Datasheet

Trend Vision One™ - Threat Insights

See threats coming from miles away. Powered by Trend™ Research and global threat intelligence.

Another emerging threat is making the news, and you're scrambling to determine whether you're vulnerable. Don't wait to find out if you're next. Do you know who is targeting you? What vulnerabilities they are exploiting? How can you best protect your assets from specific threats? How can you defend your organization before the attackers even hit send on their phishing email?

Take back control of your environment with Trend Vision One - Threat Insights. Get the tools and confidence to hunt down threats and preempt alerts. Be better prepared for advanced, emerging threats that may be coming your way.

Empowering security operations

Threat intelligence curated by Trend Micro experts. As part of our Trend Vision One™ platform, Threat Insights provides you with rich context on latest vulnerabilities and IoCs, including emerging threats and threat actors that are already in or targeting your environment. This allows your SOC teams to elevate XDR alert investigations and ASRM vulnerability management.

Threat intelligence is woven into our DNA. With over 35 years of dedicated threat research, a global network of researchers and sensors, and the industry-leading Trend Micro™ Zero Day Initiative™—the number one bug bounty program—we offer unparalleled insight into emerging threats. Trusted by law enforcement, our unique perspective on cybersecurity threats remains unmatched.

Key capabilities

Customers like you utilizing XDR for endpoint, email, network, or cloud can enjoy these features without extra charge:

- **Endpoint, email, network, and cloud integration.** Threat intelligence sources allow you to expand beyond endpoints, across layers such as server, email, cloud, and network, providing you with a comprehensive and diverse depth of threat insights. Trend Vision One allows you to protect against alerts and threats derived from all security layers
- **Automated investigations.** Streamline threat identification and investigation by combining malware analysis, malware search, and threat insights. This integration enables you to reduce the time and skills required for manual incident investigations, allowing for quicker and more efficient threat response
- **Custom intelligence sweeping.** Automate the detection of threats within your environment by integrating custom, third-party intelligence feeds into your Trend Vision One platform. Receive tailored threat investigations to quickly identify and mitigate potential security risks
- **Open-source intelligence (OSINT) feeds.** Access collections of data gathered from publicly available sources to identify potential cybersecurity threats. These feeds enhance Trend Research, providing you with additional context and insights for improved threat detection and response

Key benefits:

- Stay ahead of latest threats
- Access in-depth indicators of compromise (IoCs) and vulnerability intelligence
- Streamline threat hunting
- Enrich XDR alert investigations
- Elevate attack surface risk management (ASRM) vulnerability management

> The idea that I can bring IoCs very quickly and search across my organization is a game changer. I used to spend up to a week just to answer the question of "are we affected by this?"

Executive Director
Large University in USA

Key features

- **Emerging threats and threat actors.** Leverage proactive identification and analysis of new cyber threats and the entities behind them. This includes tracking and reporting on the latest cyber campaigns, converting findings into actionable intelligence, and monitoring command-and-control (C&C) servers to prevent ongoing breaches
  - Drill down to emerging threats and adversaries directly impacting your organization's industry and region
  - Discover who is exploiting vulnerabilities, their typical methods, their targets, and the most effective defense strategies against them
  - Understand the infection chain and map adversary tactics, techniques, and procedures to the MITRE ATT&CK Framework
  - Stay ahead of potential security risks and ensure timely response to evolving cyber threats
- **Vulnerability intelligence.** Gain a detailed analysis of known vulnerabilities, their exploitation, impacted assets, and mitigation strategies. By correlating vulnerabilities with emerging threats and actors, you have a comprehensive view of your security posture to take proactive measures and protect against both known and potential future threats
- **Enriched IoC intelligence.** Gain advanced, detailed information about specific indicators that may signify a cybersecurity threat. The search function enables your analysts to fully understand the impact and access richer context effortlessly
- **Threat hunting queries.** Proactively search for cyber threats within your environment. These queries, based on the latest intelligence, are tailored to detect and investigate suspicious activities or indicators of compromise. By utilizing these queries, you can uncover hidden threats and take swift action to mitigate potential risks

Threat intelligence is in our DNA

Extensive experience and coverage

Benefit from our vast library of insights drawn from 500,000+ commercial customers, millions of consumers, and a network of 250 million+ sensors spanning across 175+ countries. Leverage the broadest layers of native detection solutions for unparalleled diversity and depth of threat intelligence.

Global research network

Rely on our team of 400+ internal researchers worldwide for comprehensive regional threat analysis, crucial for safeguarding multinational operations.

