Evaluation of ForeNova NovaCommand

A test commissioned by ForeNova and performed by AV-TEST

Date of the test report: January 23, 2023 (version 1.00)

Executive Summary

AV-TEST conducted a comprehensive evaluation of ForeNova NovaCommand Network Detection and Response (NDR) in December 2022, with a focus on detecting and responding to malicious activity within an enterprise network. The test consisted of three scenarios, each designed to simulate the actions of advanced persistent threats (APTs):

Scenario 1: Database server breach - extracting data from a database

Scenario 2: Encrypting sensitive data, Ransomware - encrypting data on target host

Scenario 3: Cryptojacking, crypto mining malware - using system resources to mine cryptocurrency

During the test, ForeNova NovaCommand effectively tracked and alerted on the simulated threat actor's actions as they moved through the network and carried out further malicious activities. These results demonstrate the importance of having robust network detection and response capabilities in place to protect against advanced threats.

Overall, NovaCommand provided good coverage of the attacker behavior and helps IT personnel detect advanced attacks. The test results showed that NovaCommand detected the majority of steps in the three test scenarios and reported on the techniques used. In Scenario 1, only the Command and Control and Exfiltration steps were not detected. All other tactics and techniques were well covered. In Scenario 2 all steps were detected. In Scenario 3, some techniques in the Discovery and Lateral Movement stage were missed while techniques were detected in the Initial Access and Command and Control stages. These results indicate that NovaCommand is effective at detecting and reporting on a range of tactics and techniques used by attackers, which can aid IT professionals in identifying and responding to potential threats. The full details of the test setup and the testing scenarios can be found in the following sections of this test report.

Network Detection and Response

Network detection and response (NDR) products are a type of security software designed to monitor network activity for signs of potential threats and take appropriate action when necessary. They are used to detect and respond to cyber attacks, such as advanced persistent threats (APTs), which are highly sophisticated attacks that often target specific organizations or individuals. NDR products are useful because they can help organizations identify and mitigate potential risks to their networks by continuously monitoring for suspicious activity and alerting IT personnel when necessary. They can also help organizations understand the nature and scope of an attack, which can aid in the development of effective response and recovery plans. Additionally, NDR products can provide organizations with valuable insights into the tactics and techniques used by attackers, which can help them strengthen their overall security posture.

Overview of ForeNova NovaCommand

NovaCommand is a Network Detection and Response platform that dramatically augments attack surface visibility enabling improved surveillance of critical assets that cannot be secured with endpoint or other cybersecurity solutions. It is ideal for threat hunters to quickly sift through suspicious activity that could reveal sophisticated and evasive APT actors. Powered by multiple analytics engines including AI/ML algorithms and up-to-the-minute threat intelligence feeds, NovaCommand delivers precise threat detection and automated playbooks to respond with disrupt and deny tactics.

Test Scenarios

Scenario 1: Database server breach

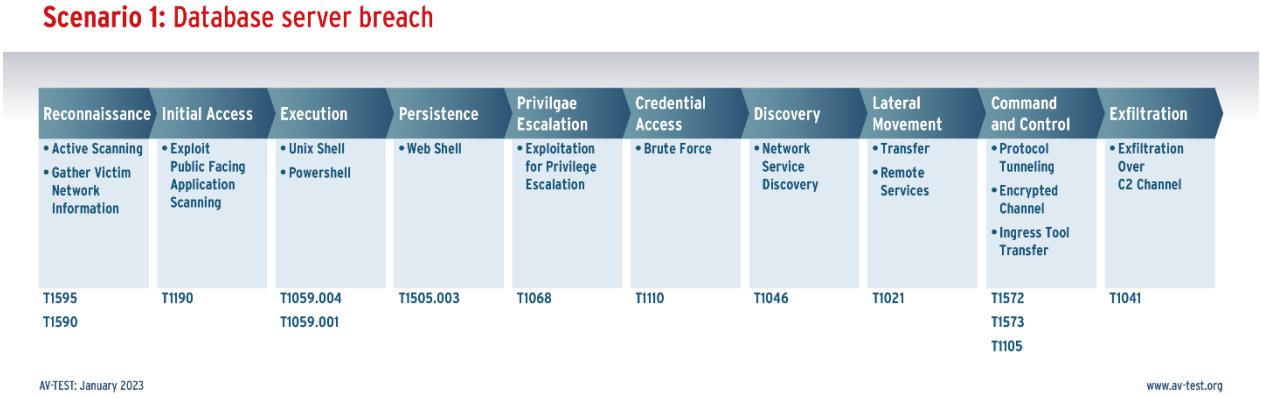
Mission Objective: Extract data from a database

