomware Distributed by Exploit Kits, Appends GDCB Extension	Not Available	Not Available	ENS
🛡️	Prevention from Campaign Fallout Exploit Kit Used in Malvertising Campaign to Deliver GandCrab Ransomware	Not Available	Not Available	ENS
🛡️	Detect abuse of the Task Scheduler feature for persistence and execution	Schtasks.exe	T1053.005 - Sche...	Trellix Endpoint
🛡️	Prevention from Campaign GandCrab Run (2018-09-24) - "My letter just for you"	Not Available	Not Available	ENS
🛡️	Restrict execution of Msiexec.exe to privileged accounts or groups that need to use it to lessen the opportunities for malicious usage.	Not Available	T1218.007 - Msie...	Windows Active Directory GPO
🛡️	Detect information gathering about OU and domain trusts using ADFind	AdFind	T1482 - Domain T...	Trellix Endpoint
🛡️	Detect computer information query using ADFind	AdFind	T1018 - Remote S...	Trellix Endpoint
🛡️	Prevention from Campaign Operation Bad Tidings	Not Available	Not Available	ENS
🛡️	Prevention from Campaign Operation Frankenstein	Not Available	Not Available	ENS

Countermeasures (Revision 1)

Outcome : Maximum native logging for PowerShell Script Block execution.

Stage : Before

Type : Preparation

Capabilities : Windows Active Directory GPO

Applicability : User Device

Operator : Windows SysAdmin

Frequency : Once

Component : Processes

Category : Process Created

Goal : Visibility

Platform : Windows

Tactics : Execution

Techniques : PowerShell - T1059.001

Tools : PowerShell

View Actions 0 / 4

Not Started

Notes 4 Add notes

- Jul 11, 2022 10:45 AM +02:00

Revision 1 : 0

✓

CONFIGURE insightsepo admin

Test
- Jul 11, 2022 10:45 AM +02:00

Revision 1 : 0

✓

MONITOR insightsepo admin

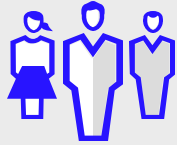
Test
- Jul 11, 2022 10:45 AM +02:00

✓

VALIDATE insightsepo admin

Advanced Threat Landscape Analysis System (ATLAS)

Aggregates data from rich data sources to provide the latest visibility into global emerging threats, including campaign-specific data such as industry sector and geolocation.



Customers with complete
Threat Intelligence and
Hunting teams

High

Level of CTI Maturity

CUSTOMER PROBLEMS:

1. Top-priority, highly sensitive data under constant targeting from evolving global cyberthreats
2. Needs-based situational awareness based on the types of threats targeting the organization
3. Requires internal analysis only for targeted attacks

KEY BENEFITS:

- Unique global insights power tailor-made threat mitigation
- Identifies both current and future/emerging threats, keeping you ahead of latest threats
- Experienced research teams deliver tailor-made threat reporting for attacks targeting your specific organization

ATLAS Overview

Main dashboard showing Global File, URL, IP Prevalence up to 1 year back

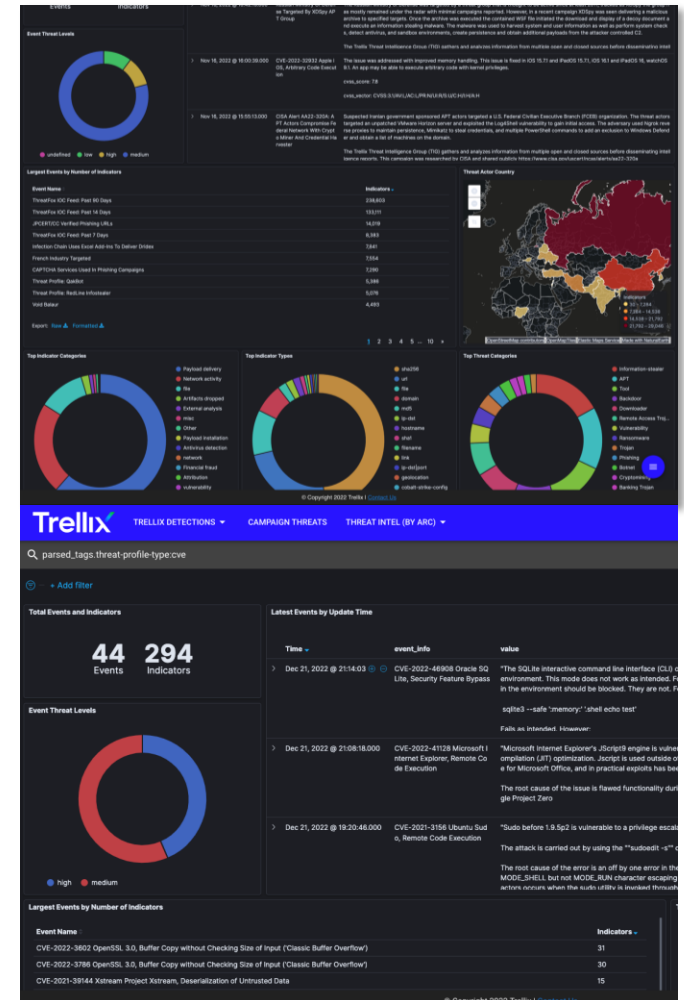
Detections, divided per GEO Sector, Products, etc.

