- Classified - Confidential -

SmartApeSg Delivering NetSupport RAT

Note:

This document is a comprehensive overview of our Malware Detection and Report services, specifically tailored for one of our clients.

The document have been reclassified from "Confidential" to "Unclassified," it's been carefully edited to remove all sensitive information, ensuring the privacy and security of all parties involved.

Through this report, we aim to showcase our methodical approach to identifying, analyzing, and recommending actions against malware threats that our clients might face. It is crafted to reflect the meticulous attention to detail and thoroughness we apply in monitoring and detecting malware, embodying our commitment to maintaining the highest standards of cybersecurity.

Our role includes detecting malware, analyzing it, and offering recommendations to mitigate threats. We also provide IR (Incident Response) frameworks and playbooks for various scenarios, ensuring readiness for a structured response. While some clients take on the implementation of these measures, we're prepared to lead in response, containment, isolation, and eradication of threats, using our expertise to effectively manage incidents from start to finish.

- Classified - Confidential -

Table of contents

- Classified - Confidential -

Executive Summary

On February 26th, our Security Operations Center (SOC) at HoundBytes identified critical security alerts through our advanced Threat Intelligence (TI) systems after recent security agent installation on the host. These alerts were triggered by the discovery of a known malicious hash indicator within a critical library file on an organizational laptop. This finding points to the presence of the NetSupport RAT, a sophisticated malware known for allowing unauthorized remote access and control over the infected systems. This discovery underscores the importance of vigilant monitoring and immediate response to mitigate potential security breaches.

Incident Overview

The alert was initiated following the identification of a hash corresponding to a Dynamic-Link Library (DLL) file utilized by the OpenVPN executable on the device identified as client-asset. The operation, executed under the SYSTEM user account, highlighted elevated system privileges. The DLL, named libssl-3-x64.dll, is part of the Pritunl VPN client installed on the device, recognized by its MD5 hash 4ad9afd9ff710d89aa7530241771f9d9. The presence of this hash indicated a compromise, suggesting that the device was at risk of being exploited by malicious actors through the NetSupport RAT.

Threat Analysis

Further analysis confirmed that the implicated DLL version, libssl version 3.1.1, had been compromised and potentially modified to function as a component of the NetSupport RAT infrastructure. This RAT is known for its capabilities to remotely control infected devices, execute arbitrary commands, access confidential information, and potentially distribute further malware. The use of a compromised VPN client DLL for such purposes is particularly concerning, as it can allow attackers to intercept and decrypt VPN traffic, facilitating unauthorized access to sensitive organizational data and systems.

We have identified a likely source of the security breach as an outdated version of a widely-used VPN application, specifically an older iteration of its lib-ssl library. To verify our hypothesis, we conducted a control experiment by installing Pritunl on a fresh Windows setup and examined the hash of the potentially compromised file. The findings confirmed that the file in question was not corrupted on the new installation, strongly suggesting that the malware infection is associated with an outdated and vulnerable version of the software on the initially affected computer. It is imperative that any system running this specific software version undergoes a thorough security review immediately.

- Classified - Confidential -

Risk Assessment

The discovery of the NetSupport RAT within our network represents a significant risk to the confidentiality, integrity, and availability of our organizational data. The RAT's ability to bypass security measures, coupled with its potential for data exfiltration and lateral movement within the network, poses a severe threat to our security posture. The interception of encrypted communications by unauthorized parties could result in substantial harm to the organization's operations and reputation.

The gravity of this situation cannot be overstated, meriting the highest possible alert level. Given that the compromised computer is primarily used for HR and financial operations, the potential for significant harm is high. This machine also enjoys unrestricted access to our VPN, thereby posing a risk to the entirety of our network infrastructure. Additionally, the physical location of this computer increases the risk of internal network compromise if it is connected within the office environment

Conclusion and Confirmation

The collective evidence, from the clean DLL in the controlled test to the suspicious IP address previously involved in cyber attacks and known as a command-and-control (C2) server, leads us to confirm this incident as a true positive. The sophistication of this malware, along with its classification as a potentially new strain of Advanced Persistent Threat (APT), underscores the severity of the threat. The urgency is further amplified by the fact that alerts have been triggered in other quarters, indicating a broader concern.

Recommendations

To mitigate the risks posed by this incident, we recommend the following immediate actions:

Isolation and Investigation

Temporarily disconnect the impacted laptop from our network to halt any potential lateral movement or data exfiltration. A comprehensive investigation should be conducted to determine whether any data has been compromised or if the adversary has obtained further network access.

Patch and Update

Verify and update all instances of the Pritunl VPN client and the libssl library across the organization to the latest version, addressing this vulnerability. Should a patch be unavailable, assess alternative solutions devoid of known vulnerabilities.

Enhanced Monitoring

Augment monitoring of network traffic, with a particular focus on VPN connections, to identify any unusual activities indicative of data interception or exfiltration.

Awareness and Training

Strengthen security awareness among staff, underlining the significance of reporting suspicious activities and the inherent risks of utilizing compromised software.

Technical investigation

Threat Intel Hash Indicator Match

On 26th of February, HoundBytes SOC identified multiple Threat Intel Alerts related to a hash based IoC.

Rule description

This rule is triggered when a hash indicator from the Threat Intel Filebeat module or integrations has a match against an event that contains file hashes, such as antivirus alerts, process creation, library load, and file operation events.

