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

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.

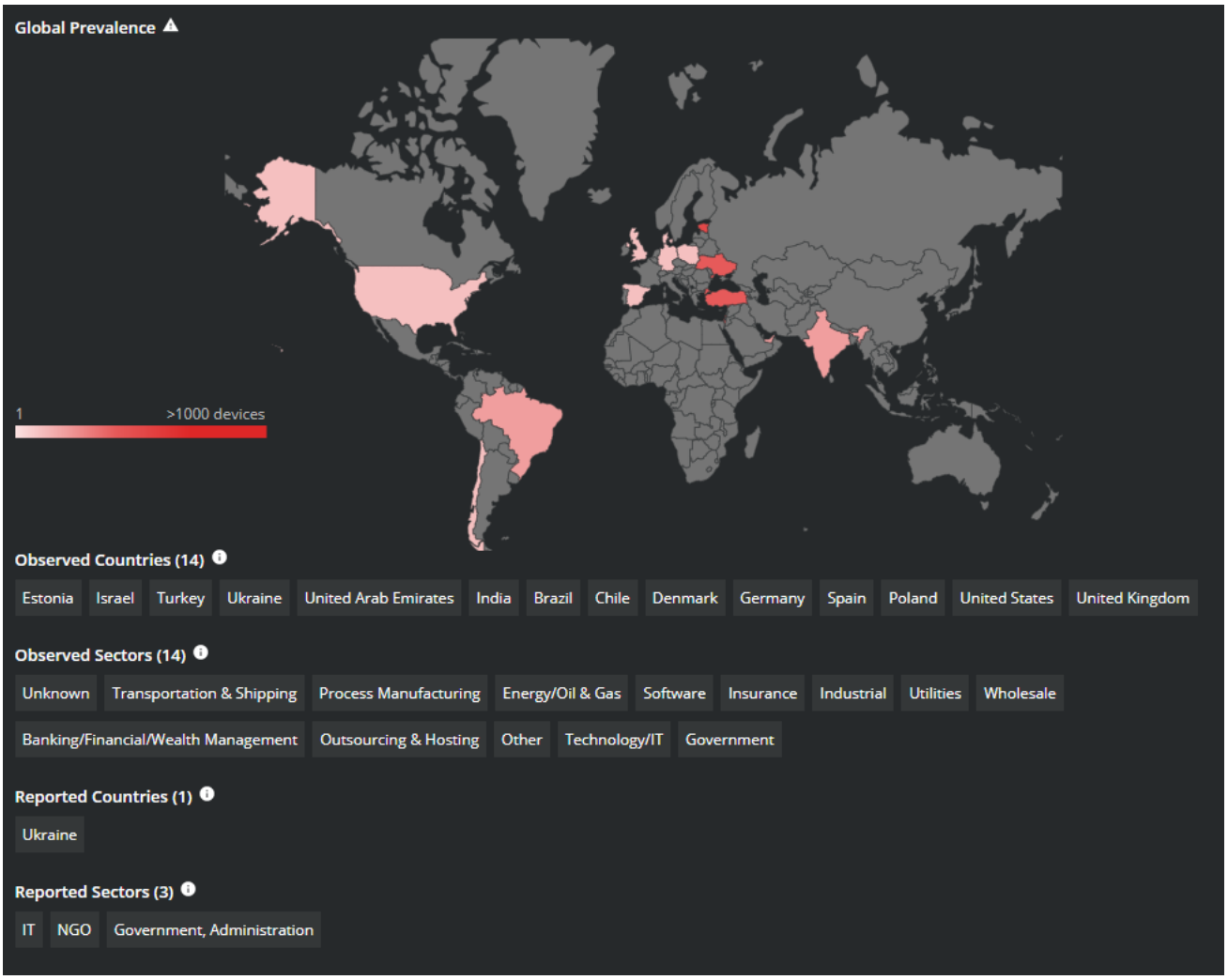


Figure 1. Global Prevalence of WhisperGate. Source: MVISION Insights

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.

