

# Security Copilot Promptbook: Threat Actor Profile

---

 [applied-gai-in-security.ghost.io/security-copilot-promptbook-threat-actor-profile/](https://applied-gai-in-security.ghost.io/security-copilot-promptbook-threat-actor-profile/)

January 3, 2024

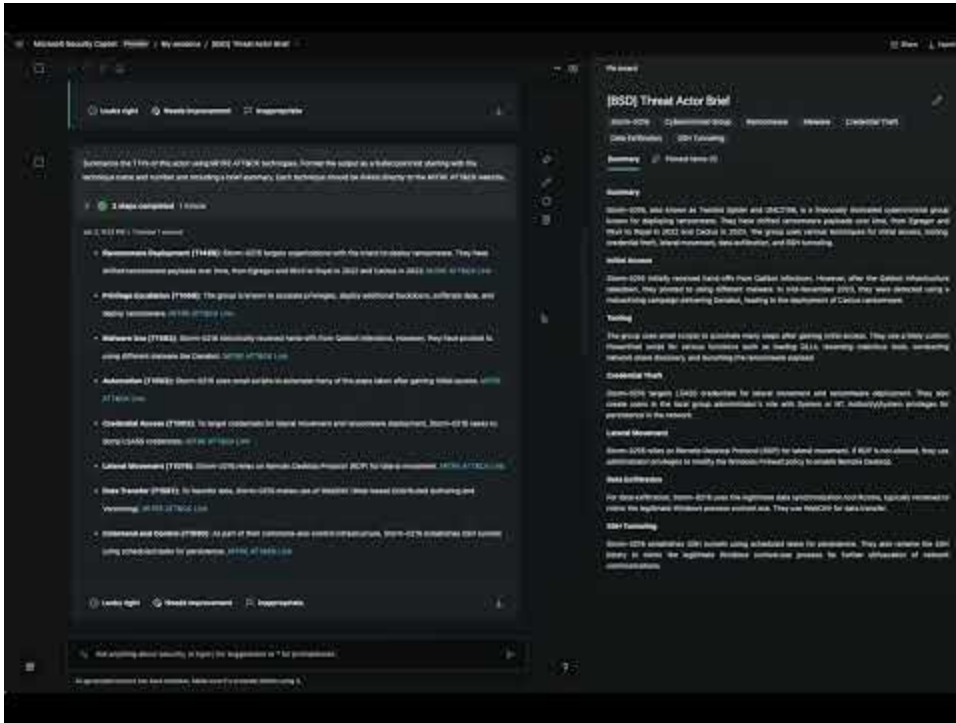
Most attacks, whether complex or simple, motivated by different reasons, typically share one common element: a person controlling the keyboard. While automation can assist in the initial stages of a compromise, the execution of objectives generally involves another individual at a workstation, much like yourself. Humans, being habitual, often struggle to completely conceal their digital traces, no matter how cautious they are. These digital breadcrumbs are what security researchers track to attribute attacks and gain insight into their adversaries. By comprehending the tactics, techniques, and procedures (TTPs) used, defenders can gain an advantage in staying ahead.

Threat naming is a core part of the security industry and broader adversary understanding. Public and private sectors organizations use the insights and information at their disposal to help form profiles of who is or might target their business. What used to be reserved mostly within the government is now very mainstream and part of day-to-day security operations. This explosion of information about threat actors, their tools and the vulnerabilities they exploit can be difficult to keep up with and organize. Between different actor names to complex campaign tracking, organizations can struggle to understand which threat actors matter to them and how to best operationalize the data.

In this post, I will demonstrate leveraging generative AI to go from threat actor name, all the way to a fleshed out profile within a matter of minutes using Security Copilot and the Threat Actor Profile promptbook. The example actor we will use is Storm-0216, a reference back to the [previous promptbook on automating a vulnerability impact assessment](#) posting. All the threat intelligence information is being sourced from Microsoft Defender Threat Intelligence which is included with Security Copilot.