Alert Reason

Library event with process openvpn.exe, by SYSTEM on client-asset created critical alert Threat Intel Hash Indicator Match.

Highlights

Host.name: client-asset

User.name: SYSTEM

Process.executable: C:\Program Files (x86)\Pritunl\openvpn\openvpn.exe

Dll.path: C:\Program Files (x86)\Pritunl\openvpn\libssl-3-x64.dll

Threat match detected

dll.hash.md5 4ad9afd9ff710d89aa7530241771f9d9

Indicator.file.hash.md5: 4ad9afd9ff710d89aa7530241771f9d9

Indicator.type: file

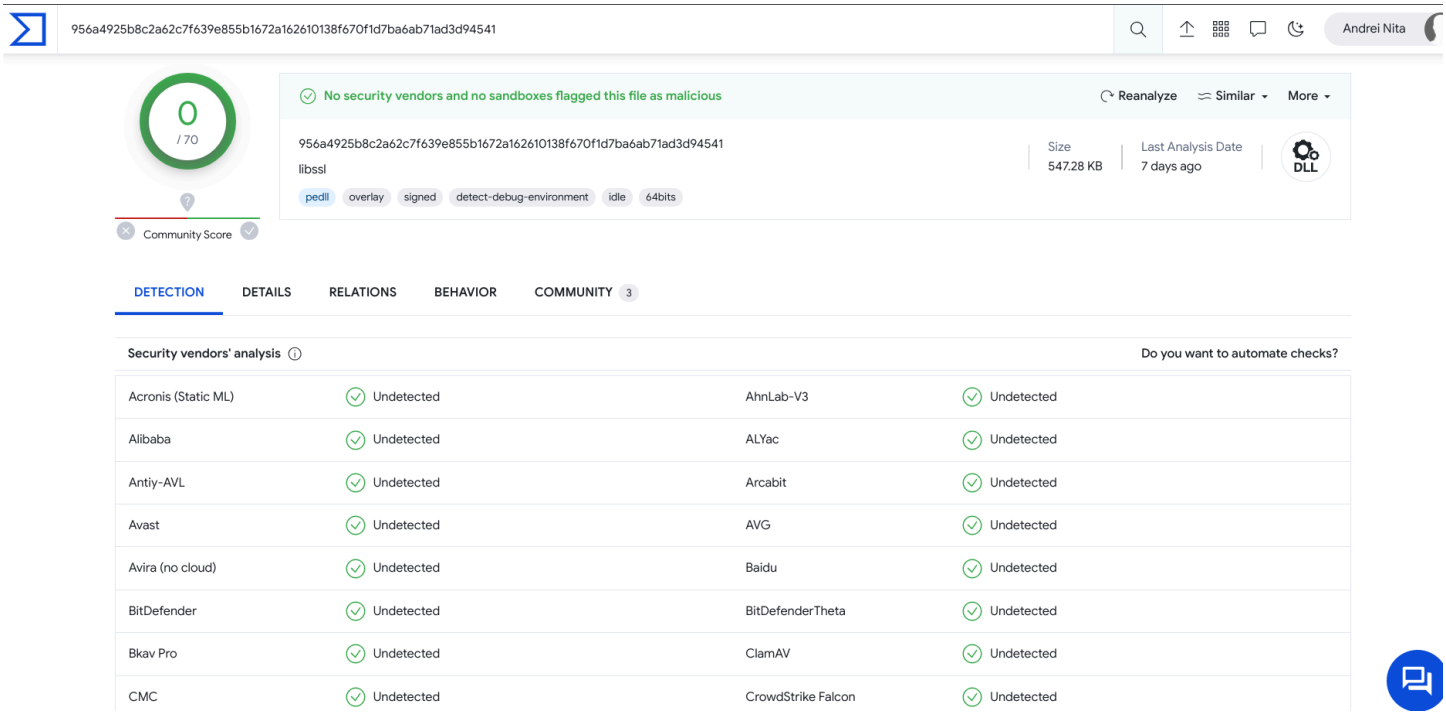
Matched.atomic: 4ad9afd9ff710d89aa7530241771f9d9