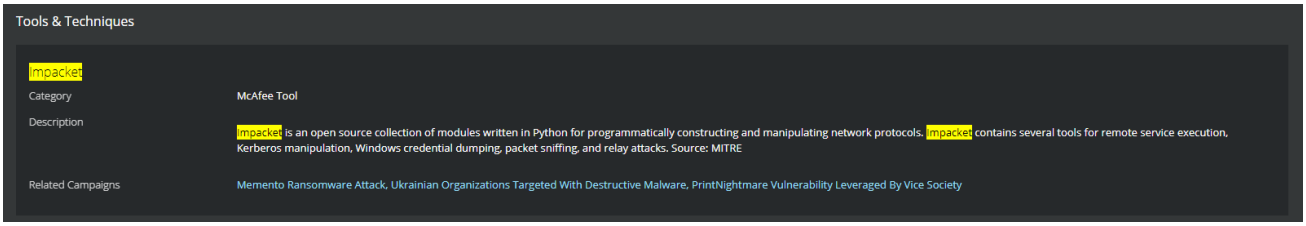
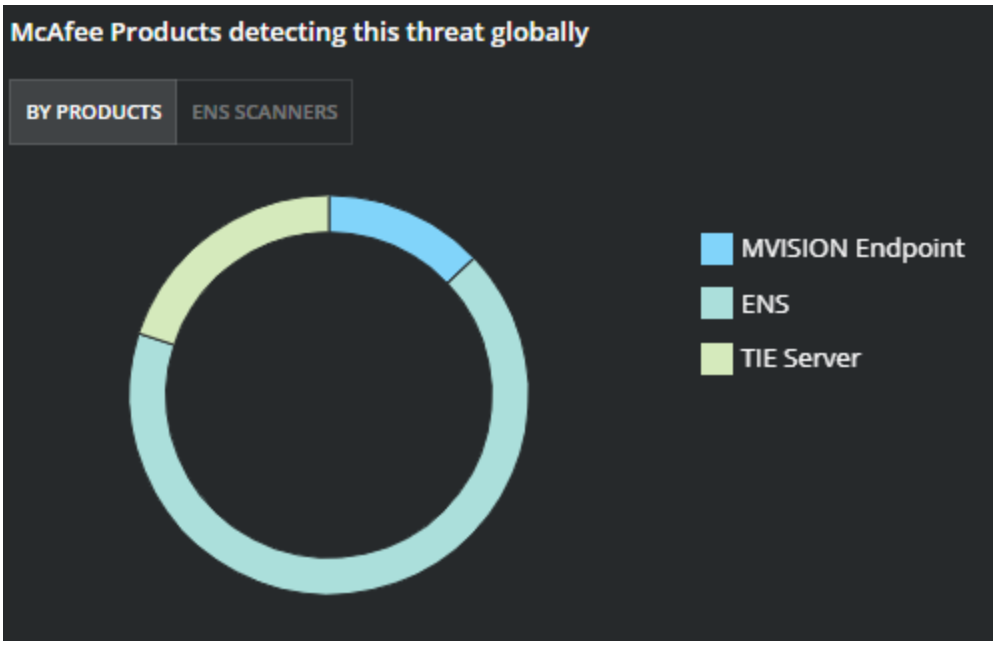


Figure 2. Tool Description and Campaigns Utilizing Impacket. Source: MVISION Insights

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.