- Which attacks are most relevant to your organization.
- When and where they are occurring.
- What industry sectors are affected.
- Whether they belong to any organized campaigns.



Campaign dashboard data is imported from Trellix's backend intelligence platform, MISP. As part of this process, ATLAS automatically enriches our prevalence data with campaign IOCs.

The vulnerability dashboard collates the analysis of the latest high-impact vulnerabilities. The analysis and triage are performed by the Advanced Research Center's industry experts on vulnerabilities.



Search... (e.g. client_country:US AND _exists_:event_id)

2023-09-15 to 2023-10-14

APPLY



Malicious File Detection Counts

665,098
Total - Detections

1,399
Campaign - Detections

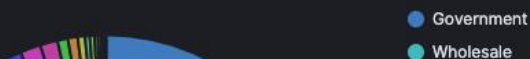
22,843
Total - Unique MD5s

62
Campaign - Unique MD5s

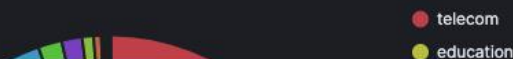
95
Total - Unique Customers

10
Campaign - Unique Customers

Top Customer Sectors

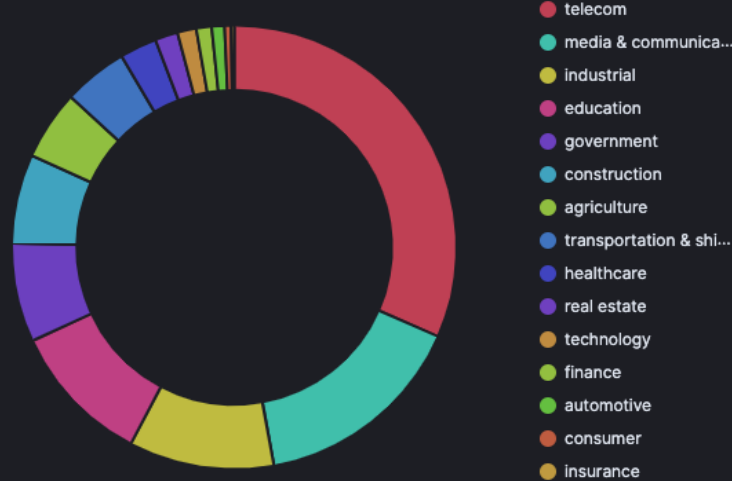
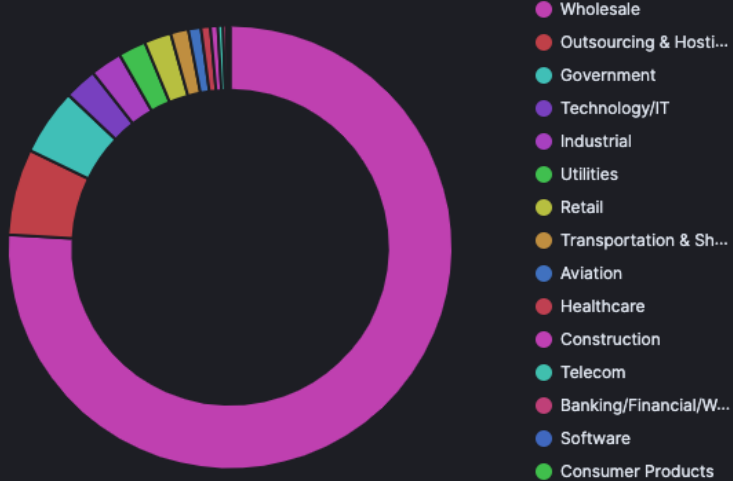