Industry-leading intelligence

Curated threat data minimizes false positives, relieving your analysts of unnecessary workload burdens.

Critical source of vulnerability intelligence

By leveraging our ZDI program supported by 16,000 external researchers and events like Pwn2Own, customers gain access to a wealth of diverse threat intelligence.

Law enforcement collaboration

Trusted by global law enforcement, we actively collaborates on investigations to provide your team with critical insights.

Go deeper on XDR alerts and ASRM risks

Enrich XDR alert investigations

Leverage the effectiveness of the Trend Vision One XDR workbench alerts by providing comprehensive threat intelligence. This means going beyond just showing what happened and also revealing the "who, why, and how" behind the attack.

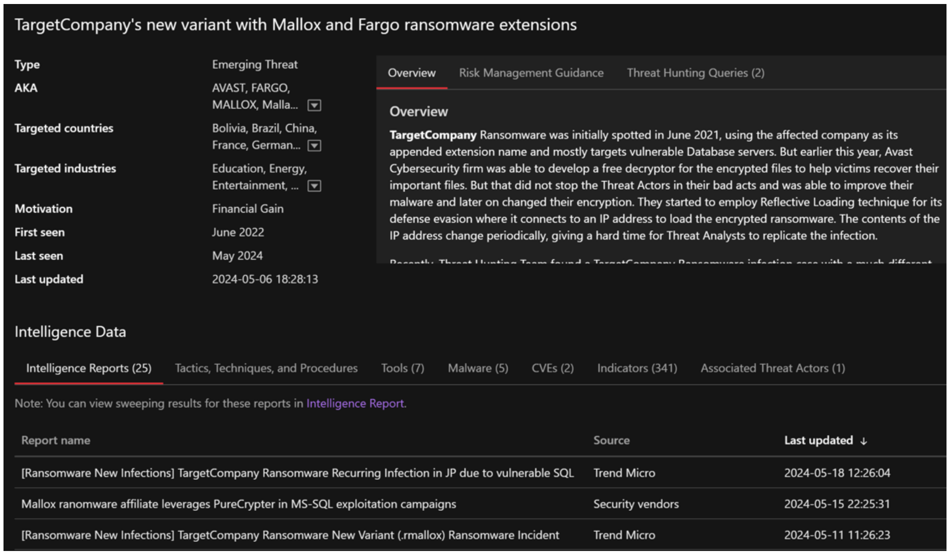
Elevate ASRM vulnerability management

Take your vulnerability management to the next level by showing emerging threats, threat actors, and hunting queries associated with the specific Common Vulnerabilities and Exposures (CVEs) in your environment. This allows your team to make faster and more informed risk management decisions.

Features at a glance

	INCLUDED WITH XDR	TREND VISION ONE – THREAT INSIGHTS
Endpoint, Email, Network, Cloud Integration	●	●
Automated Investigations	●	●
Custom Intelligence Sweeping	●	●
Open-Source Intelligence Feeds	●	●
Emerging Threats and Threat Actors		●
Vulnerability Intelligence		●
Enriched IoCs Intelligence		●
Threat Hunting Queries		●

Rich details on a specific threat - targeted countries, industries, risk management guidance, hunting queries, TTPs, CVEs, IOCs, and more.