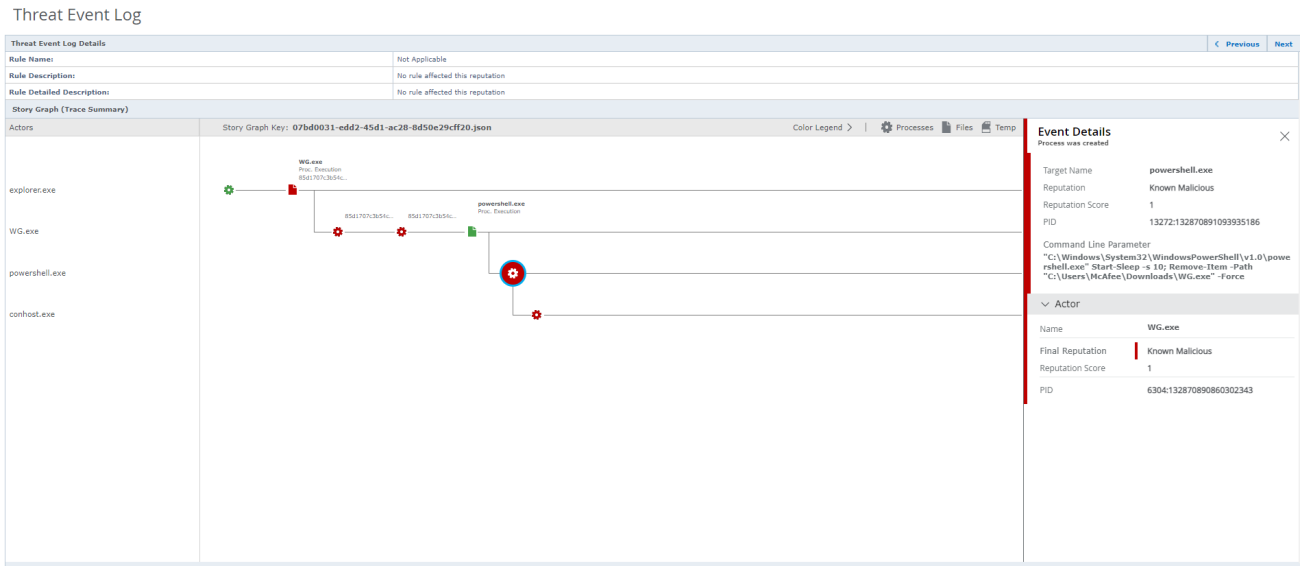


Figure 3. Story Graph summary of WhisperGate activity within ENS shown in MVISION ePO