Top Whois Sectors

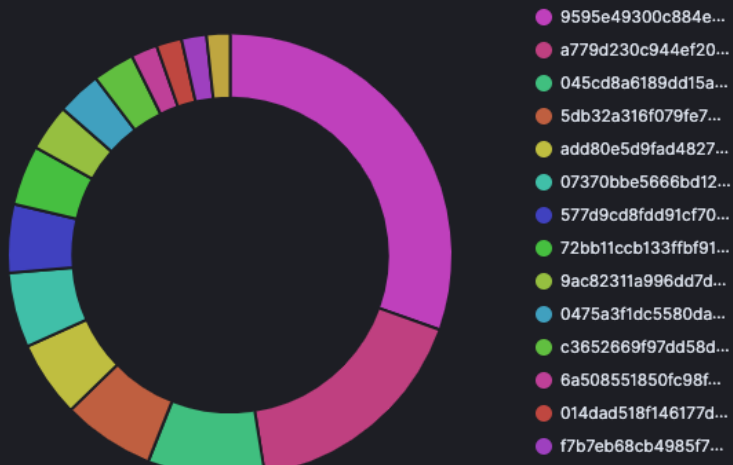


Top Country Codes

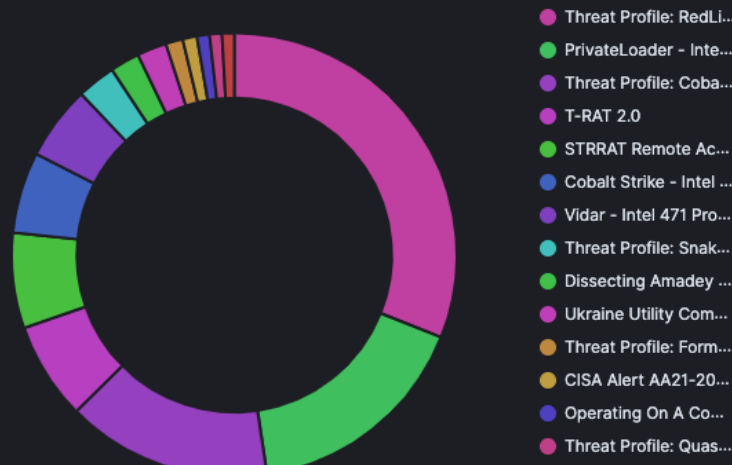




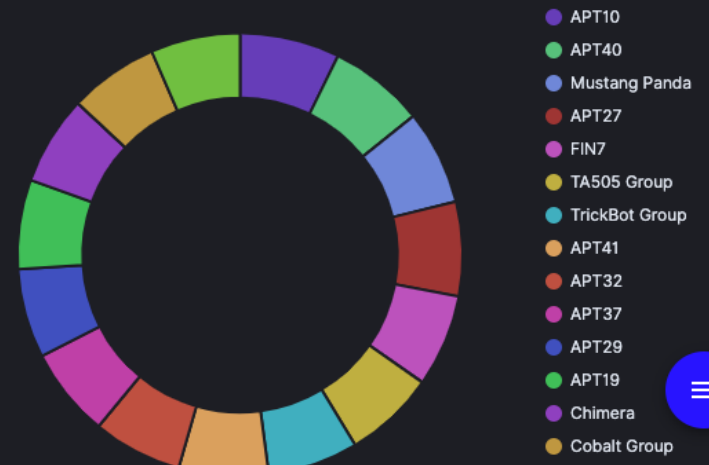
Top MD5s

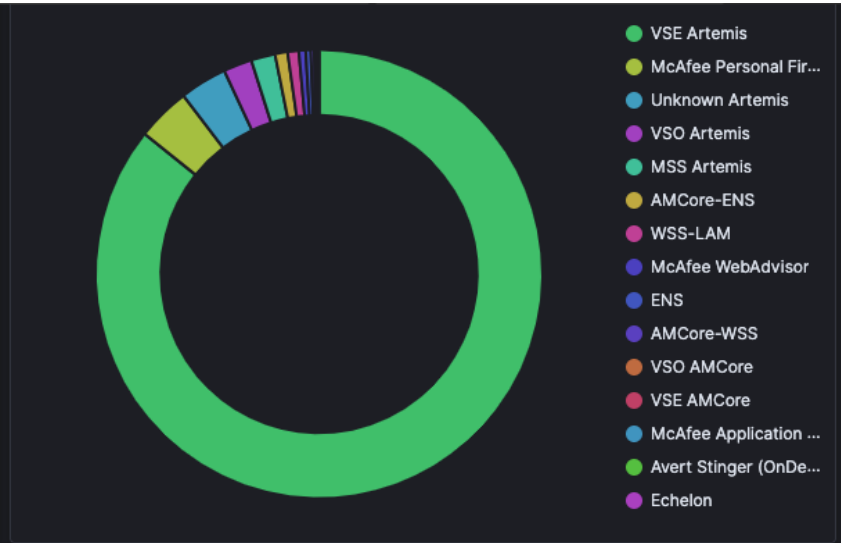
