WHITE PAPER

An Analysis of Attacker Activity through NDR, EDR, and NGFW Data

Executive Summary

Intrusions are complex to detect, as attackers continuously evolve their techniques to avoid exposure, progressing through multiple attack stages to remain undetected for an extended dwell time. Once they have successfully breached an organization, threat actors often use common practices, such as multi-hop proxies, combining malicious activity with legitimate network traffic, ingress tool transfers, and forced authentication to advance their efforts. These clever activities make it challenging for security teams to discover and distinguish between genuine and malicious activity.

To combat this challenge, security teams often use telemetry and observations from multiple security tools to gain a complete picture of the events happening within their networks. Security teams need unified visibility across the environment, correlating and analyzing multiple data sources to gain more context and help them decide on the right response and mitigation strategies.

This white paper takes a closer look at the valuable insights security teams can gain when they correlate network detection and response (NDR), endpoint detection and response (EDR), and next-generation firewall (NGFW) data across the network. These multi-dimensional analytical and response capabilities help teams detect any evidence of malicious behavior early in the attack life cycle, ultimately accelerating analysis and enabling analysts to respond to issues quickly.

The data provided in this report is the result of the FortiGuard Labs Applied Threat Research (ATR) team's analysis of more than 11 trillion NDR-originated network events in 2023, which offer insights into the most observed MITRE ATT&CK tactics and techniques attackers used in in that same timeframe to carry out their operations. Any source reporting on "top" ATT&CK techniques is inherently dependent on the lens through which they're being viewed. This report reveals network-based artifacts that provided FortiNDR Cloud with observations or detections of attacker activity.

The Most Common MITRE ATT&CK Tactics Observed in 2023

FortiNDR Cloud network sensors perform deep packet inspection of all observed network traffic and extract key protocol metadata for processing. This metadata is organized into records called "events." Subsequently, events are then correlated into observations. Detections are triggered when events or observations match specific criteria.

In 2023, FortiNDR Cloud analyzed 11 trillion network events from across Fortinet's global customer base. The analysis showed that out of more than 463,000 detections observed in 2023, customers identified less than 1% as false positives.

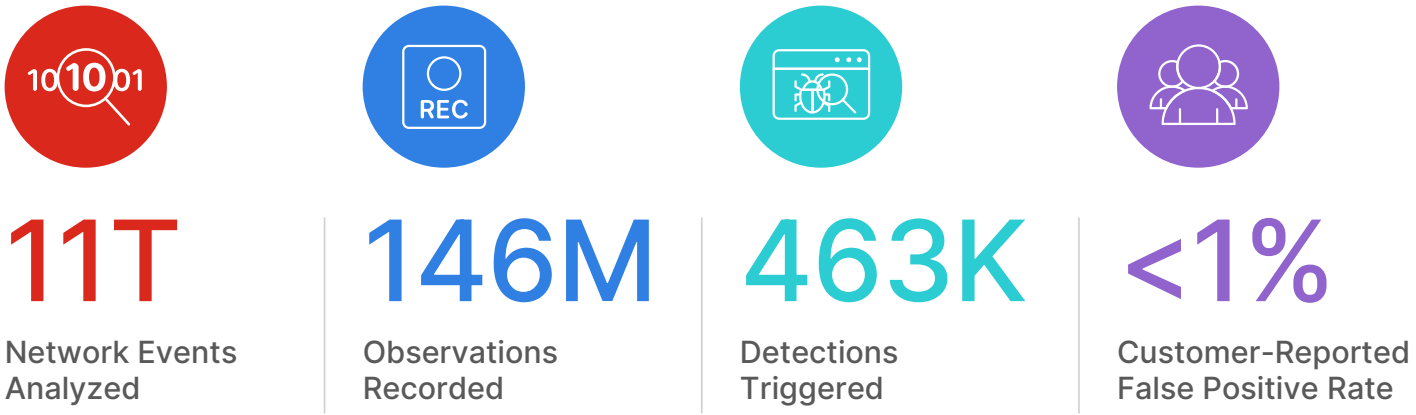

Figure 1: Less than 1% of FortiNDR Cloud detections were labeled as false positives in 2023

FortiNDR Cloud detections are automatically mapped to the MITRE ATT&CK framework. Below is a look at the most common detections observed across the data set:

Figure 2: FortiNDR Cloud detections are mapped to MITRE ATT&CK tactics

Our analysis uncovered high volumes of command and control (C2) (44%) and execution activity (38%). Because C2 techniques are network-based, network data provides the greatest opportunity to detect such techniques. However, the techniques used for the Impact and Credential Access tactics do not provide significant artifacts detectable through network data; hence, there are negligible detections.

