

Update on WhisperGate, Destructive Malware Targeting Ukraine – Threat Intelligence & Protections Update

trellix.com/en-us/about/newsroom/stories/threat-labs/update-on-whispergate-destructive-malware-targeting-ukraine.html



Stories

The latest cybersecurity trends, best practices, security vulnerabilities, and more

By [Taylor Mullins](#), [Mo Cashman](#) and [Raj Samani](#) · January 20, 2022

Recent news reports of a “ransomware” campaign targeting Ukraine has resulted in significant press coverage regarding not only attribution but also possible motive. Unlike traditional ransomware campaigns where the motive is obvious, this campaign is believed to be pseudo in nature. In other words, the intention is likely to cause destruction of infected systems since the wiper at stage 4 simply overwrites data on the victim’s system, meaning

no decryption is possible. The malicious software drops a fake ransomware note while overwriting the master boot record in the background. The ransom note contains a Bitcoin address to send the ransom payment and contains a Tox ID to contact the threat actor. The infection process is carried out using the publicly available Impacket tool.

While the WhisperGate malware was initially detected in attacks against Ukraine, additional detections have started to be seen across the globe. The [Trellix Advanced Threat Research Team](#) has put together the following analysis of WhisperGate.

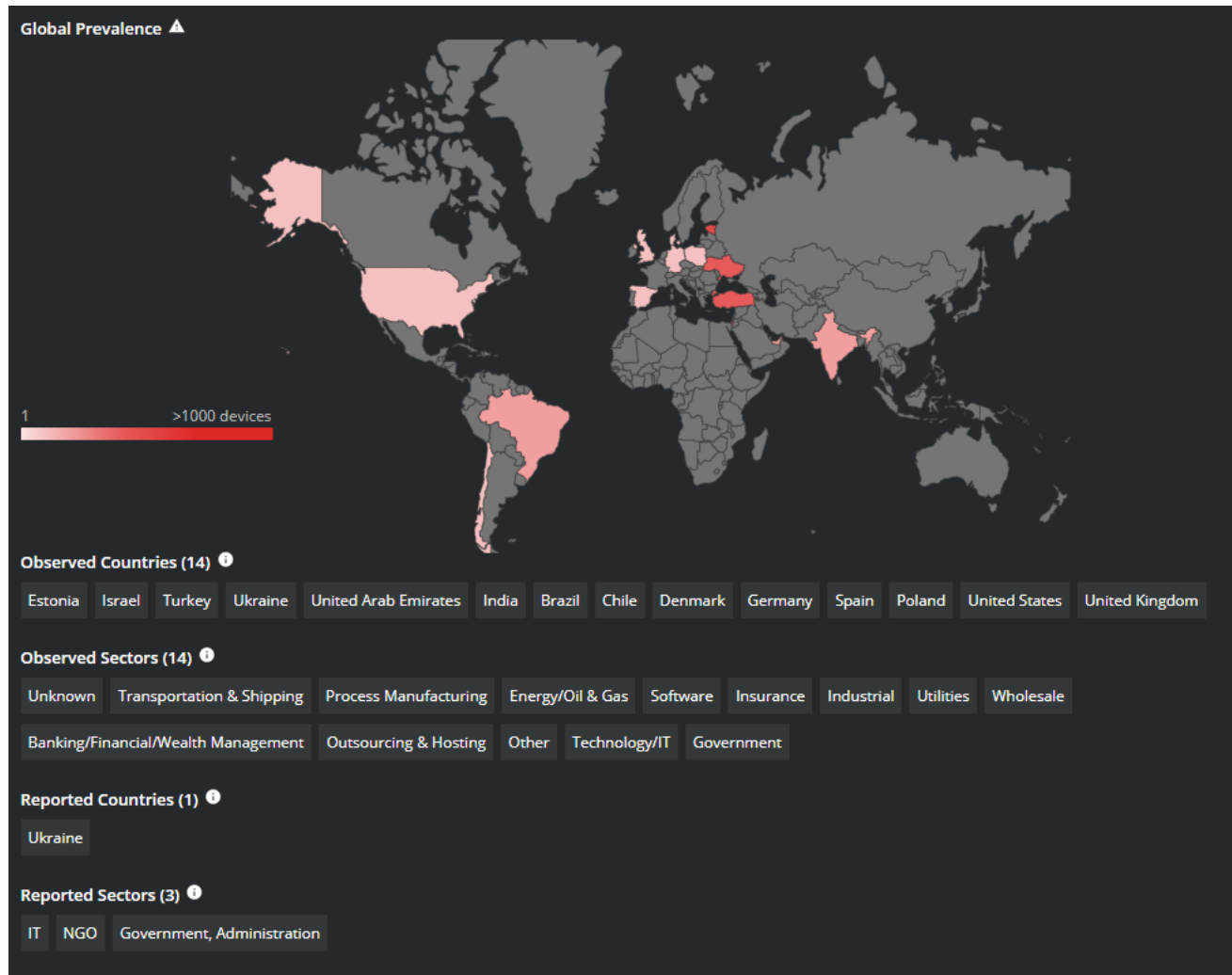


Figure 1. Global Prevalence of WhisperGate. Source: MVISION Insights

Recommended Steps to Mitigate against WhisperGate

The advisory released by the CISA provides several recommendations to secure your environment against WhisperGate that were gathered from their analysis of malware samples discovered in the wild.

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.

- Ensure that software is up to date, prioritizing updates that address vulnerabilities being exploited.
- Disable all ports and protocols that are not essential for business purposes.
- Ensure that Cloud Service security controls have been reviewed and implemented.

CISA: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

Open-Source Tools Being Observed in Attacks

An open-source tool being observed in attacks using WhisperGate is Impacket. Impacket is a collection of Python scripts that can be used by an attacker to target Windows network protocols. This tool can be used to enumerate users, capture hashes, move laterally and escalate privileges. Impacket has also been used by APT groups, in particular Wizard Spider and Stone Panda.

In the observed intrusions related to WhisperGate, the malware executes via Impacket to assist threat actors in lateral movement and execution.

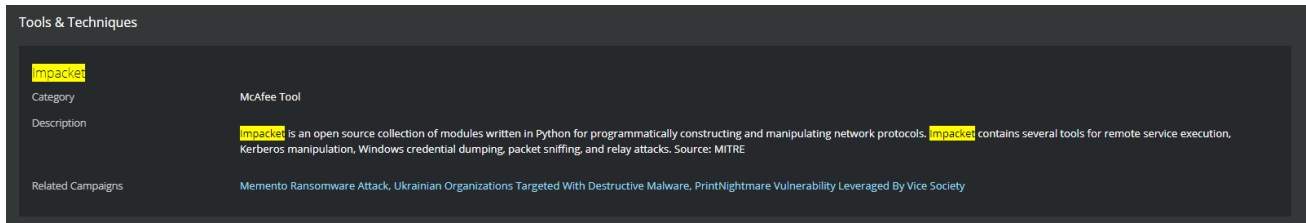
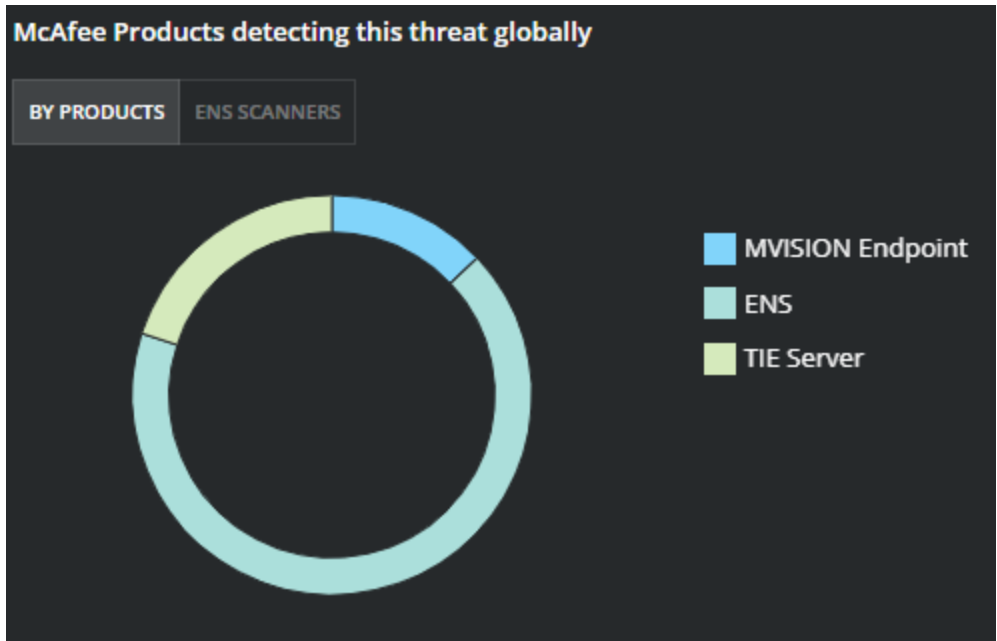