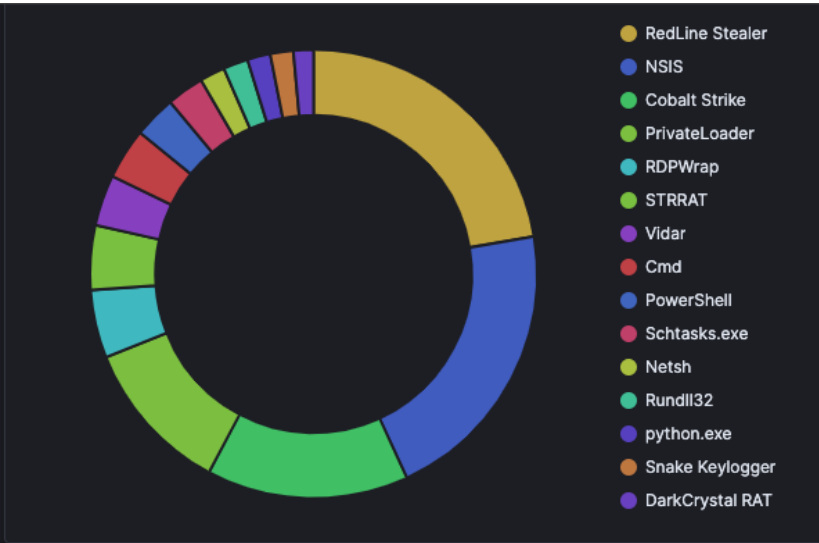
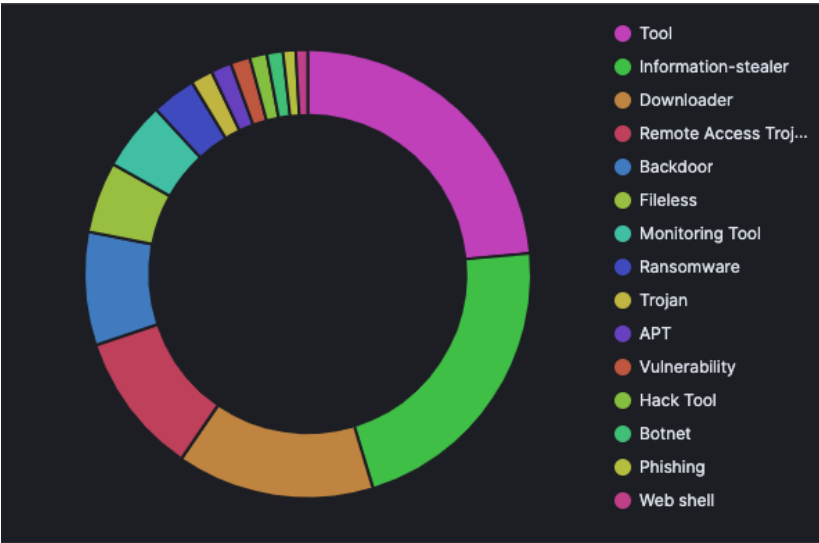


Top Event Names



Top Threat Actors





Search... (e.g. client_country:US AND _exists_:event_id)