Regarding execution activity, FortiNDR Cloud detects malicious portable executable (PE) file activity and is mapped to the MITRE ATT&CK technique of T1204: User Execution. These detections are triggered based on hash values produced by FortiNDR Cloud when a user downloads the file. Behind the scenes, FortiNDR Cloud submits the hashes to the FortiGuard Indicators of Compromise (IOC) service, which determines the detection's malicious nature and confidence level based on the data received.

The Most Common MITRE ATT&CK Techniques Observed in 2023

The chart below ranks the most observed MITRE ATT&CK techniques under each tactic. The percentages correspond to the proportion of detections by technique within each tactic. Several MITRE ATT&CK techniques are mapped to multiple tactics. For that reason, each detection is applied to the most relevant tactic based on the context in which it was observed.

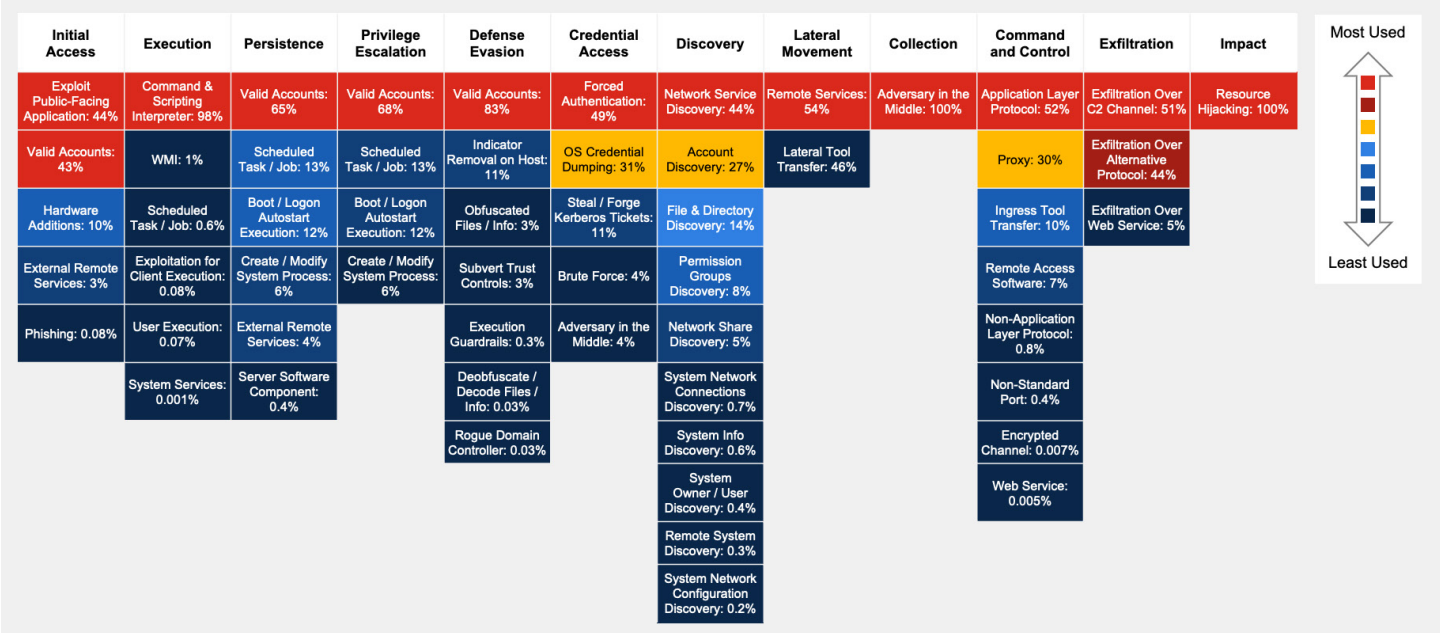

Figure 3: The MITRE ATT&CK heatmap shows the ATT&CK techniques observed through FortiNDR Cloud

Based on our analysis of the detections spotted across the entire MITRE ATT&CK framework, we observed the following trends:

- **Widespread use of C2 techniques:** Attackers continue to use a variety of C2 techniques, such as Domain Name System (DNS) tunneling, long DNS queries, and web shells. Without consistent C2, adversaries cannot interact with their implants or access a victim's environment to achieve their objectives. Building robust C2 is critical in determining an adversary's success during an intrusion. When successfully utilized, C2 provides an adversary with consistent access into the host or environment. It obscures the initial ingress point and allows the adversary to continue their mission, even if defenders secure the original exploit that allowed initial access.