Test Environment:

Machine A: Threat Actor	Machine B: Point of Entry	Machine C: Target Host
Microsoft Windows Server 2019 (Build 17763)	Linux Ubuntu 16.04 LTS	Microsoft Windows Server 2019 (Build 17763)
Python environment, Java environment, vulnerability scan and exploit tools to attack Struts 2	Tomcat 8.5, Java openjdk 1.8.0_292, Apache Struts 2.3.12	Microsoft SQL Server 2016

1. Using the NMap tool to scan a machine (MachineA) for the Tomcat service, and then confirm the presence of a Struts2 vulnerability
2. Running an exploit and confirm access to MachineA
3. Discovering the privileges and network environment of MachineA
4. Setting up a Command and Control (C2) server and starting a listener
5. Downloading and executing a trojan or implant on MachineA using the Struts2 exploit
6. Using the fscan tool to bruteforce another machine (MachineC) and retrieve login credentials
7. Placing a webshell backdoor on MachineA using the Struts2 exploit
8. Accessing the webshell on MachineA and executing the whoami command
9. Transferring a tool called sqltool_amd64_upx and using it to execute a command on MachineC
10. Using sqltool_amd64_upx to download and execute a trojan or implant on MachineC.
11. Upload and execute exploit to get system rights.
12. Create backup for all databases, zip them together, and exfiltrate the archive.

The graph below outlines the tactics and techniques used in this scenario.



Scenario 2: Encrypt sensitive data, Ransomware

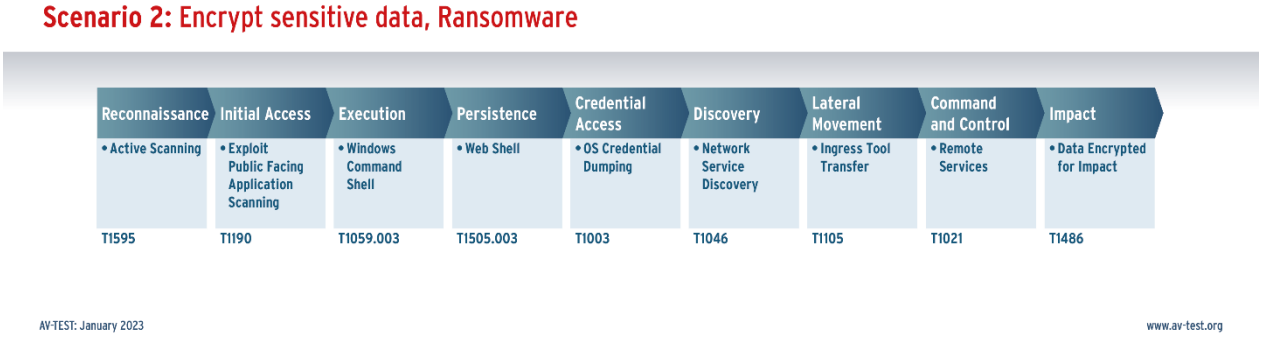
Mission Objective: Encrypt data on target host

Test Environment:

Machine A: Threat Actor	Machine B: Point of Entry	Machine C: Target Host
Kali Linux	Microsoft Windows Server 2019 (Build 17763)	Microsoft Windows Server 2019 (Build 17763)
Webacoo	Java environment, Oracle WebLogic 12.1.3.0 with weak passwords Precondition: The AD server administrator has logged this machine as a member	Active Directory server

1. Using the NMap tool to scan the target computer and detect that it has WebLogic software running on port 7001
2. (Optional) Using Hydra to try to brute force the WebLogic admin panel by guessing different username and password combinations
3. Using the WeBaCoo tool to prepare a shell and Metasploit to exploit a vulnerability in WebLogic to open a meterpreter session
4. Using a Python tool to serve files on port 8000 and transferring those files to the target computer using the Webacoo shell
5. Using various command-line tools to gather information about the target computer's domain and IP address
6. Using a script called pthexec.ps1 to check available credentials on the target computer
7. Transferring ransomware to the target computer
8. Using the pthexec.ps1 script to move and execute the ransomware on another computer.

The graph below outlines the tactics and techniques used in this scenario.