Matched.field: dll.hash.md5

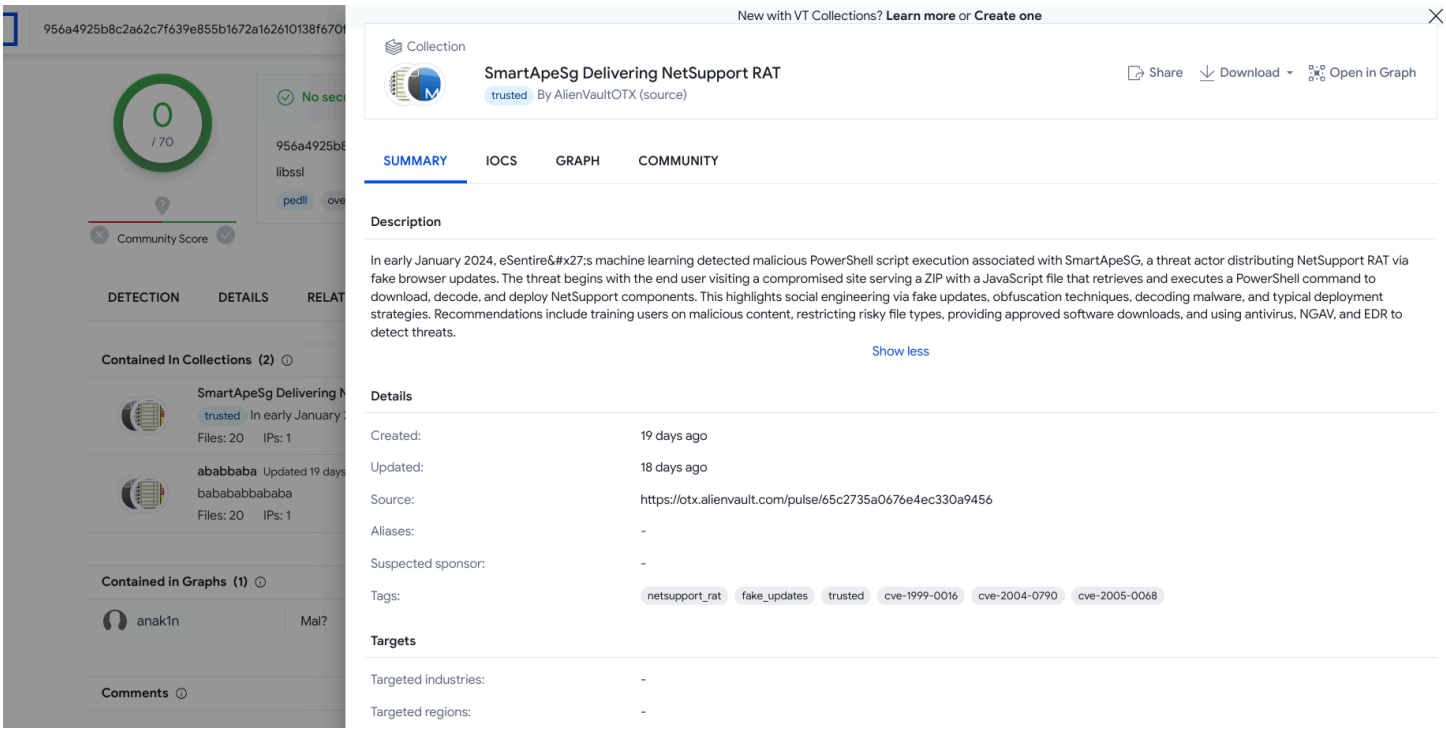
Matched.id: 0am25lfpW50tkQ2ScHBCpgBQc7g=

- Classified - Confidential -

Initial verification with VirusTotal:

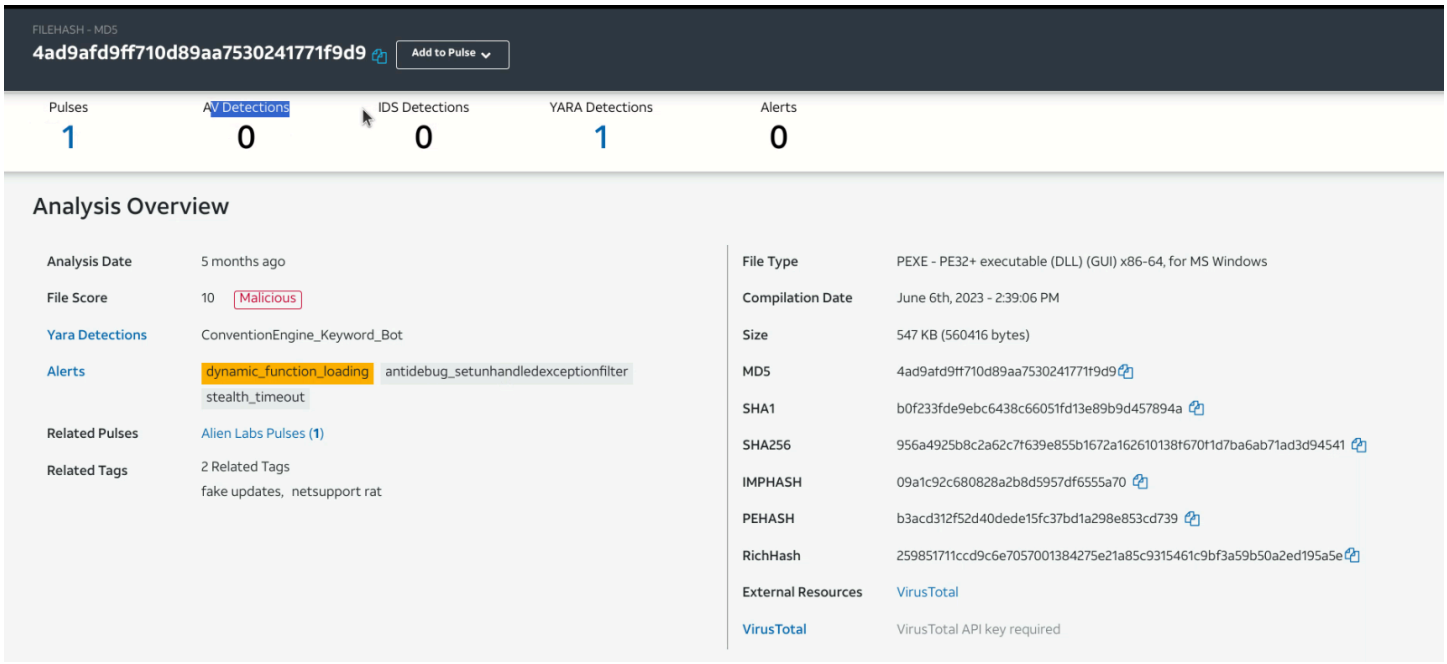


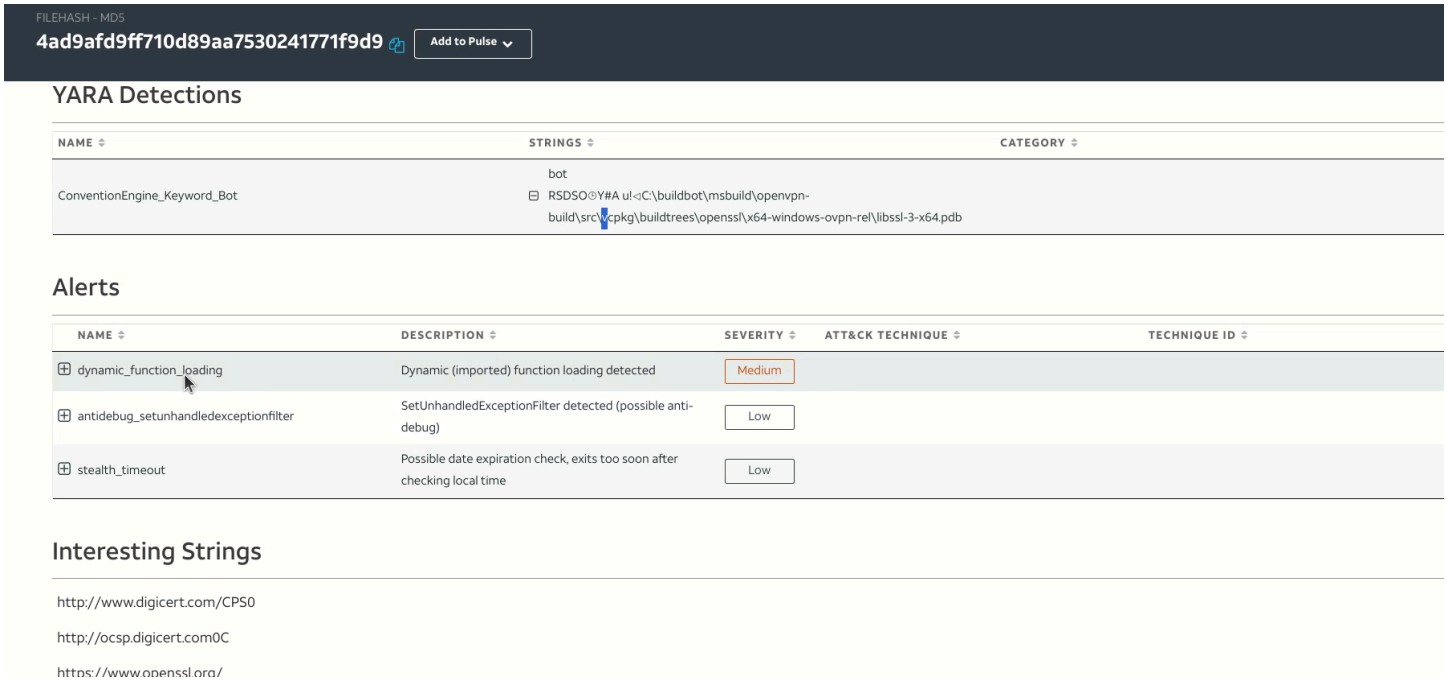
Normally all vendors are marking this as clean, however checking the community we can see the following things:



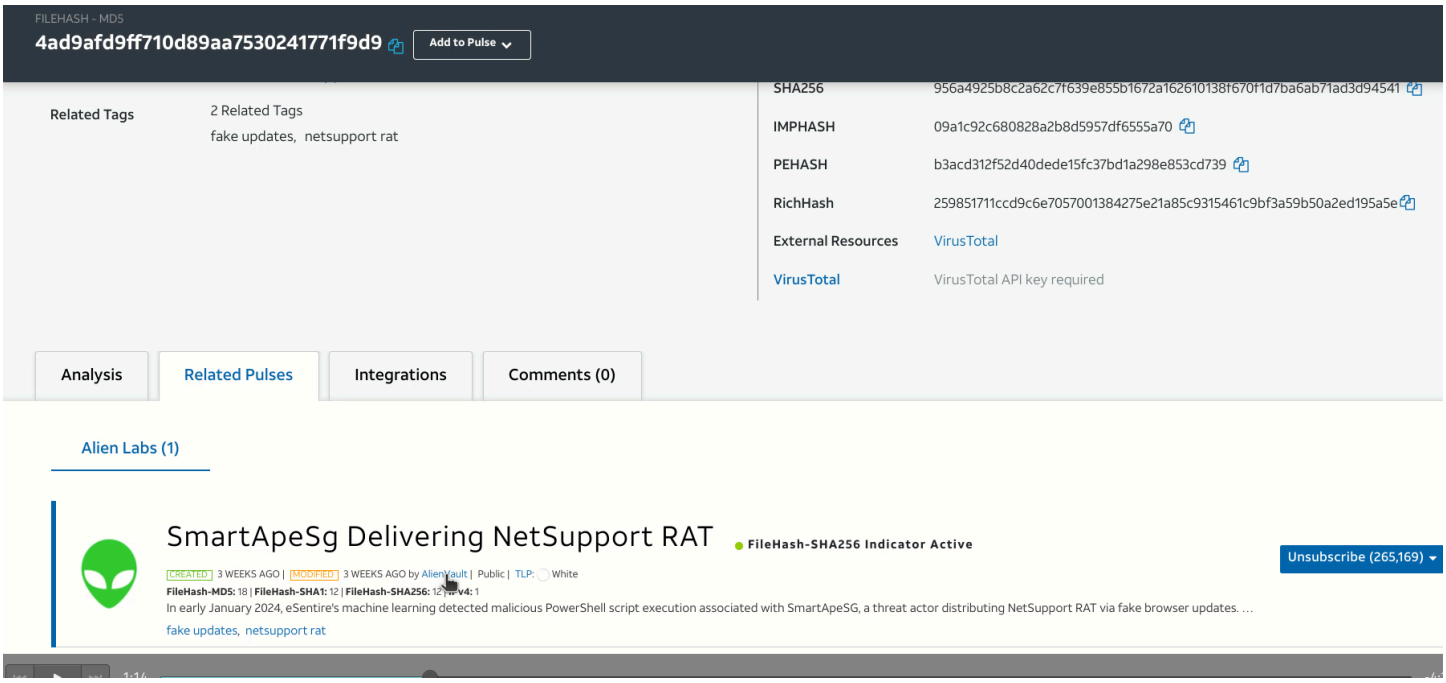
In early January 2024, eSentire's machine learning detected malicious PowerShell script execution associated with SmartApeSG, a threat actor distributing NetSupport RAT via fake browser updates. The threat begins with the end user visiting a compromised site serving a ZIP with a JavaScript file that retrieves and executes a PowerShell command to download, decode, and deploy NetSupport components. This highlights social engineering via fake updates, obfuscation techniques, decoding malware, and typical deployment strategies. Recommendations include training users on malicious content, restricting risky file types, providing approved software downloads, and using antivirus, NGAV, and EDR to detect threats.

https://www.virustotal.com/gui/collection/alienvault_65c2735a0676e4ec330a9456



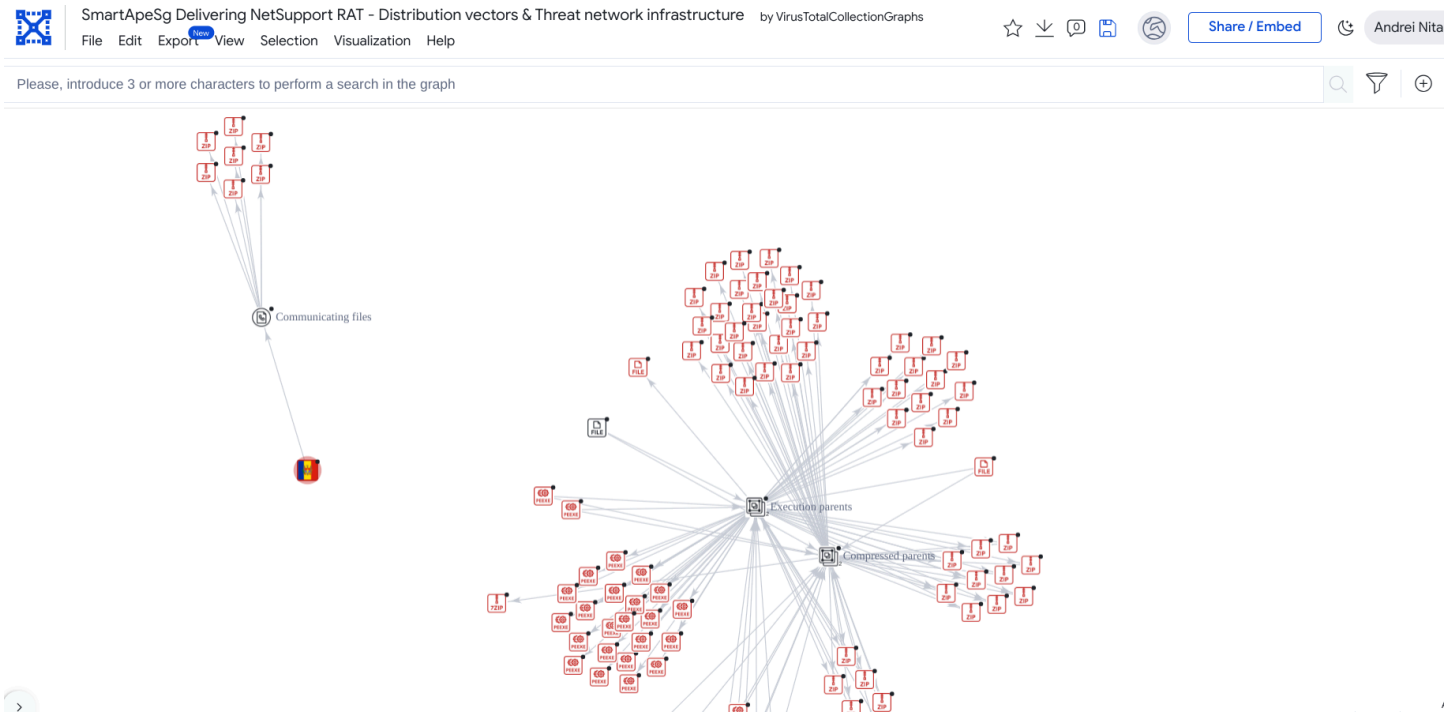


- Classified - Confidential -



- Classified - Confidential -

Checking the arbitrary infection history by graph:



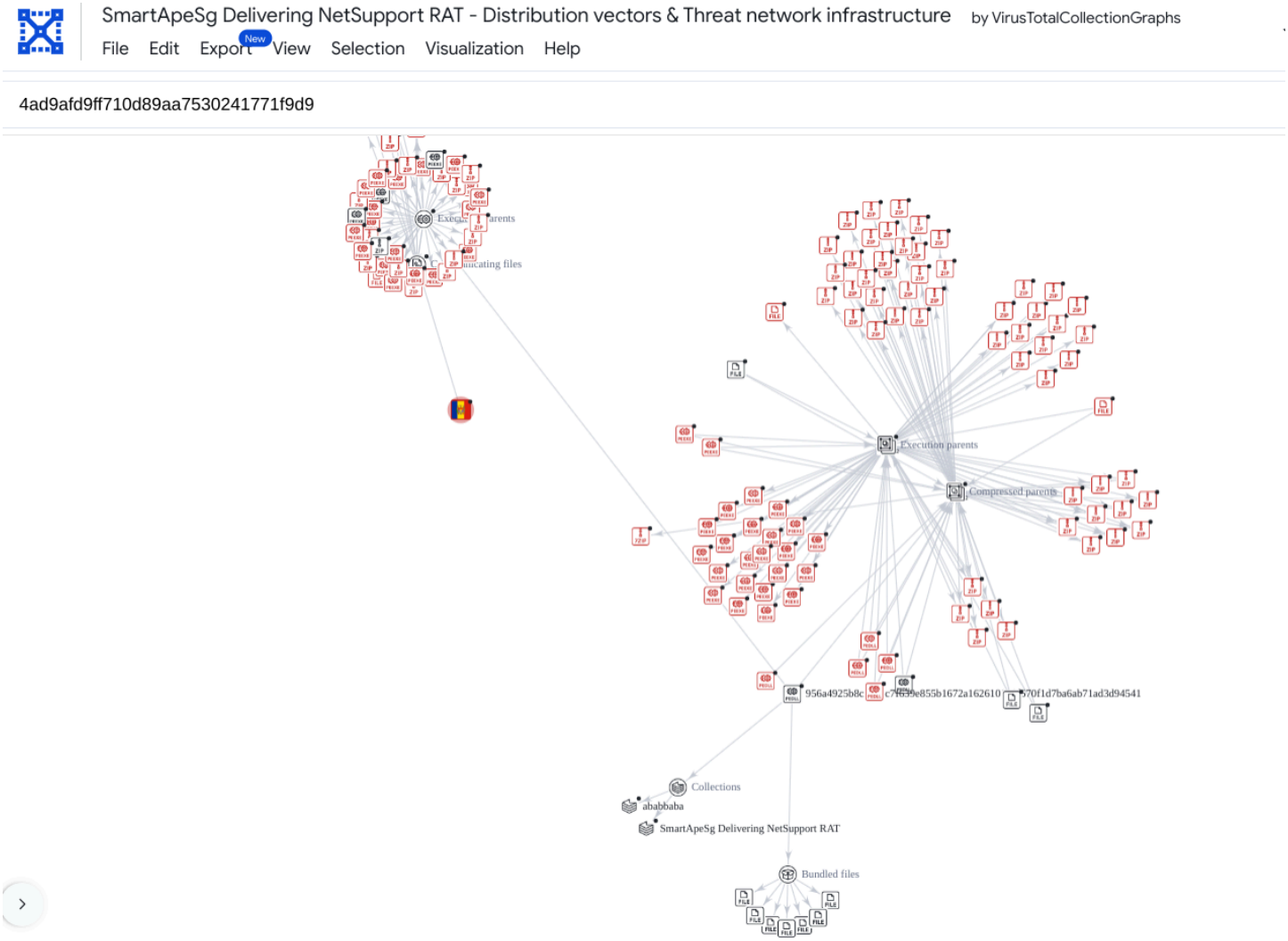
The graph specifically mentions "SmartApeSg Delivering NetSupport RAT - Distribution vectors & Threat network infrastructure" which indicates a possible investigation into the distribution methods and infrastructure of a Remote Access Trojan (RAT) known as NetSupport.

In the graph, there are nodes labeled "Communicating files," "Execution parents," and "Compressed parents," which are likely categories of artifacts found during the analysis. The nodes with "file" icons represent individual files, which could be malicious executables or documents, while nodes with "cloud" icons might represent external communication points, like command and control servers.

The multitude of connections shown suggests a complex infrastructure or a large number of related samples being analyzed for this specific threat. Since the text in the image is too small to read individual file names or IP addresses, it's not possible to provide a detailed analysis without more context or a higher-resolution image.