2019-01-01 to 2023-07-14

APPLY

2,932 Events 503,390 Indicators

Event Threat Levels



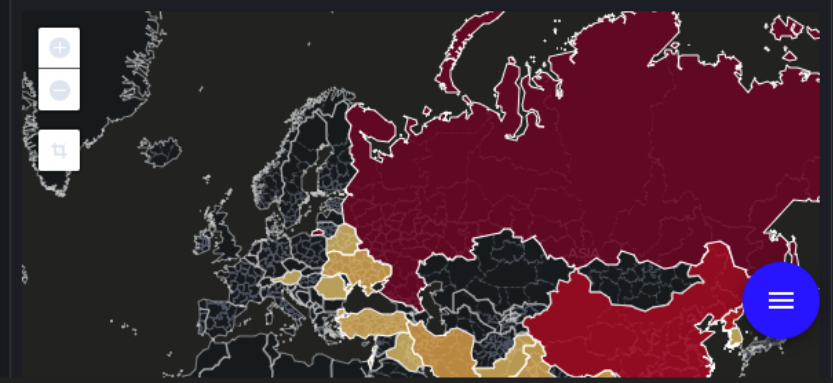
● undefined ● high ● low ● medium

Time ▾	event_info	value
> Jul 13, 2023 @ 22:44:53.000	Cobalt Strike - Intel 471 Provided Feed	<p>Cobalt Strike is a suite of tools used by red teams in penetration testing engagements. The entire suite can be purchased and used as a malware tool set. The main component infecting the system is Beacon. Users of Cobalt Strike can also generate a loader component that injects Beacon into memory, this is also called a stager. The Cobalt Strike toolkit is very popular among targeted ransomware actors and espionage groups.</p> <p>This Insights Entry for Cobalt Strike is part of Intel 471's *Malware Freemium* which offers near real-time technical intelligence on 3 malware families as a free taster of our full Malware Intelligence offering.</p>
> Jul 13, 2023 @ 22:43:20.000	CVE-2023-33157 Microsoft Sharepoint, Remote Code Execution	<p>Sharepoint is vulnerable to a deserialization attack. Software reverse engineering has detected an update to the Microsoft.BusinessData assembly (Microsoft.BusinessData.dll) which is used by sharepoint to deserialize XML files. In particular the method IsAllowedForDeserializationTypeString has been significantly altered with the old version being:</p> <pre>public static bool IsAllowedForDeserializationTypeString(string s) { if (string.IsNullOrEmpty(s)) {</pre>
> Jul 13, 2023 @ 22:34:34.000	CVE-2023-32046 Microsoft Internet Explorer/MSHTML, Remote Code Execution	<p>MSHTML, and other applications that use this library (Internet Explorer, File Explorer for instance) are vulnerable to an attack allowing malicious users to leak NTLM hashes. In this case the vector is a internet shortcut (.lnk) file. Attackers encode a UNC path for the shortcut image into the lnk file, enticing the system to reach out to a malicious server when the file is viewed. Users must view a folder or webshare where the file is hosted but do not need to click the file or otherwise interact with it. Leaking hashes in this way is used by attackers to gain remote code execution either through pass the hash attacks on the local network or via password cracking and subsequent logics on the internet.</p> <p>This attack has been detected in use in the wild. It is a variation on several previously known attacks such as CVE-2023-23397.</p>

Largest Events by Number of Indicators

Event Name ▾	Indicators ▾
PrivateLoader - Intel 471 Provided Feed	63,243
JPCERT/CC Verified Phishing URLs	50,599
Cobalt Strike - Intel 471 Provided Feed	30,742
Threat Profile: Cobalt Strike	28,221
ThreatFox IOC Feed: Past 14 Days	23,928
Threat Profile: RedLine Infostealer	11,134
Infection Chain Uses Excel Add-Ins To Deliver Dridex	7,841
French Industry Targeted	7,554