  Given the criticality of C2 in enabling an adversary to effectively pursue their objectives, this provides defenders with consistent opportunities for detection. Network metadata is an immutable "source of truth" of any network activity, including C2, as attackers cannot manipulate or change network packets. Blocking observed C2 communications or destroying an attacker's C2 infrastructure often stops a cyberattack in its tracks. Addressing these common tactics, techniques, and procedures can significantly reduce the danger presented by C2 infrastructure.
- **Continued use of commodity remote access trojan (RAT) malware:** RATs, such as Lokibot and IcedID banking Trojan, continue to trend in detection activity. Loki, an open-source remote access tool, provides attackers with features like file transfer over HTTP or SFTP, launching a local browser, taking screenshots, and running keyloggers. Loki is often used as a post-exploitation tool to advance malicious activity. The FortiGuard ATR team considers Loki to be high severity given that it's commonly used for lateral movement following a compromise of a single host. IcedID banking Trojan, on the other hand, hooks into users' browser sessions and can take screenshots to steal credentials for financial institutions. IcedID is also used to facilitate Access-as-a-Service offerings where access to compromised networks is sold to additional malicious actors. The FortiGuard ATR team considers IcedID high severity due to granting malicious actors high levels of access to an organization's environment and sensitive data. These tools are often used as a precursor to conduct further C2 activity.
- **Valid accounts are increasingly used for defense evasion:** The Valid Accounts technique (T1078) in the Defense Evasion phase of MITRE ATT&CK is still a relevant indicator of potential threat activity. This technique detects how adversaries obtain and abuse credentials of existing accounts to execute Initial Access, Persistence, Privilege Escalation, or Defense Evasion. One such example is how FortiNDR Cloud detects a customer's internal Remote Desktop Protocol (RDP) servers being accessed by individuals outside the corporate network. This is generally an undesired configuration, as sensitive information may be exposed, leaving the business open to attack. Internet-facing services can also be subject to regular brute-force attempts by scanners and compromised devices. Another such detection associated with Valid Accounts is the Domain Accounts technique (T1078.002), which looks at domain controllers authenticating with a previously unseen NT LAN Manager (NTLM) username. This type of activity may indicate that a threat actor has gained access to a domain controller.
- **PowerShell is often used for malicious activity:** Our analysis shows that attackers continue to use PowerShell for malicious activity. PowerShell is a popular scripting tool that is used as a staging tool for malware and for developing more robust toolkits, such as the Empire post-exploitation tools. While commonly used in systems administration, malware authors use PowerShell scripts extensively for post-exploitation actions. FortiNDR Cloud covers various detection techniques using PowerShell in the following categories: Ingress Tool Transfer (T1105) and PowerShell (T1059.001).
- **Early intrusion discovery techniques are prevalent:** Several suspicious Active Directory and Lightweight Directory Access Protocol (LDAP) enumerations were detected, including enumeration of users, groups, domain trusts, and others. Threat actors can use LDAP or Distributed Computing Environment and Remote Procedure Calls to enumerate all groups, administrators, users, computers, domain controllers, and domain trusts within a domain. After compromising a network, adversaries may query Active Directory to better understand an organization's network layout and assets. Detecting adversary activity during discovery allows for intrusions to be isolated before adversaries can properly gain a foothold in the network.

A Real-World Example of Unified Network and Endpoint Detections in Action: The Rhysida Ransomware Intrusion

When comparing our findings in this report with a real-world attack scenario, such as the Rhysida ransomware intrusion, we can examine specific attacker techniques and share valuable insights into the tactics used by today's ransomware groups, giving security teams tips for protecting against these malicious activities.

The Rhysida group was first identified in May 2023 when they claimed their first victim. This group deploys a ransomware variant known as Rhysida and offers it as Ransomware-as-a-Service to fellow threat actors via the dark web. Since its arrival, the group has listed at least 50 victims across the world on its website. The group made headlines when it was reported that they had successfully deployed their ransomware in systems associated with the Chilean Army.