Scenario 3: Cryptojacking, crypto mining malware

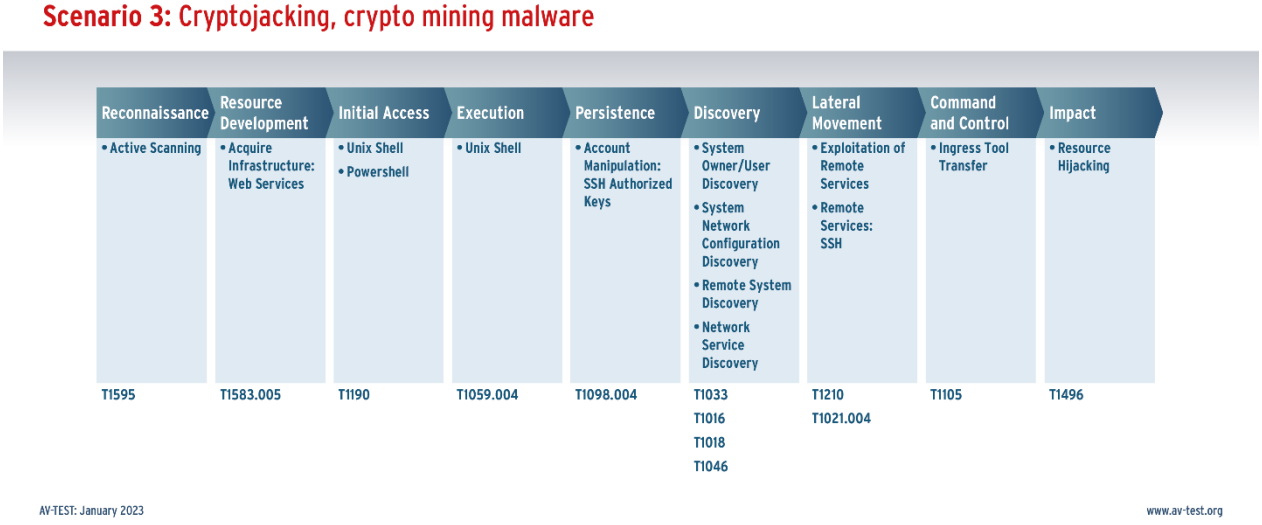
Mission Objective: Use system resources to mine cryptocurrency

Test Environment:

Machine A: Threat Actor	Machine B: Point of Entry	Machine C: Target Host
Kali Linux	Microsoft Windows Server 2019 (Build 17763)	Linux CentOS-7
Webacoo	PHP, MySQL 5.6+, Joomla 3.4.6 web app	Redis 6.2.1 Database

1. Starting a server to allow file downloads using a Python tool
2. Scanning directories on the target webserver using a tool called dirb and finding that it has Joomla software installed
3. Starting a tool called Sliver and using a custom Python script to exploit a vulnerability in Joomla to download and run a trojan/implant on the target webserver
4. Using Sliver to connect to the trojan/implant, download and generate an ssh key pair, and discover information about the target webserver's environment
5. Using a tool called fscan to scan the network and find that another computer, MachineC, has a port open running Redis software
6. Using fscan to exploit unauthorized access to Redis on MachineC and write an ssh public key to the authorized_keys file on that machine
7. Connecting via ssh to MachineC and checking the user's identity
8. Downloading, extracting, and running a cryptocurrency mining tool called XMRig on MachineC.

The graph below outlines the tactics and techniques used in this scenario.