Threat Actor Country



Q parsed_tags.threat-profile-type:cve



📅 2019-01-01 to 2023-07-14

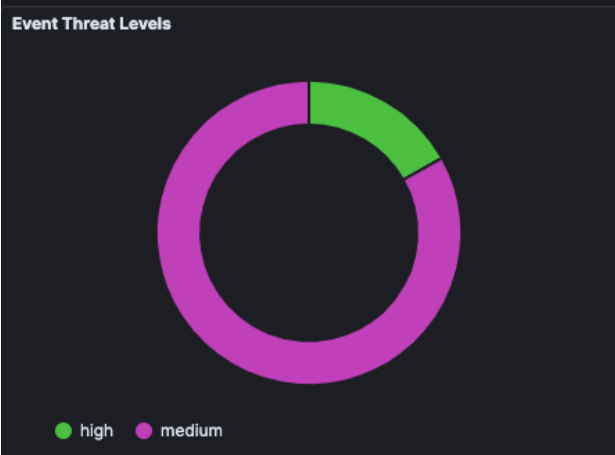
APPLY

+ Add filter

Total Events and Indicators

148 Events

695 Indicators



Latest Events by Update Time

1-50 of 148

Time ▾	event_info	value
> Jul 13, 2023 @ 22:43:20.000	CVE-2023-33157 Microsoft Sharepoint, Remote Code Execution	Sharepoint is vulnerable to a deserialization attack. Software reverse engineering has detected an update to the Microsoft.BusinessData assembly (Microsoft.BusinessData.dll) which is used by sharepoint to deserialize XML files. In particular the method IsAllowedForDeserializationTypeString has been significantly altered with the old version being: <pre>public static bool IsAllowedForDeserializationTypeString(string s) { if (string.IsNullOrEmpty(s)) {</pre>
> Jul 13, 2023 @ 22:34:34.000	CVE-2023-32046 Microsoft Internet Explorer/MSHTML, Remote Code Execution	MSHTML, and other applications that use this library (Internet Explorer, File Explorer for instance) are vulnerable to an attack allowing malicious users to leak NTLM hashes. In this case the vector is a internet shortcut (.lnk) file. Attackers encode a UNC path for the shortcut image into the lnk file, enticing the system to reach out to a malicious server when the file is viewed. Users must view a folder or webshare where the file is hosted but do not need to click the file or otherwise interact with it. Leaking hashes in this way is used by attackers to gain remote code execution either through password cracking and subsequent logics on the internet. This attack has been detected in use in the wild. It is a variation on several previously known attacks such as CVE-2023-23397.
> Jul 13, 2023 @ 22:29:42.000	CVE-2023-36874 Microsoft Windows (Error Reporting Service), Elevation of Privilege	The Windows Error Reporting Service (WER) is vulnerable to an elevation of privilege. This attack is made locally by low privileged users. This attack requires users to make folders and be able to create performance traces. Software reverse engineering detected that the patch fixing this vulnerability was in the linked library wercplsupport.dll. This library is used for interoperation of WER and the control panel UI element. In particular the WerComReport::SubmitReport function was amended. This function is used for submitting error reports. This suggests that the exploit is triggered by manual submission of a .wer report.

Largest Events by Number of Indicators

Event Name	Indicators ▾
CVE-2016-6415 Cisco IOS, Information Disclosure	9
CVE-2021-35587 Oracle Access Manager, Remote Code Execution	8
CVE-2023-3460 Ultimate Members Plugin, Elevation Of Privilege	7
CVE-2023-34362 In Progress MOVEit Transfer, Remote Code Execution	7

Threat Actor Country

Country	Count
USA	1
UK	1
FR	1
RU	1
CA	1
DE	1
IT	1
JP	1
IN	1
BR	1
AR	1
MX	1
ES	1
PT	1
GR	1
TR	1
PL	1
CZ	1
SK	1
SE	1
NO	1
DK	1
FI	1
EE	1
LV	1
LT	1
SI	1
HR	1
CY	1
IS	1
LU	1
BE	1
NL	1
CH	1
AT	1
AU	1
NZ	1
SG	1
HK	1
MO	1
MY	1
TH	1
VN	1
PH	1
ID	1
IN	1
BD	1
PK	1
AF	1
IR	1
IL	1
EG	1
SA	1
AE	1
QA	1
OM	1
YE	1
SD	1
SO	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1
NE	1
TD	1
CG	1
GA	1
NG	1
GH	1
KE	1
UG	1
RW	1
ET	1
SS	1
SD	1
LR	1
SI	1
SL	1
GN	1
CI	1
BE	1
ML	1
BF	1

Trellix Threat INTaaS Packaging

	Basic	Advanced	Advanced Plus
Trellix Threat and Efficacy Reporting	2x Year	Quarterly	Monthly
Health Watch/ Hunting	Yearly	Yearly	2x Year
Tailored Request for Information	4 Small annually	1 Major / 7 Small annually	2 Major / 14 Small annually
Executive Briefing		Quarterly	Monthly
Security Assessment			Yearly
Services Credits		40 hours	80 hours

Offering at a Glance

Trellix Threat and Efficacy Reporting

- Automated collection and reporting of the efficacy of the Trellix solutions in the environment
- Correlated detection events with threat campaigns and actors
- Briefing with management team on the findings and recommendations to improve efficacy

Tailored Request for Information

- Detailed research of submitted information
- Tailored report readout on the RFI submission
- Provide additional IOC, YARA, SNORT, Expert Rules to detect/prevent the RFI

Executive Briefing

- Tailored presentation of RFI findings and efficacy reporting to the executive management team

Security Assessment

One of the following assessments may be utilized during the subscription

- XDR Strategy and Maturity
- SOC Maturity
- IR Readiness
- Purple Team Exercise

Example RFI

Small Request (2-3 business days)

Requests require about 2 to 3 days to compile and enrich data through various sources.