We're following how this RAT spreads and communicates, which is essential in formulating a response to the threat.

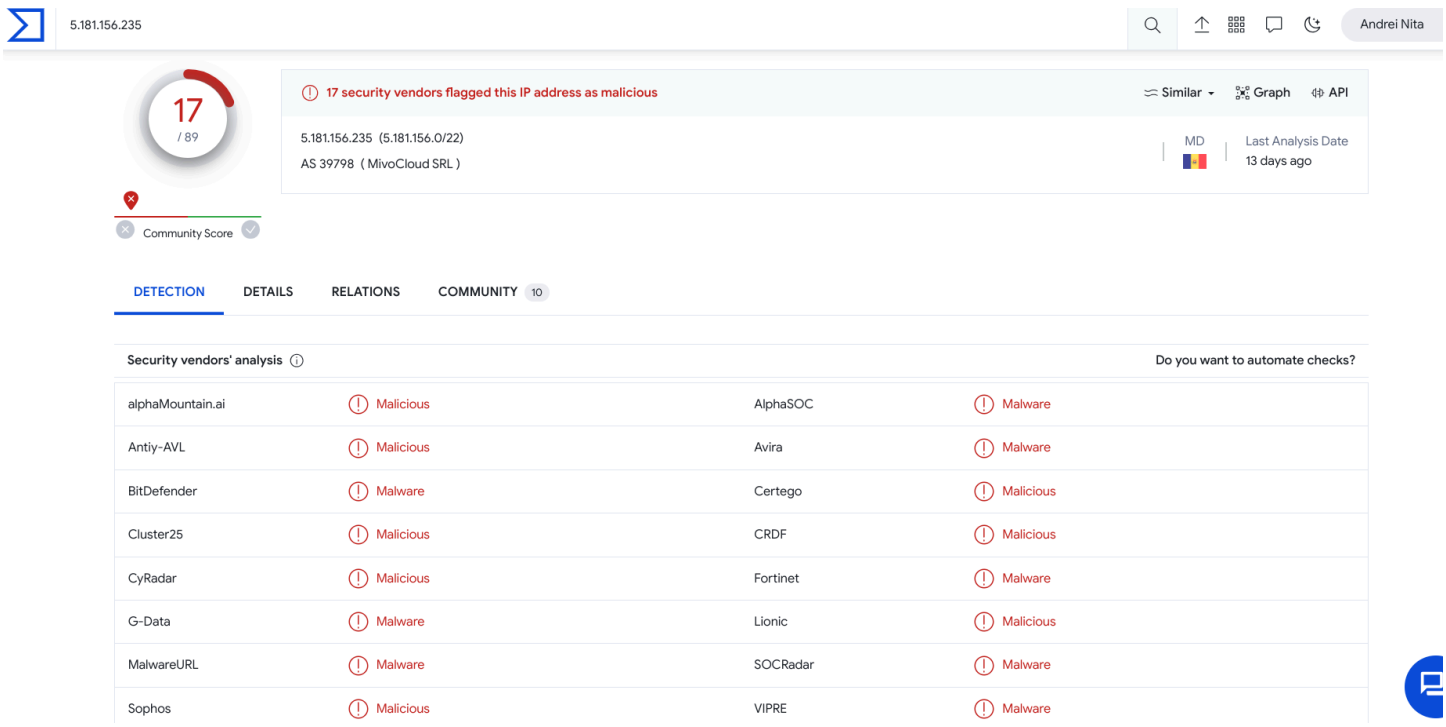
- Classified - Confidential -



Investigating this patterns we've found that other security experts documented such cases:
https://medium.com/walmartglobaltech/smartapesg-4605157a5b80

- Classified - Confidential -

There are multiple IoCs related to IP's from Moldova:



Other Security Threat Researchers noted about these:

https://blogs.vmware.com/security/2023/11/netsupport-rat-the-rat-king-returns.html#:~:text=One%20such%20software%20is%20NetSupport,launching%20point%20for%20subsequent%20attacks.