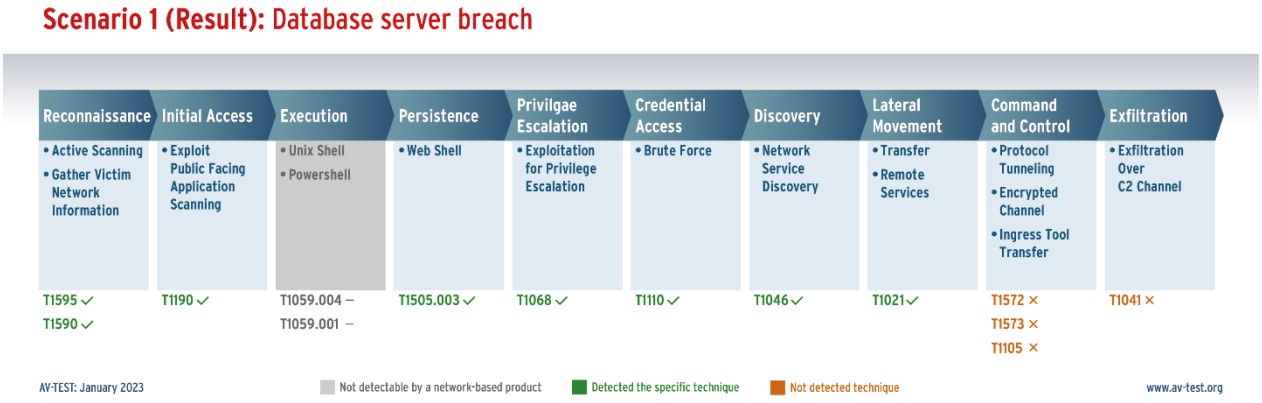
Test Results

The results of the test have been mapped to the MITRE ATT&CK tactics and techniques previously displayed. There are some steps that cannot be detected by a network-based product, so they are not included in the rating. These steps are marked in grey. If the NDR product was able to detect the specific technique, the result for that technique is shown in green. Techniques that were not detected are displayed in orange.

Overall, ForeNova NovaCommand provided good coverage of the attacker behavior and helps IT personnel detect advanced attacks. The test results showed that NovaCommand detected the majority of steps in the three test scenarios and reported on the techniques used. In Scenario 1, only the Command and Control and Exfiltration steps were not detected. All other tactics and techniques were well covered. In Scenario 2, the Discovery step was not detected, but all other steps were detected. In Scenario 3, techniques in the Discovery stage were missed while some techniques were detected in the Initial Access, Lateral Movement, and Command and Control stages. These results indicate that NovaCommand is effective at detecting and reporting on a range of tactics and techniques used by attackers, which can aid IT professionals in identifying and responding to potential threats.

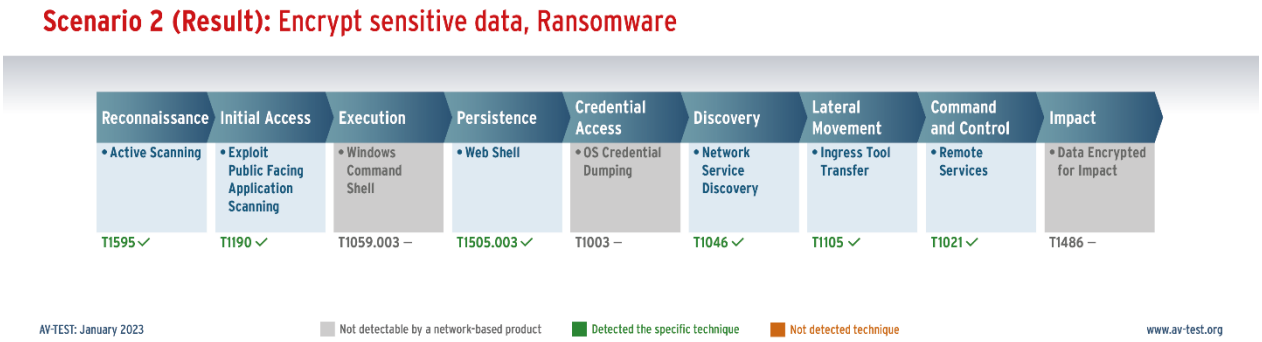
Scenario 1: Database server breach

The following graph illustrates the various stages of the attack and the points at which NovaCommand was able to detect and alert on the malicious actions. The results show that 7 out of 10 tactics were fully covered in this scenario. The Execution step cannot be covered, as it involves only local actions that cannot be monitored by a network detection and response (NDR) product. The Command and Control and Exfiltration steps were not detected, as is often the case with advanced C2 communication tools that create traffic that cannot be realistically detected as malicious. This highlights the importance of detecting the attacker at an earlier stage, which NovaCommand did effectively in this scenario.