- First-level enriched data
- Telemetry detections
- Yara rules
- IoCs
- Automated data enrichment
- Hash connections (MD5, SHA1 & SHA256)
- DNS/passive DNS
- Domain connections
- Subdomain connections
- Host connections
- File connections
- URL connections
- Digital certificates associations
- Email addresses
- IP connections
- Initial malware analysis report

Examples

Drive-by exploitation capture/analysis

"We have a user who accidentally clicked on this URL. I would like to request an analysis and better understand the nature of this link, if malware was installed, etc."

Interpretation of media events/reporting

"The attached article mentions the use of specific malware. Does Trellix have detection data on this malware? If so, could we receive any historical information, details on geographies, and sectors targeted by this malware."

Major Request (5+ business days)

Requests require infrastructure mapping, campaign-specific connection analysis, trending analysis and more deep-dive

- Threat actor profile
- Attributions
- Vender/ App / Device Risk Profile
- Comprehensive malware analysis report

Examples

Geography-based threat actor research

"We have offices located in various countries within Europe and the Middle East. Can you identify the top threat actors in each region that target our sector and provide known TTPs and historical events? Is our company at risk from these threat actors?"

Malware analysis (Static, behavioral, and/or reverse engineering)

"We have discovered two samples that seem to have been silently infected our systems since 2020. We suspect they are Qakbot variants, although their capabilities, attribution, and initial threat vector remain unknown. We have attached the files and need a comprehensive inspection, including IoCs, unpacked payload, evasion and de-obfuscation techniques, if any exist."

Example Reports



TLP: GREEN

We bring security to life.

Table of Contents

Table of Contents.....	1
General Overview.....	2
Data acquisitions and unpacking techniques	3
Icedid malware.....	5
Javascript (Stage 2).....	5
Powershell script (Stage 3).....	5
.NET DLL analysis (Stage 4).....	6
Icedid malware (Stage 5) configuration	7
Features.....	11
Cobalt Strike beacon.....	13
Payload execution.....	13
Javascript (Stage 2).....	13
Powershell script (Stage 3).....	13
.NET DLL analysis (Stage 4).....	14
Cobalt Strike beacon (Stage 5) configuration.....	15
Features.....	18
Conclusion.....	19
IoCs.....	20
Icedid.....	20
Hashes.....	20
C2 IP.....	20
Registry key.....	20
Cobalt Strike.....	21
Hashes.....	21
C2 IP.....	21
Persistence.....	21
Registry key.....	21
Appendix.....	23
Bibliography	23



We bring security to life.

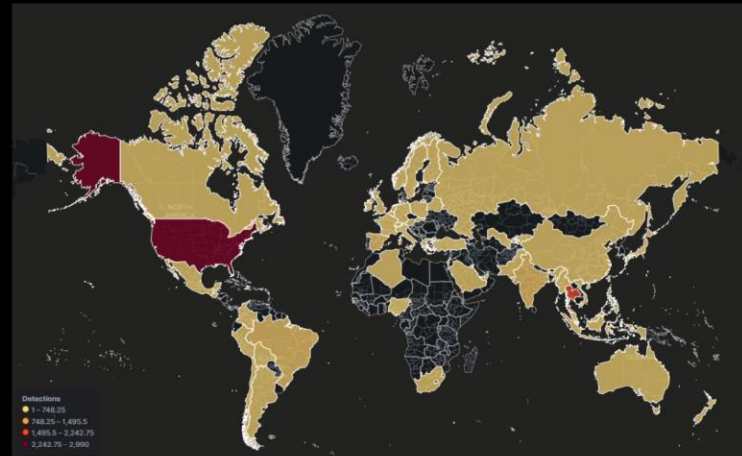


Figure 1. Global detections for 173.231.184.124

2) 20.103.253.93

This is the second month in a row that the IP address appeared with the second most counts. The IP was still not detected by any vendors as malicious.^{vi} Similar to the previous IP address, this IP had many malicious files communicating to it.^{vii}

Trellix Detections

Trellix does not have malicious detection data for this IP.

3) 137.252.250.181

Second month in a row for this IP as well. The IP address was not detected by any vendors as malicious.^{viii} Little information was identified for this IP address.