## Promptbook Demonstration

---



Watch Video At:

<https://youtu.be/oAT6pzcEwL8>

For those who prefer to see more of a live demonstration, I put together a brief video explaining the basic controls within Security Copilot and myself walking through the Promptbook that's been created.

## Prompt Walkthrough

Give me a profile summary of Storm-0216. Include an executive summary at the start.

>  3 steps completed 30 seconds

Jan 2, 3:14 PM | 32 seconds

## Executive Summary

Storm-0216 is a financially motivated cybercriminal group known for targeting organizations with the ultimate intent to deploy ransomware. They have been observed working with the actors behind the Qakbot banking trojan to load a backdoor, commonly Cobalt Strike. The group is known to escalate privileges, deploy additional backdoors, exfiltrate data, and deploy ransomware. They have shifted ransomware payloads over time, from Egregor and REvil to Royal in 2022 and Cactus in 2023. Storm-0216 is also tracked by other security researchers as Twisted Spider and UNC2198.

## Detailed Profile

Storm-0216 has been active since 2020 and has shifted through a number of popular ransomware payloads including Egregor, Maze, REvil, Conti, Hive, Black Basta, Royal, and Cactus.

For initial access, Storm-0216 historically received hand-offs from Qakbot infections. However, in mid-November 2023, Microsoft Threat Intelligence detected a malicious advertising campaign delivering Danabot, a commodity information stealer tracked as Storm-1044. These Danabot infections have led to Storm-0216 hands-on-keyboard activity and deployment of Cactus ransomware.

Storm-0216 uses small scripts to automate many of the steps taken after gaining initial access. They also incorporate Cobalt Strike, the open-source Impacket tool, and the DWAgent legitimate remote management tool.

To target credentials for lateral movement, Storm-0216 seeks to dump LSASS credentials, often by leveraging the living-on-the-land binarytaskmgr.exe (Task Manager). With sufficient privileges, Storm-0216 also creates users in the local group administrator's role with System or NT Authority\System privileges.

Storm-0216 relies on Remote Desktop Protocol (RDP) for lateral movement. If RDP is not allowed in the environment, Storm-0216 has used administrator privileges to modify the Windows Firewall policy to enable Remote Desktop.

For data exfiltration, Storm-0216 uses the legitimate data synchronization tool Rclone, typically renamed to mimic the legitimate Windows process svchost.exe.

As part of their command-and-control infrastructure, Storm-0216 establishes SSH tunnels using scheduled tasks for persistence. Identified tunneling tools used by Storm-0216 include the open-source GO Simple Tunnel (GOST) and chisel.

Summarize the threat actor

The first step within this Promptbook is to ask for a profile of the named threat I want to know more about. Storm-0216 was an attractive target as the group was making use of a recent vulnerability I had used in my previous promptbook example. The prompt is simple and open, generating an executive summary and filling in whatever else Security Copilot knows about the threat. Normally, I like to refine prompts to deliver specific results, but an open prompt like this allows us to seed the session with useful context that can be helpful later.

Within the initial summary, I see accurate information and a preview of the jargon across the industry. This group goes by other names like Twisted Spider and UNC2198. They also make use of several different tools and backdoors, each with their own unique names and explanations. Knowing nothing about this group, this response is a helpful start to get acquainted, though it's a bit overwhelming. In the next prompts, I will narrow in on key areas and transform this data into something an organization could better operationalize.

Summarize the TTPs of this actor using MITRE ATT&CK techniques. Format the output as a bullet point list starting with the technique name and number and including a brief summary. Each technique should be linked directly to the MITRE ATT&CK website.