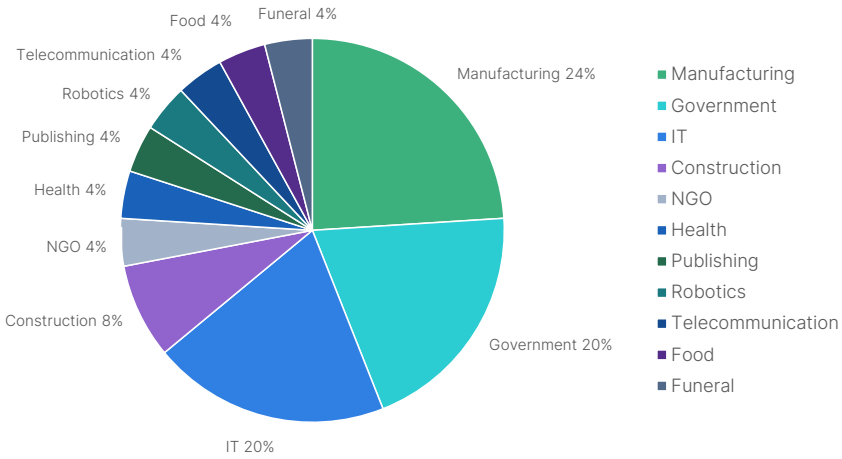

Figure 4: Rhysida victims by industry

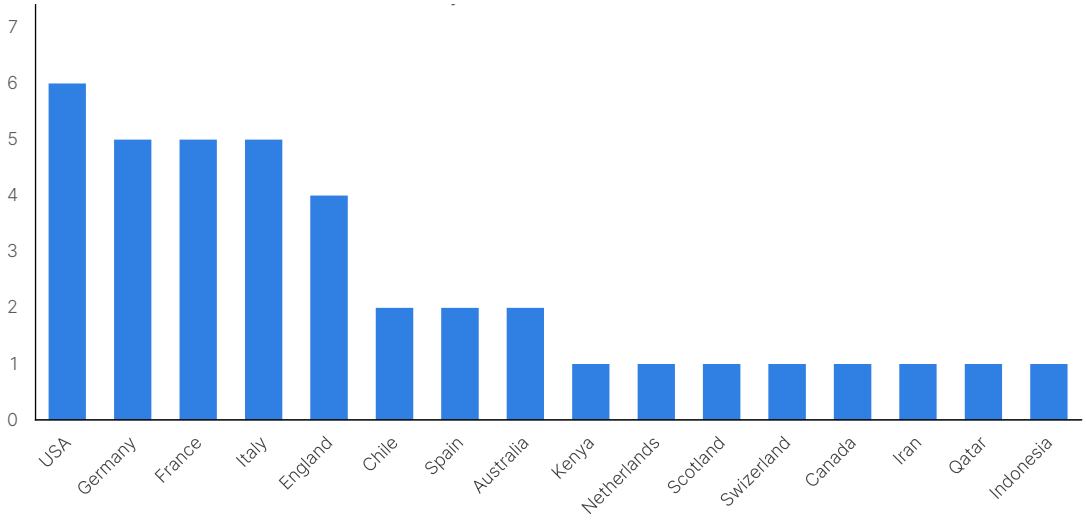

Figure 5: Rhysida victims by location

Rhysida's list of victims includes organizations from various industries, including education and manufacturing. Victims of Rhysida intrusions are geographically diverse, with the United States, France, Germany, England, and Italy being the top five countries in terms of the number of victims compromised.

The diagram below details one intrusion that resulted in the deployment of the Rhysida ransomware. The FortiGuard Managed Detection and Response team detected this intrusion using FortiEDR, which was later investigated by the FortiGuard Incident Response team.