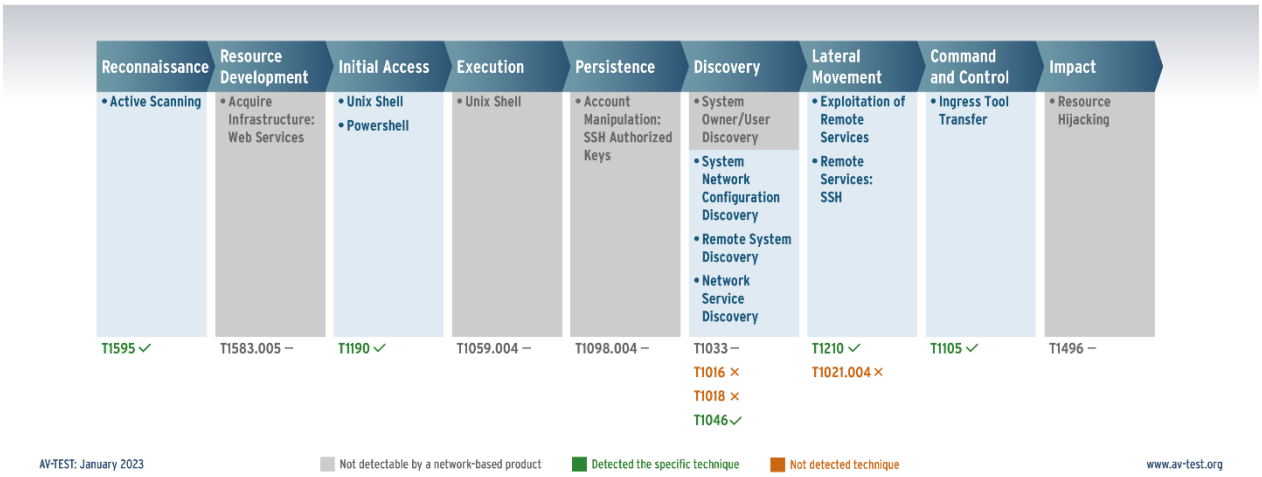
Scenario 2: Encrypt sensitive data, Ransomware

In scenario 2, 9 tactics were covered, with 3 of them (Execution, Credential Access, and Impact/Data Encryption) being local actions that cannot be detected by a network detection and response (NDR) product. Of the remaining tactics, all were successfully detected. This is an excellent result and demonstrates that NovaCommand is able to reliably detect and report tactics used in this scenario. Additionally, detecting an attack at an earlier stage, such as the Discovery phase, can be more challenging for NDR products, as the attackers may not yet have fully established their foothold on the network.



Scenario 3: Cryptojacking, crypto mining malware

In scenario 3, an attacker tried to install crypto mining hardware on a victim machine using 9 tactics, 4 of which were local actions (Resource Development, Execution, Persistence, and Impact) that cannot be detected by a network detection and response (NDR) product. The Reconnaissance, Initial Access and Command & Control tactics were fully covered, and all the techniques used were detected. For the Discovery tactic, 1 technique was local and not relevant for NDR products, while 2 were not detected primarily due to encrypted traffic and one technique, a detection challenge for most NDR technologies. In the Lateral Movement stage, 1 out 2 techniques were detected.



However, despite these missed detections, NovaCommand alerted on all stages except for the local ones, providing opportunities for IT personnel to detect the attack at different stages. This

demonstrates the value of having an NDR product in place, as it can alert on potential threats even if it does not detect every single tactic or technique used by the attacker.

Conclusion

NDR products, or network detection and response products, are designed to monitor network activity for signs of potential threats and take appropriate action when necessary. One such NDR product is ForeNova NovaCommand, which is specifically designed to detect and respond to advanced persistent threats (APTs).

APTs are a significant threat to organizations because they are highly sophisticated and often target specific organizations or individuals. APTs are designed to evade traditional security measures and remain undetected for long periods of time while they gather sensitive information or disrupt operations. This makes them particularly dangerous because they can operate unnoticed for extended periods, potentially causing significant damage before they are detected.

This test, which evaluated ForeNova NovaCommand against three APT scenarios, provides insight into the product's capabilities and how well it can detect and report on various tactics and techniques used by attackers. By simulating real-world APT threats, the test helps to determine how effective NovaCommand is at detecting and responding to these types of threats. This information is valuable for IT professionals who are responsible for protecting their organization from cyber attacks, as it helps them make informed decisions about which security tools and practices to implement.

Overall, the test results showed that ForeNova NovaCommand was effective at detecting and reporting on a range of tactics and techniques used by attackers in the three test scenarios. In Scenario 1, NovaCommand detected the majority of steps and techniques, with only the Command and Control and Exfiltration steps not being detected. In Scenario 2, all steps were detected. In Scenario 3, some techniques in the Discovery and Lateral Movement stage were missed while all techniques were detected in the Initial Access, and Command and Control stages. These results suggest that NovaCommand is a useful tool for detecting and responding to APT threats, and can aid IT professionals in identifying and mitigating potential risks to their organization.