>  3 steps completed 53 seconds

Jan 2, 3:15 PM | 54 seconds

- **T1566.001: Phishing: Spearphishing Attachment:** The group uses malicious advertising campaigns to deliver Danabot, an information stealer, as part of their initial access strategy.
- **T1078: Valid Accounts:** They create users in the local group administrator's role with System or NT Authority\System privileges to target credentials for lateral movement.
- **T1021.001: Remote Services: Remote Desktop Protocol:** They rely on RDP for lateral movement and, if RDP is not allowed in the environment, they use administrator privileges to modify the Windows Firewall policy to enable Remote Desktop.
- **T1003.001: OS Credential Dumping: LSASS Memory:** They dump LSASS credentials, often by leveraging the living-on-the-land binarytaskmgr.exe(Task Manager).
- **T1573.002: Encrypted Channel: Asymmetric Cryptography:** As part of their command-and-control infrastructure, they establish SSH tunnels using scheduled tasks for persistence.
- **T1564.001: Hide Artifacts: Hidden Files and Directories:** For data exfiltration, they use the legitimate data synchronization tool Rclone, typically renamed to mimic the legitimate Windows process svchost.exe.
- **T1059.003: Command and Scripting Interpreter: Windows Command Shell:** They use small scripts to automate many of the steps taken after gaining initial access.
- **T1059.001: Command and Scripting Interpreter: PowerShell:** They incorporate Cobalt Strike, the open-source Impacket tool, and the DWAgent legitimate remote management tool.
- **T1496: Resource Hijacking:** They are known to deploy ransomware as part of their attack chain.

Summarize the actor TTPs and align against MITRE ATT&CK framework.

Here, our prompt is more specific, both in the request and the format. I've asked Security Copilot to align what it knows about Storm-0216 within the MITRE ATT&CK framework. Without specifying this, I get useful results, but they are less organized and difficult to parse.

I really like this alignment as the ATT&CK framework is leveraging across multiple solutions and companies, giving defenders a common taxonomy to reference. By requesting that data be mapped to this framework, it becomes more actionable.

For the format, I specify a bullet list and explicitly request the name and number of the MITRE technique along with a brief summary. Without this level of detail, I find that the responses will vary across each Promptbook run which isn't ideal, though very much a normal outcome when using generative AI. Finally, there's a request to link each technique to its given MITRE page for deeper explanation. I find this helpful as a quick reference to learn more. This view could alternatively be expressed as a table, though the bullet list is easier to consume.

If there are TI articles related to this threat actor, provide a list and summary of them and include links to source material.

>  3 steps completed 28 seconds

Jan 2, 3:16 PM | 29 seconds


- [Storm-0216 deploys Cactus ransomware beginning April 2023](#): This article discusses how Storm-0216 began deploying Cactus ransomware as early as April 2023. The group regularly shifts ransomware payloads from various ransom ecosystems over time, most recently deploying Royal ransomware in December 2022 before incorporating Cactus payloads.
- [Qakbot rebuilds infrastructure, distributor shifts to DarkGate](#): This article highlights how Qakbot operators have attempted to stand up new infrastructure within days of the takedown. One of the most prolific distributors of Qakbot malware, an initial access broker Microsoft tracks as Storm-0464, pivoted to distributing DarkGate malware in a phishing campaign that launched on September 20.
- [Danabot leads to Cactus ransomware](#): This article reveals that beginning in November 2023, Microsoft Threat Intelligence detected a malicious advertising campaign delivering Danabot, an information stealer tracked as Storm-1044. These Danabot infections have led to Storm-0216 hands-on-keyboard activity and deployment of Cactus ransomware.
- [Qlik Sense vulnerabilities exploitation leads to pre-ransomware activity](#): This article discusses how Microsoft Threat Intelligence observed possible initial access brokers exploiting several known disclosed vulnerabilities in Qlik Sense Enterprise installations. If successfully exploited, these vulnerabilities could let an attacker perform unauthenticated remote code execution and elevate privileges.
- [Activity profile: Qakbot distributor Storm-0464 shifts to DarkGate and IcedID](#): This article provides an activity profile of Storm-0464, a financially motivated access broker known for distributing Qakbot and facilitating access to hands-on-keyboard ransomware operators like Storm-0506, Storm-0216, and Storm-0826 who deploy Black Basta ransomware.

List and summarize threat articles associated with the threat actor.