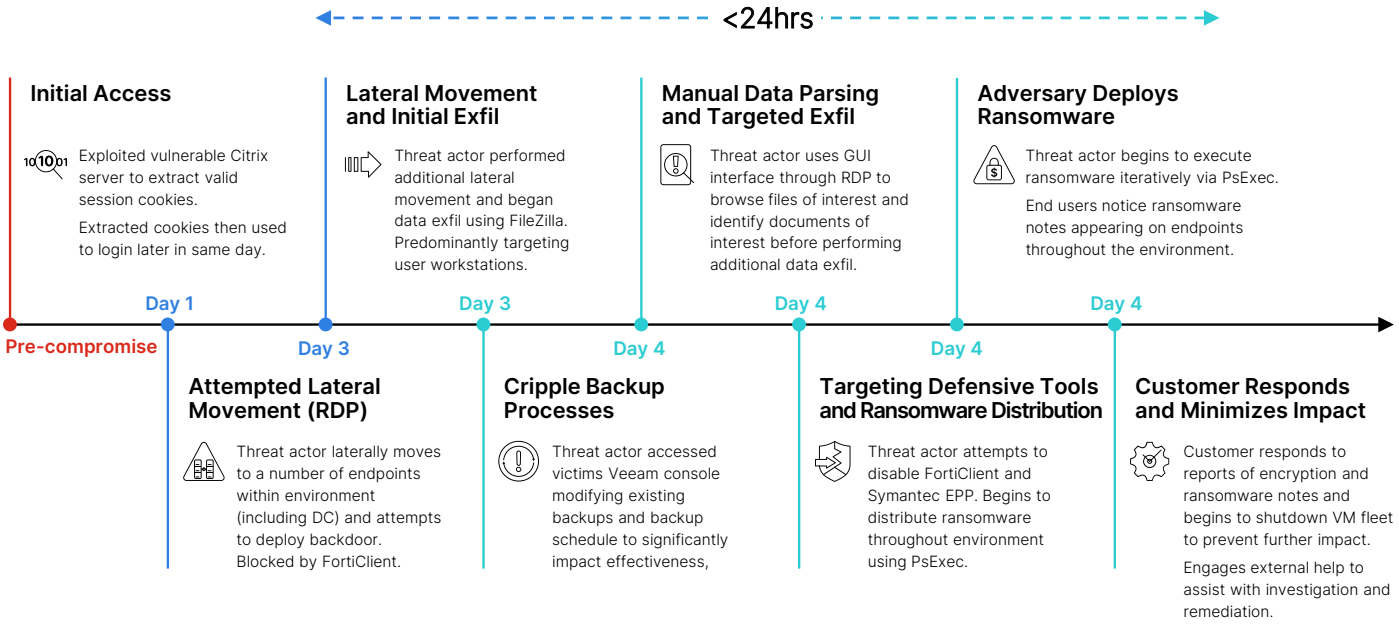

Figure 6: The attack timeline of the Rhysida intrusion

Fortinet investigation of a Rhysida ransomware incident

Rhysida group has been observed using legitimate software such as PowerShell to perform discovery functions and find information about users and systems within the network. We've observed attackers using PSExec to schedule tasks and change registry keys to maintain persistence, leveraging AnyDesk for remote connections and relying on WinSCP for file transfers. The group also attempted to exfiltrate data from various systems using a publicly available cloud storage platform.

We have observed Rhysida attack instances across different victims, yet these attacks typically follow a similar pattern:

1. Rhysida operators acquire credentials and access environments through victim VPN devices.
2. Attackers perform lateral movement through RDP to key servers such as domain controllers.
3. Operators then perform credential dumping using basic methods, such as taskmanager.exe or procdump.
4. Attackers deploy a SOCKS-based PowerShell backdoor as secondary access.
5. Threat actors conduct data exfiltration after manual file appraisal through RDP or AnyDesk.
6. Operators deploy ransomware to ESXi hypervisors first to maximize impact.

Tips for Detecting and Combating Ransomware Attacks

Where the above demonstrates a case study of the techniques employed by Rhysida ransomware operators, there are significant commonalities across various ransomware operators that analysts can use to hunt for and prevent ransomware attacks.

Below are actionable recommendations that security teams can follow to combat ransomware attacks based on these commonalities. The attack techniques outlined here refer to previously observed and mentioned in the report, all mapped to the MITRE ATT&CK framework.