Figure 2. Tool Description and Campaigns Utilizing Impacket. Source: MVISION Insights

Trellix Protections and Global Detections

Trellix Global Threat Intelligence is currently detecting all known analyzed indicators for this campaign.



Blocking WhisperGate Attacks with Endpoint Security

Trellix ENS is currently detecting WhisperGate IOCs from the standpoint of signature detections and the malware behavior associated with WhisperGate activity.

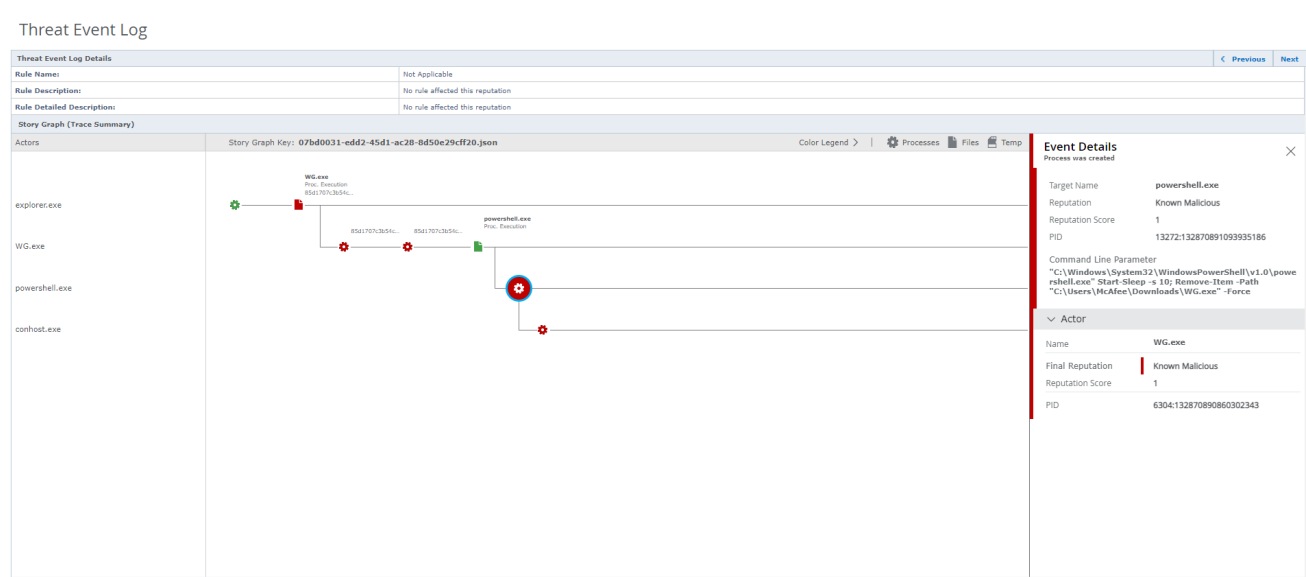


Figure 3. Story Graph summary of WhisperGate activity within ENS shown in MVISION ePO