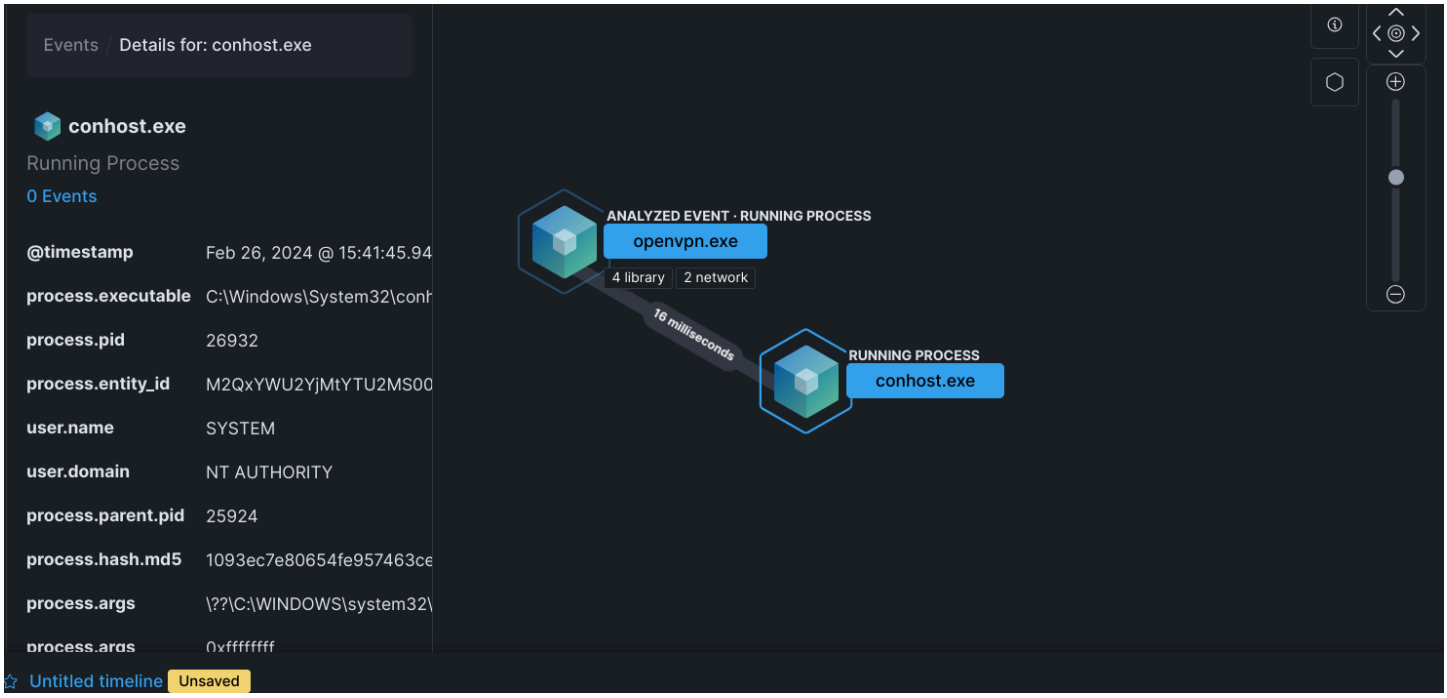
https://www.esentire.com/blog/smartapesg-delivering-netsupport-rat

https://otx.alienvault.com/indicator/ip/5.181.156.235

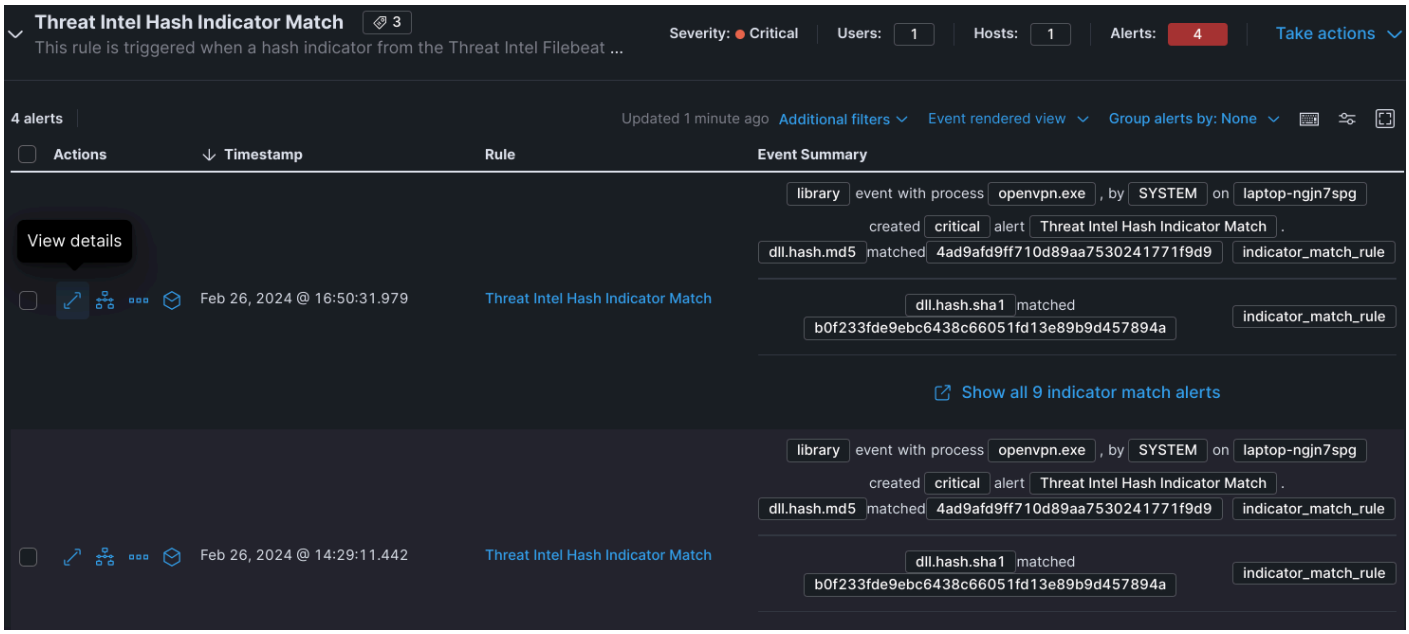
- Classified - Confidential -

- Classified - Confidential -

More relevant information caught by our SIEM never seen elsewhere:



- Classified - Confidential -



- Classified - Confidential -