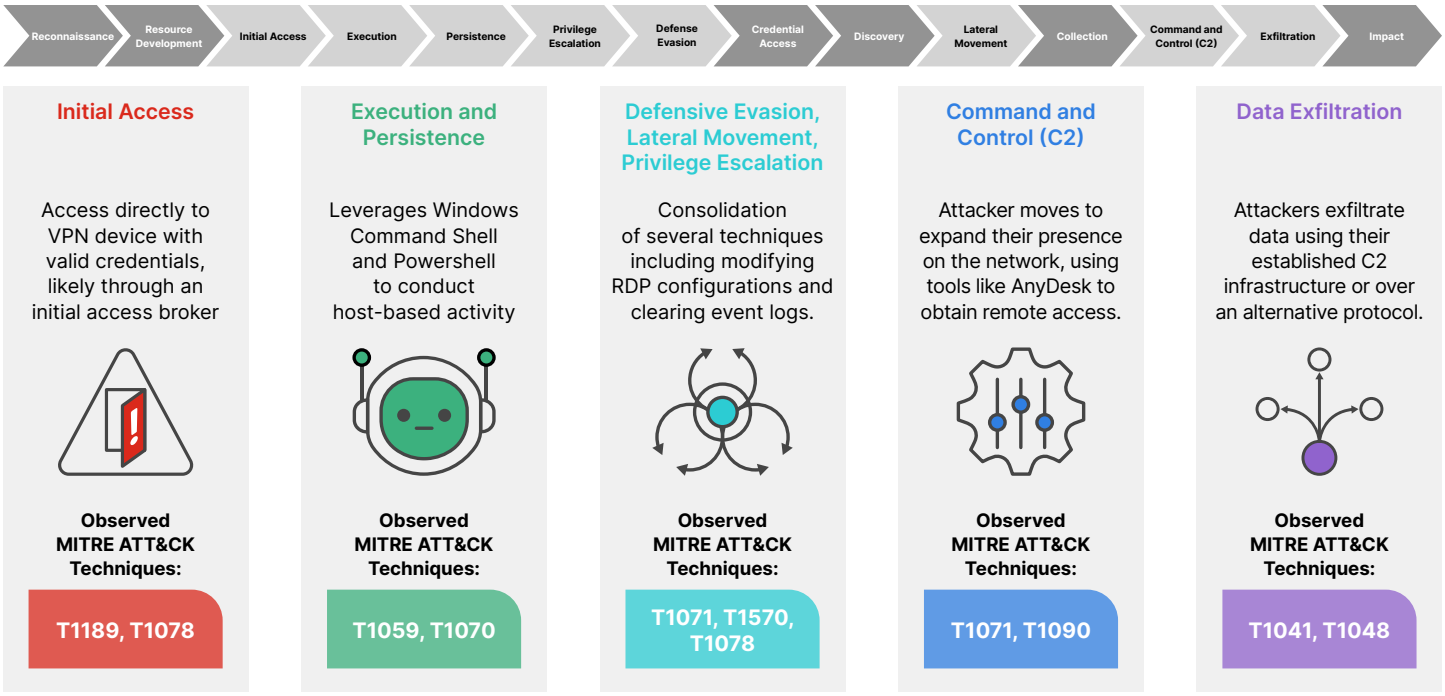

Figure 7: Observed ransomware techniques across the MITRE ATT&CK framework

The diagram above represents a ransomware attack where the attacker leverages common ransomware tactics and techniques outlined in this report. Each MITRE ATT&CK tactic presents security teams with unique detection and mitigation opportunities, which we outline below.

MITRE ATT&CK Techniques Identified:

T1189, T1078 | T1059, T1070 | T1071, T1570, T1078 | T1071, T1090 | T1041, T1048

Initial Access

Attackers often use valid credentials or exploit a public-facing application to access network resources. The ransomware group may have obtained access through an initial access broker.

Threat hunting tip: Despite using valid credentials, security analysts should leverage NDR-based and behavioral analytics to determine how initial access occurred by reviewing historical data to look for anomalous web traffic (PE downloads, ISO, and ZIP files) that indicate unusual user activity.

Mitigation strategy: Enable multi-factor authentication (MFA), establish a cybersecurity awareness program for employees to prevent phishing attacks, and regularly patch your vulnerabilities. Establish governance that limits access to sensitive systems requiring administrator permissions.

MITRE ATT&CK Techniques Identified:

T1189, T1078 | T1059, T1070 | T1071, T1570, T1078 | T1071, T1090 | T1041, T1048

Execution and Persistence

Once the attacker gains access to an endpoint, they will conduct various host-based activities, such as discovery and defense evasion, allowing them to establish persistence.

Ransomware perpetrators may leverage Windows Command Shell and PowerShell, as shown in the image below. In this instance, the ransomware utilizes a native API to perform actions like querying registry keys and modifying registry values. During system startup, a scheduled task named “Rhsd” executes the ransomware payload, ensuring the malicious code is activated with each system startup. Also, similar behavior was observed during the analysis of SystemBC, which is a variety of proxy malware.