WhisperGate Threat Intelligence from the Trellix Advanced Threat Research Team and MVISION Insights

MVISION Insights will provide the current threat intelligence and known indicators for WhisperGate. MVISION Insights will alert to detections and Process Traces that have been observed and systems that require additional attention to prevent widespread infection.

MVISION Insights will also include Hunting Rules for threat hunting and further intelligence gathering of the threat activity and adversary.

Campaign Name: Ukrainian Organizations Targeted with Destructive Malware

Analyzed Indicators (18) Export

MD5 (9) SHA256 (9) IP Address (0) IP:Port (0) URL (0) Domain (0) Hostname (0)

A196C6B8FFCB97FFB276D04F354696E2391311DB38...	9CDAACABA35C3A473EC5B652D035A9593EE822609E...
FF3B45ECFBDB780848B4C829D2B6078D8F7673D82...	DCBBAE5A1C61D8BBB7DCD6DC5DD1EB1169F5329958...
BBE1949FFD9188F5AD316C6F07EF4EC18BA00E375C...	251252E82E8CEF5B5F69E10DC5F7240E854CA13F39F...
35D56E74DB9D77C1F94D163F1628E9F167730AD44A...	9EF7DBD3DA51332A78EFF19146D21C82957821E464...
00BC665D96ECADC68EB2A9384773A70391F08F8E7A...	

Figure 4. Analyzed Indicators with Detections. Source: MVISION Insights

Ukrainian Organizations Targeted With Destructive Malware > DUCK101 > Event > File Name: Whisper.exe
Process Trace

Start (svchost.exe) → Create Process (consent.exe) → Create Process (Whisper.exe) → Loads DLL (Whisper.exe) → Exit Process (Whisper.exe) → Loads DLL (Whisper.exe) → is associated with (Ukrainian Organizati...)

Process: C:\Users\iofuscated\Downloads\Whisper.exe

Activity	Create Process
Timestamp	Jan 19, 2022 11:42:13 AM -06:00
Command-Line Arguments	"iofuscated\Downloads\Whisper.exe"
SHA256	a196c6b8ffcb97fb276d04f354696e2391311db38...
SHA1	189166e332c73c242ba5889d5798...
MD5	545c9a0ba7d927346ca24fa7973f...
File Size	27 KB
First Seen	4 days ago
Classification Name	Risk.Generic.Dlx
Classification Type	Trojan
Category	Payload delivery
Insights Type	Analysed
Comments	Sage1.exe

Determinism: Unique
Lethality: Destructive

United States Turkey Israel
Brazil Germany Estonia India
Prevalent in Country: Ukraine United Kingdom
United Arab Emirates Chile Spain
Denmark Poland
Banking/Financial/Wealth Management
Other Transportation & Shipping
Prevalent in Sector: Energy/Oil & Gas Industrial
Insurance Outsourcing & Hosting
Process Manufacturing Software
Technology/IT Utilities Wholesale