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

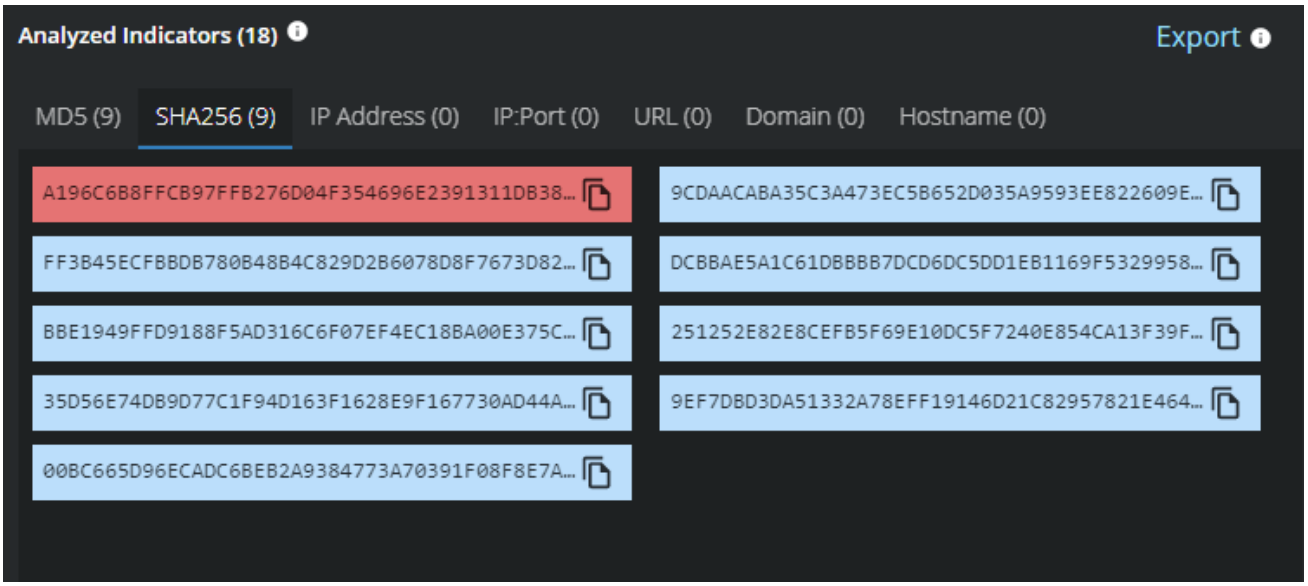


Figure 4. Analyzed Indicators with Detections. Source: MVISION Insights

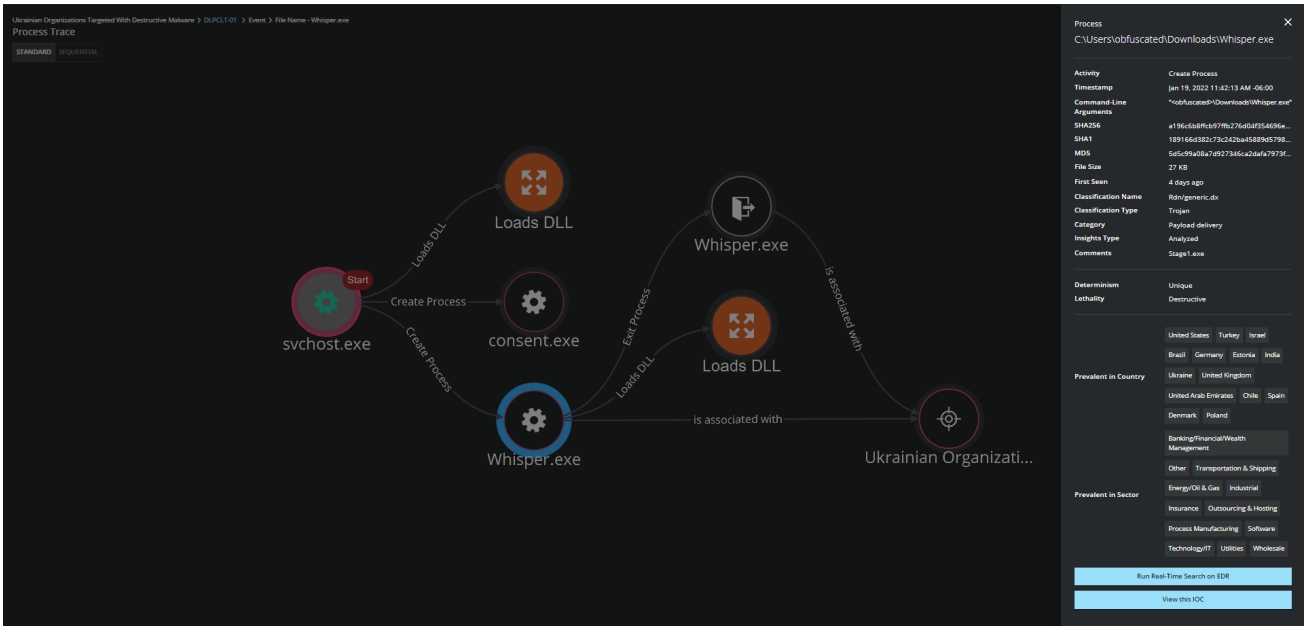


Figure 5. Process Trace of WhisperGate Activity. Source: MVISION Insights

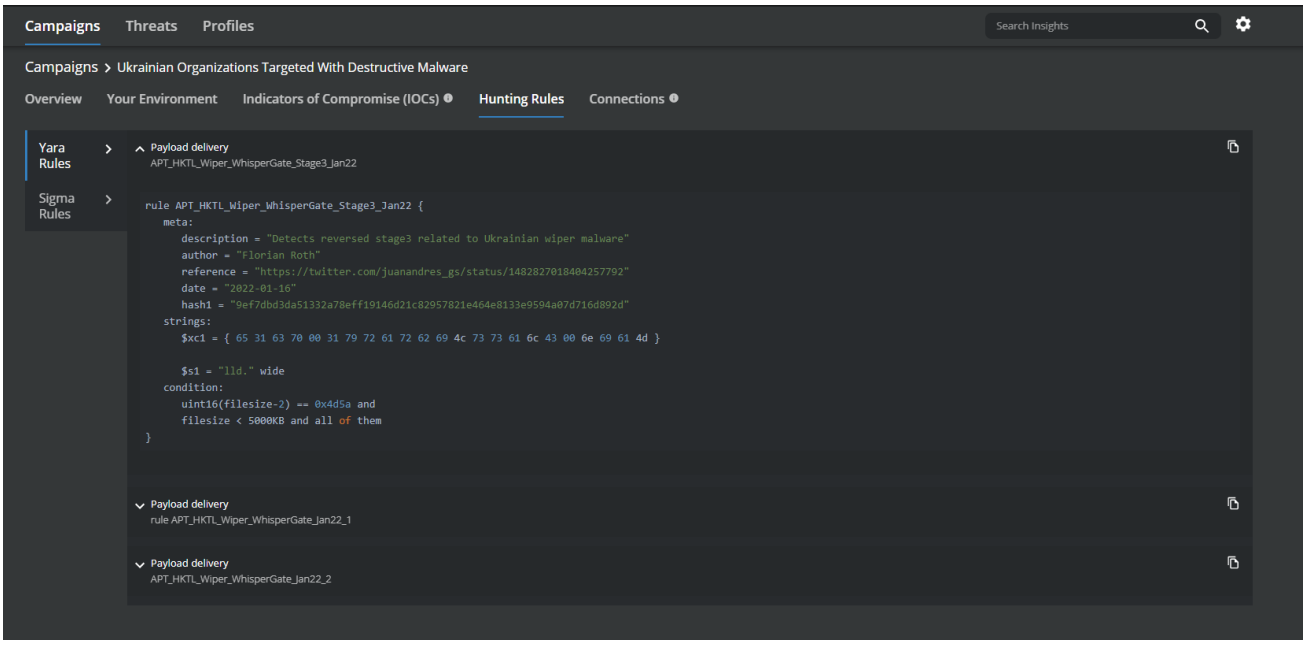


Figure 6. Hunting Rules for WhisperGate in MVISION Insights

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.