Trellix Detections

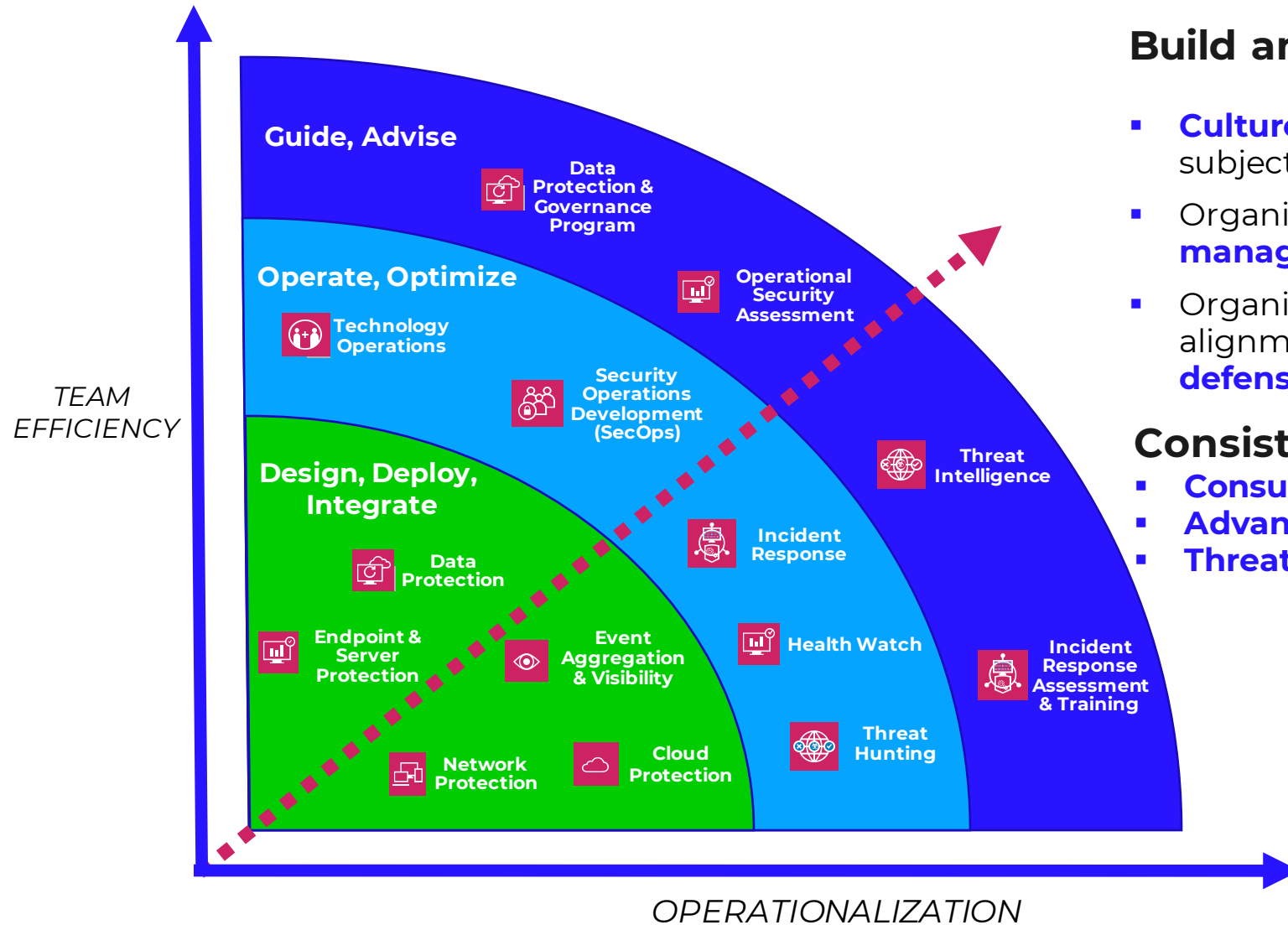
Trellix does not have malicious detection data for this IP.



Trellix Services Roadmap

Build a more productive team through investment in systems and processes

A global organization delivering over 620,000+ hours each year helping customers protect their environments from threats



Build an organization characterized by:

- **Culture of “Threat Protection”** versus single technology subject matter expertise
- Organization that thinks like **engineers and risk managers**
- Organization that continues to learn and evolve in alignment with a well understood **“big picture” of cyber defense**

Consist of:

- **Consulting Services**
- **Advanced Cyber Threat Services (ACTS)**
- **Threat Intelligence Group (TIG)**

Trellix

Thank You!