This prompt performs a basic look-up within the database of curated and OSINT aggregated intelligence from Microsoft Defender Threat Intelligence. The prompt is simple and to the point. Provide any articles that include the threat actor references and summarize them with links. Those with limited understanding of the actor can quickly browse recent reporting with the option to dive further into the details of each case. As indicated in the final bullet point,

there's mention of several other related ransomware threat actors including Storm-0464, Storm-0506, and Storm-0826. These are all great candidates to run back through this same Promptbook to further our understanding of a broader ransomware ecosystem.

Based on the actor TTPs, what would be good mitigations or defense methods to protect against this threat actor? Begin with more specific examples and end with generic ones. Format as a table with sections for "category", "description" which includes the work to be done, and "reason" with example why this is important for the threat actor.

>  2 steps completed 19 seconds

Jan 2, 3:16 PM | 20 seconds

 Export to Excel 

Category	Description	Reason
<b>Email Security</b>	Implement strong email security measures, including spam filters and phishing detection. Regularly update and patch email systems.	This can help prevent the initial phishing attacks that Storm-0216 uses to deliver Danabot.
<b>User Privileges</b>	Implement least privilege policies and conduct regular audits of user privileges.	Storm-0216 creates users in the local group administrator's role with System or NT Authority\System privileges. Limiting user privileges can help prevent lateral movement.
<b>Firewall Policies</b>	Regularly review and update firewall policies. Limit the use of RDP and ensure it is secured with strong credentials and multi-factor authentication.	Storm-0216 relies on RDP for lateral movement and modifies the Windows Firewall policy to enable Remote Desktop if it is not allowed.
<b>Credential Management</b>	Regularly change and strengthen passwords. Consider implementing a password manager.	Storm-0216 dumps LSASS credentials, often by leveraging the living-on-the-land binarytaskmgr.exe(Task Manager). Strong credential management can help protect against this.

In this prompt, I shift back to more of a detailed prompt. Using the previous context formed from our broader session, I have Security Copilot outline mitigations and defense methods, starting with more specific first and ending with generic. This instruction is more open given the nature of the Promptbook, though could be tuned to an organization by incorporating

technology leveraged or specific control-points of interest. I've instructed to focus on specific to generic as I've observed the model will often mix the both and while the generic is useful, it's not always the most actionable.

For the format, I've requested a table and included headers with a small amount of instruction. The response gives me what I want and while it's generic due to the structure of the request, it's worth appreciating how these seemingly generic steps are punctuated with threat actor specific reasons. Advising an organization to apply least privilege principles is much more impactful when given the note that a known ransomware group will exploit this to move laterally and potentially wreak havoc on your organization. The former should be able to stand alone, but if that were true, ransomware wouldn't be as prolific.



Summarize the threat actor insights into an executive report. Begin with metadata points for the threat actor including aliases, suspected origin country, industries targeted, vulnerabilities exploited, and tools leveraged. Each of these should be CSV and brief. Below that, include a bullet list of key points about the threat actor as an executive summary. Below that, create paragraph sections for an overview, TTPs, and mitigation strategies. It should be suitable for a less technical audience.

>  3 steps completed 1 minute 4 seconds

Jan 2, 3:17 PM | 1 minute 5 seconds

## Executive Report on Storm-0216

### Metadata

- **Aliases:** Storm-0216, Twisted Spider, UNC2198
- **Suspected Origin Country:** Unknown
- **Industries Targeted:** Various, with a focus on organizations with high-value data
- **Vulnerabilities Exploited:** CVE-2023-41265, CVE-2023-41266, CVE-2023-48365
- **Tools Leveraged:** Cobalt Strike, Impacket, DWAgent, Rclone, GOST, chisel

### Executive Summary

- Storm-0216 is a financially motivated cybercriminal group known for deploying ransomware.
- They have been active since 2020 and have used various ransomware payloads over time.
- They use phishing campaigns for initial access and then dump LSASS credentials for lateral movement.
- They rely on RDP for lateral movement and modify the Windows Firewall policy to enable Remote Desktop if it is not allowed.
- They use the legitimate data synchronization tool Rclone for data exfiltration and establish SSH tunnels for command-and-control infrastructure.