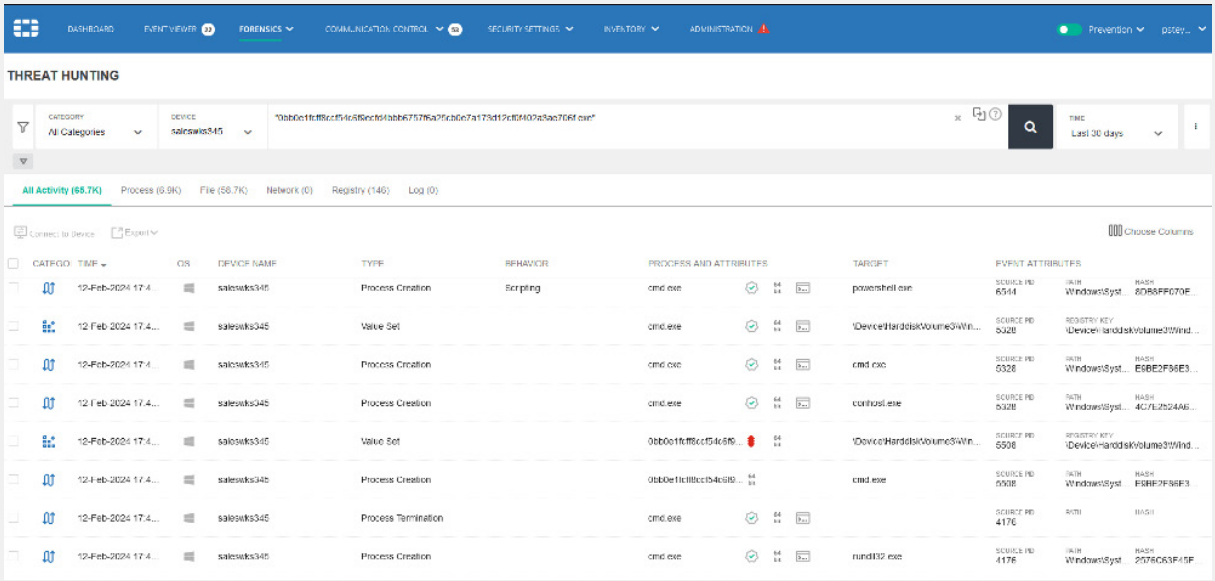

Figure 8: FortiEDR analyzes Rhysida ransomware

Threat hunting tip: Security analysts should leverage EDR-based detections to determine when malicious executables were installed and deployed and block malware installation. They should review historical NDR data to look for anomalous web traffic associated with these executables.

Mitigation strategy: EDR detections should be shared and correlated with telemetry from other integrated response tools to streamline the response process, ensuring the attacker has not expanded their presence to other endpoints.

MITRE ATT&CK Techniques Identified:

T1189, T1078 | T1059, T1070 | T1071, T1570, T1078 | T1071, T1090 | T1041, T1048

Defense Evasion, Lateral Movement, Privilege Escalation

After establishing and maintaining persistence, the attacker moves to evade detection and expand their presence on the network, moving laterally across the environment or escalating privileges. Ransomware groups leverage PowerShell scripts for multiple purposes. The script may terminate processes related to antivirus services, modify RDP configurations, delete shadow copies, and leverage malicious executables to clear event logs.

We've observed ransomware groups using PsExec to execute PowerShell execution scripts. After that, the ransomware is copied to the target system using valid user credentials.