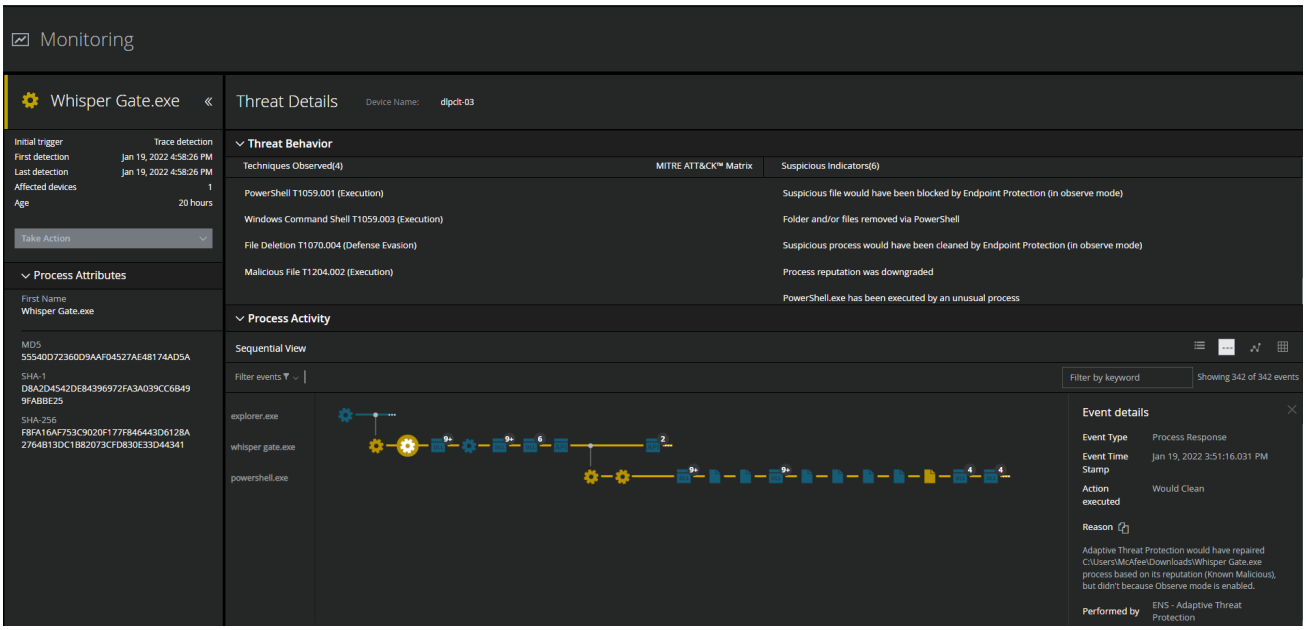


Figure 7. Threat Behavior and Process Activity for WhisperGate shown in MVISION EDR

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.