Run Real-Time Search on EDR
View this IOC

Figure 5. Process Trace of WhisperGate Activity. Source: MVISION Insights

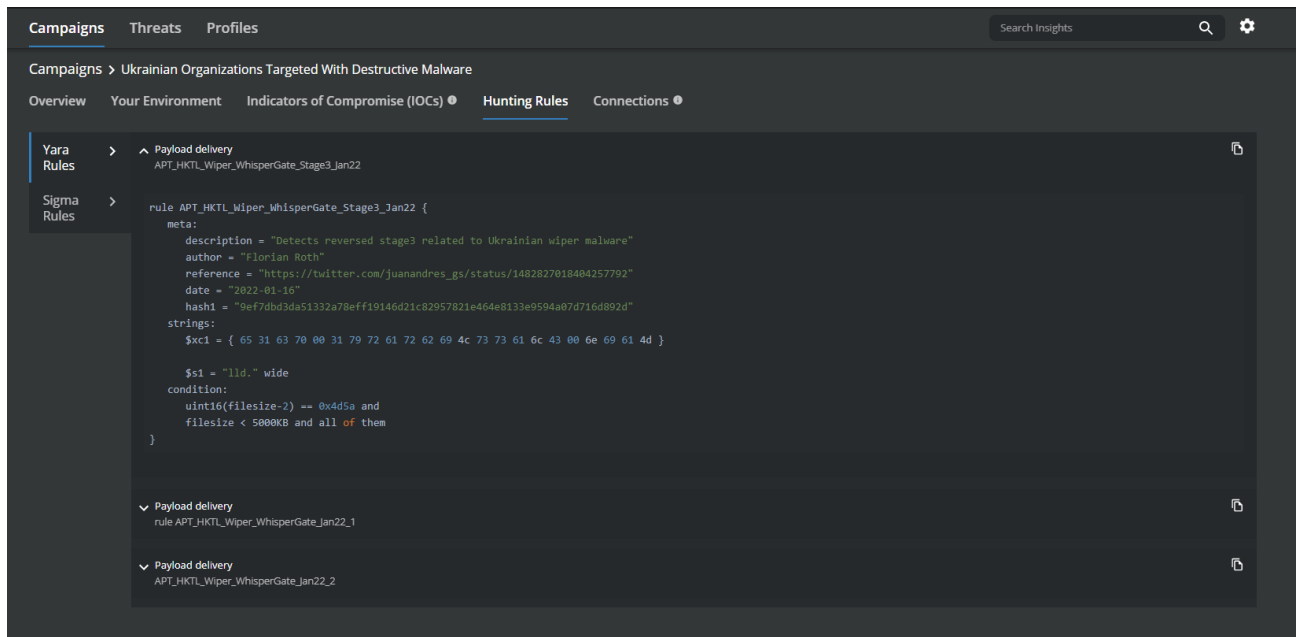


Figure 6. Hunting Rules for WhisperGate in MVISION Insights

Detecting Malicious Activity with MVISION EDR

MVISION EDR is currently alerting to the activity associated with WhisperGate and will note the MITRE techniques and any suspicious indicators related to the adversary activity.

