MITRE ENGENUITY ATT&CK EVALUATION FOR MANAGED SECURITY PROVIDERS

NVISO, a European leader in Cyber Security services, excels in MITRE ENGENUITY ATT&CK evaluations for Managed Security Services.

nviso

→ www.mitre.nviso.eu

Executive Summary

The inaugural MITRE Engenuity ATT&CK Evaluations for Managed Security Services ran in June 2022 and its results have been published today. NVISO excelled in the evaluation, demonstrating services that are at or above the level of traditional titans of the industry.

During this evaluation, NVISO was tested on its ability to detect and report advanced attacks that were executed by the MITRE team. Oilrig, a well-known advanced threat actor, was the emulated threat actor in this inaugural managed services evaluation.

Key Highlights

1. NVISO **successfully detected and reported every step** of the executed campaign
2. The excellent results confirm NVISO's innovative **XDR and automation-first approach**
3. NVISO is a viable option for organizations that prefer a **European-based, world-class MSSP**
4. While not the biggest provider, NVISO delivers **at or above the quality seen** by industry titans

The remaining sections of this document present our results in more detail. Furthermore, we invite readers to visit the MITRE evaluation website, which provides full visibility in raw results.

→ www.mitre-engenuity.org

IMPORTANT

NVISO was not allowed to block anything in the target environment, only report. This reflects our detection and analysis capabilities but does not reflect normal operations – where at several steps during this simulated attack, NVISO would have blocked multiple items and/or would have isolated machines.

STEP 1

User received phishing email with malicious word document

NVISO detected the delivery of the phishing email, analyzed the malicious Word document and identified the suspicious activity on the endpoint.

During normal operations, the phishing email would have been deleted from user's mailbox and the suspicious activity would result in the stopping of the malicious processes.

Malware executes, collects data about the victim's environment and establishes a C2 channel over HTTP

NVISO detected the data collection activity and the C2 channel.

During normal operations, the C2 channel would have been blocked and the process initiating the C2 channel would have been stopped.

STEP 2

Attacker executes various commands on the target to discover permissions, group & account memberships, processes, system information and remote systems.

NVISO detected all commands executed by the adversary and reported the activity as suspicious.

During normal operations, these commands would have triggered an extensive investigation and the activity would have been stopped and/or the target machine would have been isolated.

STEP 3

Attacker downloads an additional tool through the C2 channel which dumps the credentials from the memory of the target and exfiltrates the stolen credentials to the attacker's environment.

NVISO detected the download of the malicious tool and the dumping of the credentials.

During normal operations, the system would now be isolated, and the dumped credentials would be rotated to avoid malicious usage.

STEP 4

Attacker downloads another tool that turned out to be a webshell. This webshell is then copied to a webserver in the Target's environment and activated. The Attacker now has a backdoor on the webserver.

NVISO detected the downloading of the webshell, identified it as a webshell, detected the copying towards the webserver and identified the activation of the webshell on the webserver.

During normal operations, the webshell would be removed from the webserver just before or after the activation and all connections between the target and the webserver would be terminated. This would also trigger an investigation in the suspicious events on the target.

STEP 5

Attacker connects to the webshell on the webserver and executes suspicious reconnaissance commands (e.g. whoami, ifconfig, netstat)

NVISO detected the connection from the Attacker to the webserver through the webshell.

During the evaluation, the webshell was not fully deployed. During normal operations, the webshell would have been deleted during the previous investigation.

STEP 6

Attacker downloads an additional tool through the webshell to the webserver. This tool proceeds to dump the credentials from the memory of the webserver. These stolen credentials are then exfiltrated from the webserver to the attacker's environment.

NVISO detected download of the suspicious tool through the webshell, the execution of the tool and the dumping of the credentials from memory.

During normal operations the webserver would be isolated, and the stolen credentials would have been rotated, in addition to starting a full investigation.

STEP 7

Attacker downloads an additional tool to the Target, which set up a remote port forwarding on the Target. Through this remote port forwarding, the Attacker authenticates to another machine through RDP.

NVISO detected the downloading of the additional tool and discovered its intent through manual analysis. The authentication from the attacker through the remote port forwarding to the other machine through RDP was also detected.

During normal operations, the remote port forwarding would have been detected, this would have triggered an investigation and the webserver might have been isolated.

STEP 8

Attacker connects through the webshell to the webserver and executes various commands.

This results in the downloading of several files by the webshell. The Attacker proceeds with using previously stolen credentials to connect to another machine in the target environment by leveraging a Pass-the-hash attack. Once connected to the remote machine, the Attacker copies over the nt.dat file. Afterwards, an SMB connection is executed to yet another machine, leveraging PSEXEC to remotely execute commands.

NVISO detected the downloading of the several files, the pass-the-hash attack, the copying of the nt.dat file and the execution of command through PSEXEC.

During normal operations, any of this activity would have triggered the blocking of several components and/or the isolation of the systems involved.

STEP 9

Attacker starts the SQL server on one of the systems in the Target environment where they already had access to.

Since this is not malicious behaviour per se, NVISO did not specifically raise any alerts on this step.

STEP 10

Attacker creates a new directory, moves the file nt.dat (identified as a data exfiltration tool) in the new directory and renames the nt.dat file to "VMware.exe". This file reads data from other files in the target environment, prepares the data for exfiltration and finally exfiltrates the data via an Exchange Web Services API to an email address.

NVISO detected the creation of the new directory, the reading of the files and the exfiltration of the files through the EWS API.

During normal operations, NVISO would have contained the file Vmware.exe before it could start exfiltrating data out of the environment.

STEP 11

Attacker cleans up and removes the newly created file "Vmware.exe", the newly created directory and all other files part of the attack.

NVISO detected the deletion of all files and directories.