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

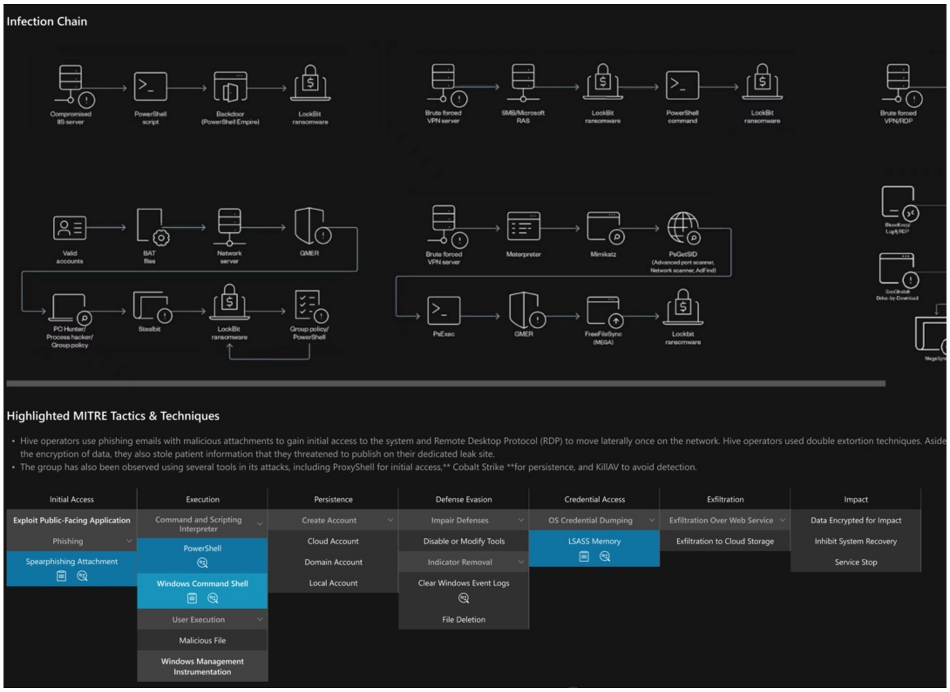
Intelligence Data

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

Mapped adversary tactics, techniques, and procedures to the MITRE ATT&CK framework.



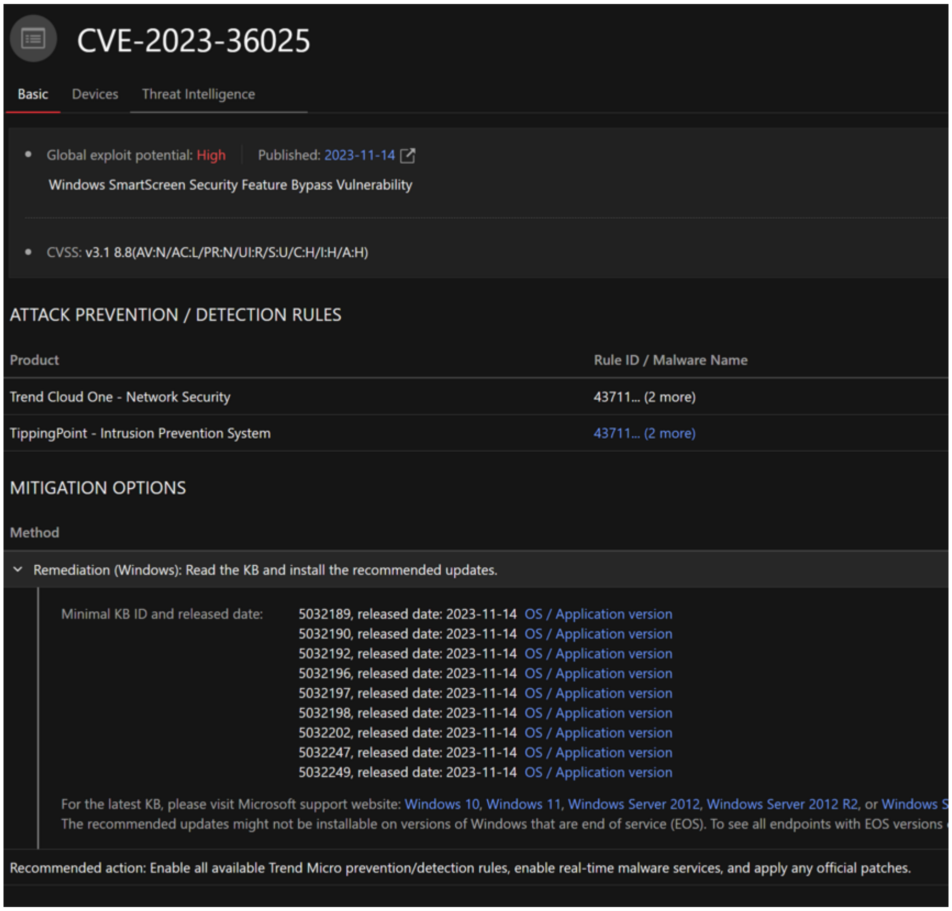
Infection Chain

Highlighted MITRE Tactics & Techniques

- Hive operators use phishing emails with malicious attachments to gain initial access to the system and Remote Desktop Protocol (RDP) to move laterally once on the network. Hive operators used double extortion techniques. Aside the encryption of data, they also stole patient information that they threatened to publish on their dedicated leak site.
- The group has also been observed using several tools in its attacks, including ProxyShell for initial access,** Cobalt Strike **for persistence, and KillAV to avoid detection.

Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Exfiltration	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Create Account	Impair Defenses	OS Credential Dumping	Exfiltration Over Web Service	Data Encrypted for Impact
Phishing	PowerShell	Cloud Account	Disable or Modify Tools	LSASS Memory	Exfiltration to Cloud Storage	Inhibit System Recovery
Spearphishing Attachment	Windows Command Shell	Domain Account	Indicator Removal			Service Stop
	User Execution	Local Account	Clear Windows Event Logs			
	Malicious File		File Deletion			
	Windows Management Instrumentation					

Vulnerabilities intelligence allows a search for a specific CVE to get the exploit potential, mitigation options, hunting queries, and more.



CVE-2023-36025

- Global exploit potential: High | Published: 2023-11-14
  Windows SmartScreen Security Feature Bypass Vulnerability
- CVSS: v3.1 8.8(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

ATTACK PREVENTION / DETECTION RULES

Product	Rule ID / Malware Name
Trend Cloud One - Network Security	43711... (2 more)
TippingPoint - Intrusion Prevention System	43711... (2 more)

MITIGATION OPTIONS

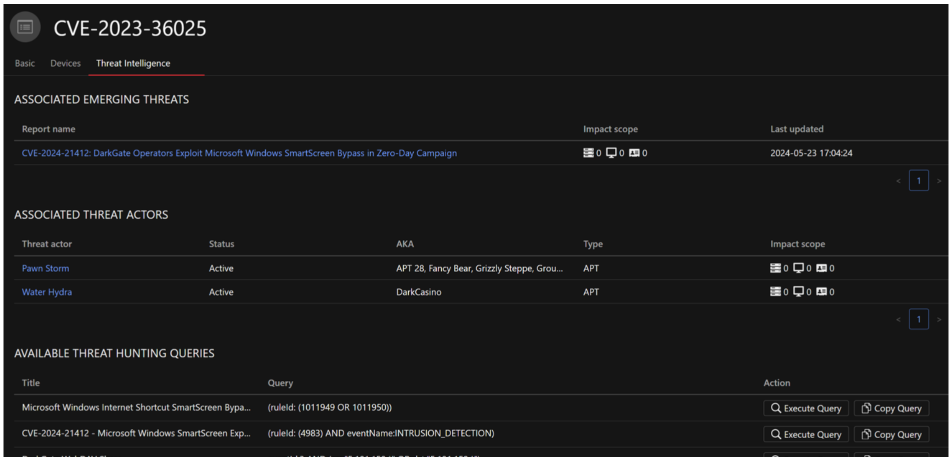
Method

Remediation (Windows): Read the KB and install the recommended updates.

Minimal KB ID and released date:	
	5032189, released date: 2023-11-14 OS / Application version 5032190, released date: 2023-11-14 OS / Application version 5032192, released date: 2023-11-14 OS / Application version 5032196, released date: 2023-11-14 OS / Application version 5032197, released date: 2023-11-14 OS / Application version 5032198, released date: 2023-11-14 OS / Application version 5032202, released date: 2023-11-14 OS / Application version 5032247, released date: 2023-11-14 OS / Application version 5032249, released date: 2023-11-14 OS / Application version

For the latest KB, please visit Microsoft support website: Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, or Windows S
The recommended updates might not be installable on versions of Windows that are end of service (EOS). To see all endpoints with EOS versions

Recommended action: Enable all available Trend Micro prevention/detection rules, enable real-time malware services, and apply any official patches.



CVE-2023-36025

ASSOCIATED EMERGING THREATS

Report name	Impact scope	Last updated
CVE-2024-21412: DarkGate Operators Exploit Microsoft Windows SmartScreen Bypass in Zero-Day Campaign	0 0 0	2024-05-23 17:04:24

ASSOCIATED THREAT ACTORS

Threat actor	Status	AKA	Type	Impact scope
Pawn Storm	Active	APT 28, Fancy Bear, Grizzly Steppe, Grou...	APT	0 0 0
Water Hydra	Active	DarkCasino	APT	0 0 0

AVAILABLE THREAT HUNTING QUERIES

Title	Query	Action
Microsoft Windows Internet Shortcut SmartScreen Bypa...	(ruleId: (1011949 OR 1011950))	Execute Query Copy Query
CVE-2024-21412 - Microsoft Windows SmartScreen Exp...	(ruleId: (4983) AND eventName:INTRUSION_DETECTION)	Execute Query Copy Query

[DS01_Threat_Insights_Datasheet_240626US]