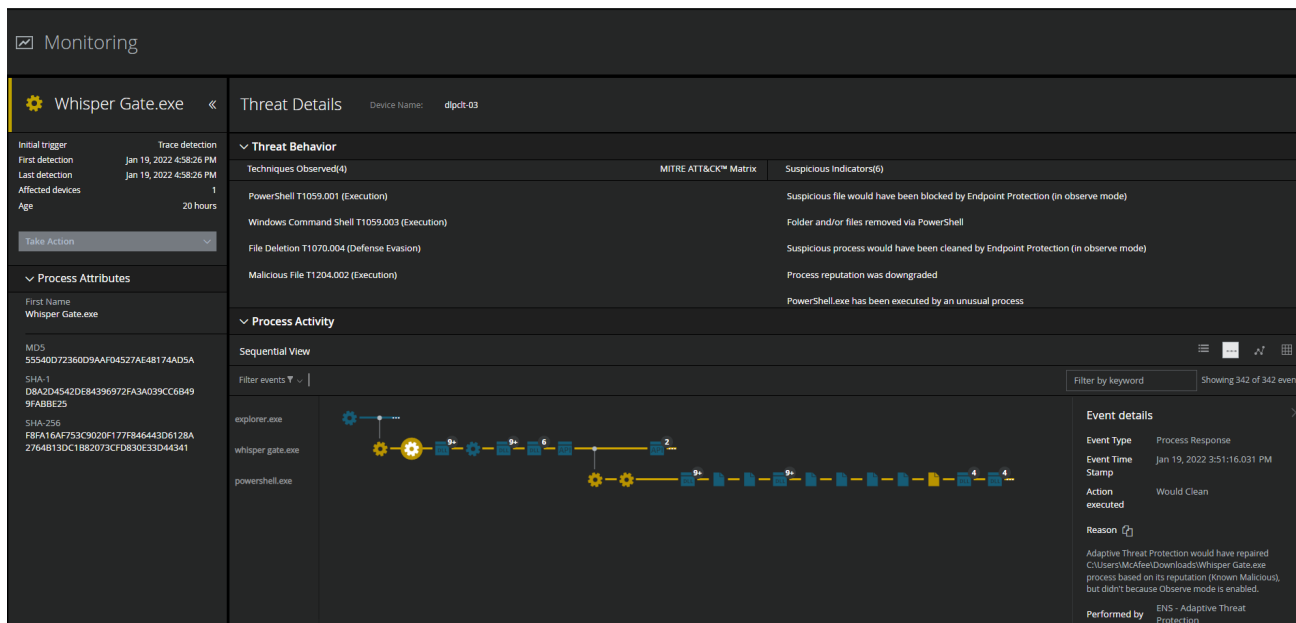


Figure 7. Threat Behavior and Process Activity for WhisperGate shown in MVISION EDR

Securing Cloud Services Against Attacks with MVISION Cloud

One of the recommendations by the CISA to mitigate against WhisperGate attacks is to ensure that cloud services and infrastructure are configured properly, and vulnerabilities patched. The Cloud Security controls provided in MVISION Cloud/UCE allow for

vulnerability scans and configuration audits of your cloud environment. Identifying areas of risks are critical to not allowing adversaries to gain initial access.

Policy Incidents

Incident Type: Vulnerability Violation | Severity: Critical

105 Incidents

Sev	Policy Name	Item Name	User Name	Incident Created On	Incident Response
Critical	High-Severity CVEs	queue-masterlatest	N/A	Dec 23, 2021 3:45 AM CST	Violation Detected
Critical	Medium-Severity CVEs	969247234605.dkr.ecr...shippinglatest	N/A	Dec 23, 2021 3:45 AM CST	Violation Detected
Critical	High-Severity CVEs	969247234605.dkr.ecr...dev-repo1:nginx-log4j-vulndemo-2.10	N/A	Dec 23, 2021 3:45 AM CST	Violation Detected
Critical	Medium-Severity CVEs	969247234605.dkr.ecr...dev-repo1:nginx-log4j-vulndemo-2.10	N/A	Dec 23, 2021 3:45 AM CST	Violation Detected
Critical	High-Severity CVEs	969247234605.dkr.ecr...front-endlatest	N/A	Dec 23, 2021 3:45 AM CST	Violation Detected
Critical	Medium-Severity CVEs	969247234605.dkr.ecr...front-endlatest	N/A	Dec 23, 2021 3:45 AM CST	Violation Detected

Vulnerability Incident (ID #480)

dev-repo1:nginx-log4j-vulndemo-2.10

Critical Severity

2 vulnerabilities were discovered in the 'dev-repo1:nginx-log4j-vulndemo-2.10' container image during a scan named 'cve-scan-5.0.0' that ran on Dec 23, 2021 3:41 AM CST

Service Name: Amazon Web Services
 Instance Name: Default
 Account Name: skyhighdemo.cloud
 Region: N/A
 Incident Created On: Dec 23, 2021 3:45 AM CST
 Last Updated: Jan 20, 2022 5:04 AM CST