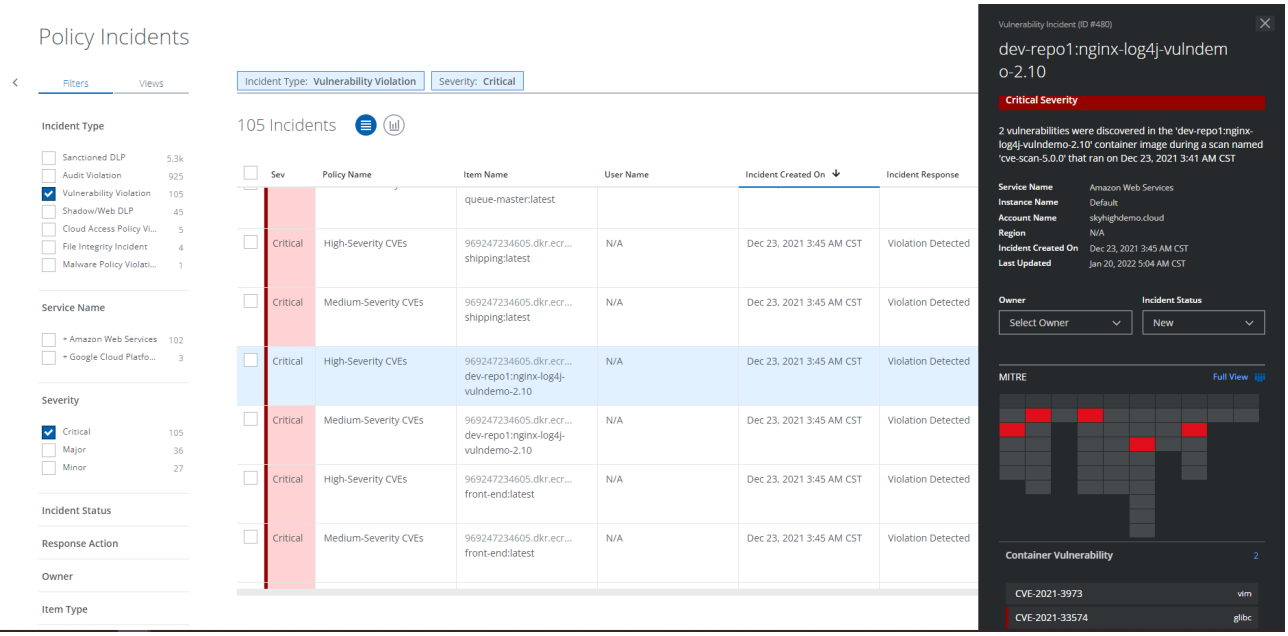


Figure 8. Vulnerability Scan Violations for AWS shown in MVISION UCE

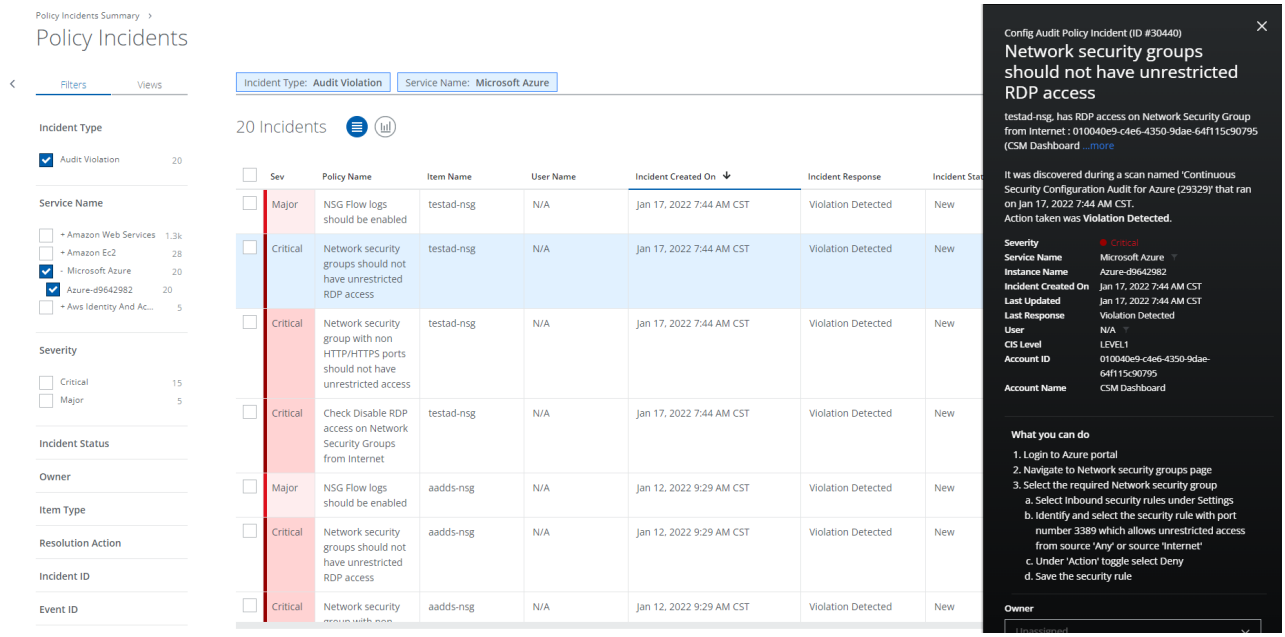


Figure 9. Configuration Audit Incidents for Azure shown in MVISION UCE

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.