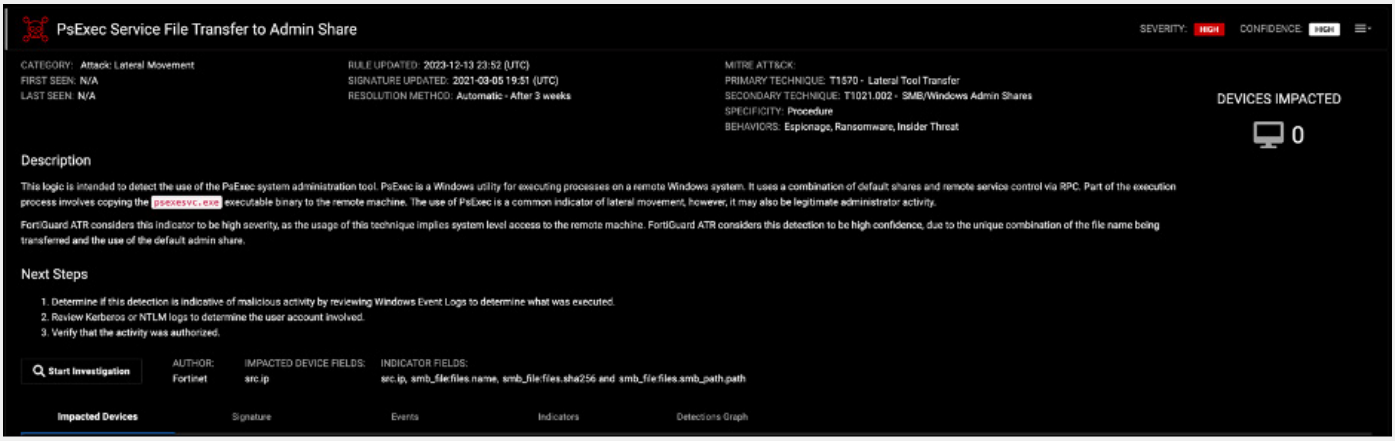

Figure 9: FortiNDR detects PSExec activity

Threat hunting tip: Leverage EDR to expand the scope of the hunt to see if any additional hosts may have interacted with suspicious websites or downloaded suspicious files. With NDR technology, the analyst can search for these downloads on endpoints that may not have an EDR agent installed, providing comprehensive visibility into any endpoints connected to the network.

Mitigation strategy: Leverage NDR to detect anomalous and malicious network activities. security operations teams should proactively hunt for threats using these detections.

MITRE ATT&CK Techniques Identified:

T1189, T1078 | T1059, T1070 | T1071, T1570, T1078 | **T1071, T1090** | T1041, T1048

Command and Control

After evading detection, the attacker often moves to expand their presence on the network, establishing their C2 infrastructure. Ransomware groups may use commodity backdoors like PortStarter and SystemBC and leverage legitimate remote desktop application tools, such as AnyDesk and TeamViewer to obtain remote access.

Threat hunting tip: Leverage EDR to expand the scope of the hunt to see if any additional hosts may have interacted with suspicious websites or downloaded suspicious files. With NDR, the analyst can search for these downloads on endpoints that may not have an EDR agent installed, providing you with comprehensive visibility across all endpoints connected to your network.

Mitigation strategy: Block all communications with C2 infrastructure or established botnets using NGFW capabilities. Prior to blocking known C2 communications, analysts should understand the full scope of the attack by leveraging EDR and NDR to monitor C2 traffic, ensuring all attack activity is recorded and blocked accordingly.

MITRE ATT&CK Techniques Identified:

T1189, T1078 | T1059, T1070 | T1071, T1570, T1078 | T1071, T1090 | **T1041, T1048**

Data Exfiltration

Once the attacker has successfully evaded detection, established their C2 infrastructure, and identified and collected valuable data, they will exfiltrate this data using their established C2 infrastructure or over an alternative protocol.

Ransomware groups will employ various methods for data exfiltration, including WinSCP, 7zip, MegaSync, and, in some cases, PowerShell data exfiltration scripts.

Threat hunting tip: Monitor network protocols and existing C2 channels for anomalous network traffic. These protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main C2 channel. This can also include web services such as cloud services. The attacker's existing C2 infrastructure can also be used for data exfiltration. Analysts should leverage NDR and EDR tools to monitor and detect this traffic.

Mitigation strategy: Block or prevent large outbound data transfers to lower the reputation of virtual private server providers or file-sharing services. Leverage data loss prevention services from a NGFW to assist in monitoring the organization's data.

Conclusion

Given the cost and effort required to find novel and effective exploitation methods, threat actors need to establish and maintain persistence in almost any attack scenario. Leveraging the additional visibility and capabilities provided by the combination of NDR, EDR, and NGFW solutions, security teams are better able to detect intrusions early and help level the playing field against ever-advancing adversaries.

Our research indicates that best practices, such as regular vulnerability patching, implementing MFA, deploying EDR technology, continually monitoring network assets using an NDR solution, and employing a robust NGFW can go a long way in preventing or stopping these attacks before attackers can complete their mission.

Deploying a unified detection and response architecture provides analysts with an end-to-end view of an attacker's actions, accelerating investigation times and providing full attack visibility while reducing alert triage times.

May 10, 2024 6:29 PM

2614106-0-0-EN