Owner: [Select Owner] | Incident Status: [New]

MITRE: [Full View]

Container Vulnerability: 2

- CVE-2021-3973: vim
- CVE-2021-33574: glibc

Figure 8. Vulnerability Scan Violations for AWS shown in MVISION UCE

Policy Incidents Summary

Policy Incidents

Incident Type: Audit Violation | Service Name: Microsoft Azure

20 Incidents

Sev	Policy Name	Item Name	User Name	Incident Created On	Incident Response	Incident Status
Major	NSG Flow logs should be enabled	testad-nsg	N/A	Jan 17, 2022 7:44 AM CST	Violation Detected	New
Critical	Network security groups should not have unrestricted RDP access	testad-nsg	N/A	Jan 17, 2022 7:44 AM CST	Violation Detected	New
Critical	Network security group with non HTTP/HTTPS ports should not have unrestricted access	testad-nsg	N/A	Jan 17, 2022 7:44 AM CST	Violation Detected	New
Critical	Check Disable RDP access on Network Security Groups from Internet	testad-nsg	N/A	Jan 17, 2022 7:44 AM CST	Violation Detected	New
Major	NSG Flow logs should be enabled	aadds-nsg	N/A	Jan 12, 2022 9:29 AM CST	Violation Detected	New
Critical	Network security groups should not have unrestricted RDP access	aadds-nsg	N/A	Jan 12, 2022 9:29 AM CST	Violation Detected	New
Critical	Network security groups should not have unrestricted RDP access	aadds-nsg	N/A	Jan 12, 2022 9:29 AM CST	Violation Detected	New

Config Audit Policy Incident (ID #30440)

Network security groups should not have unrestricted RDP access

testad-nsg, has RDP access on Network Security Group from Internet : 010040e9-c4e6-4350-9dae-64f115c90795 (CSM Dashboard ...more)

It was discovered during a scan named 'Continuous Security Configuration Audit for Azure (29329)' that ran on Jan 17, 2022 7:44 AM CST. Action taken was Violation Detected.

Severity: Critical

Service Name: Microsoft Azure
 Instance Name: Azure-09642982
 Incident Created On: Jan 17, 2022 7:44 AM CST
 Last Updated: Jan 17, 2022 7:44 AM CST
 Last Response: Violation Detected
 User: N/A
 CIS Level: LEVEL1
 Account ID: 010040e9-c4e6-4350-9dae-64f115c90795
 Account Name: CSM Dashboard

What you can do

1. Login to Azure portal
2. Navigate to Network security groups page
3. Select the required Network security group
 - a. Select inbound security rules under Settings
 - b. Identify and select the security rule with port number 3389 which allows unrestricted access from source 'Any' or source 'Internet'
 - c. Under 'Action' toggle select Deny
 - d. Save the security rule

Owner: [Unassigned]

Figure 9. Configuration Audit Incidents for Azure shown in MVISION UCE

Trellix offers Threat Intelligence Briefings along with Cloud Security and Data Protection workshops to provide customers with best practice recommendations on how to utilize their existing security controls to protect against adversarial and insider threats, please reach out if you would like to schedule a workshop with your organization.

Featured Content

PERSPECTIVES

Our CEO On Living Security

By [Bryan Palma](#) · January 19, 2022

Trellix CEO, Bryan Palma, explains the critical need for security that's always learning.

[Read More](#)

XDR

Time to Drive Change by Challenging the Challengers

By [Michelle Salvado](#) · January 19, 2022

Dynamic threats call for dynamic security – the path to resiliency lies in XDR.

[Read More](#)

THREAT LABS

2022 Threat Predictions

By [Trellix](#) · January 19, 2022

What cyber security threats should enterprises look out for in 2022?

[Read More](#)

Get the latest

We're no strangers to cybersecurity. But we are a new company.
Stay up to date as we evolve.

Please enter a valid email address.

Zero spam. Unsubscribe at any time.