### Overview

Storm-0216 is a financially motivated cybercriminal group that has been active since 2020. They are known for targeting organizations with the ultimate intent to deploy ransomware. They have been observed working with the actors behind the Qakbot banking trojan to load a backdoor, commonly Cobalt Strike. The group is known to escalate privileges, deploy additional backdoors, exfiltrate data, and deploy ransomware. They have shifted ransomware payloads over time, from Egregor and REvil to Royal in 2022 and Cactus in 2023.

### TTPs

Storm-0216 uses phishing campaigns for initial access, often delivering Danabot, an information stealer. Once they have a foothold, they dump LSASS credentials, often by leveraging the living-on-the-land binarytaskmgr.exe(Task Manager). They rely on RDP for lateral movement and, if RDP is not allowed in the environment, they use administrator privileges to modify the Windows Firewall policy to enable Remote Desktop. For data exfiltration, they use the legitimate data synchronization tool Rclone, typically renamed to mimic the legitimate Windows process svchost.exe. As part of their command-and-control infrastructure, they establish SSH tunnels using scheduled tasks for persistence.

### Mitigation Strategies

To protect against Storm-0216, organizations should implement strong email security measures, including spam filters and phishing detection. Regular audits of user privileges and implementation of least privilege policies can help prevent lateral movement. Regularly reviewing and updating firewall policies, limiting the use of RDP, and securing it with strong credentials and multi-factor authentication can also help. Regularly changing and

As a final step within this Promptbook, I ask Security Copilot for an executive report on the threat actor based on the session details. I request a metadata section that outlines common data seen across industry threat profiles including aliases, suspect origin country, industry targets, vulnerabilities exploited and tools leveraged. Below that is an executive summary formatted bullet points, followed by several narrative sections. This prompt could be further expanded to format the profile in the exact way an organization consumes data, but as it's written, it does a great first-pass.

## Follow-on Questions

---

The end of a Promptbook doesn't mean the end of the session. In fact, I'd argue it's the beginning! Now that we have a grounded session containing a bunch of information about this threat actor, what additional follow-up questions could we ask? Here's a few that immediately come to mind for myself based on my past analyst experience.

- Provide a threat actor profile on all of the other actors associated with ransomware.
- Provide vulnerability impact assessments on all mentioned CVEs known to be exploited by the group.
- What other threat actors commonly target <your industry>?
- Summarize [Cobalt Strike, Impacket, DWAgent, Rclone, GOST, chisel] tools leveraged by this threat actor. Include ways to detect these tools within my environment, specifically using network signatures in Zeek format.

## Operationalizing this Work

---

# Threat Actor Brief: Storm-0216



Storm-0216

Cybercriminal Group

Ransomware

Phishing

LSASS

RDP

Rclone

Danabot

Cobalt Strike

Cybersecurity

Mitigation Strategies

**Summary**

📌 Pinned Items (5)

## Summary

Storm-0216, also known as Twisted Spider and UNC2198, is a financially motivated cybercriminal group active since 2020. They target various industries, focusing on organizations with high-value data, and are known for deploying ransomware. The group uses phishing campaigns for initial access, dumps LSASS credentials for lateral movement, relies on RDP for lateral movement, and uses the legitimate data synchronization tool Rclone for data exfiltration.

## Overview

Storm-0216 has been observed working with the actors behind the Qakbot banking trojan to load a backdoor, commonly Cobalt Strike. The group escalates privileges, deploys additional backdoors, exfiltrates data, and deploys ransomware. They have shifted ransomware payloads over time, from Egregor and REvil to Royal in 2022 and Cactus in 2023.

## TTPs

Storm-0216 uses phishing campaigns for initial access, often delivering Danabot, an information stealer. Once they have a foothold, they dump LSASS credentials, often by leveraging the living-on-the-land binarytaskmgr.exe(Task Manager). They rely on RDP for lateral movement and, if RDP is not allowed in the environment, they use administrator privileges to modify the Windows Firewall policy to enable Remote Desktop. For data exfiltration, they use the legitimate data synchronization tool Rclone, typically renamed to mimic the legitimate Windows process svchost.exe. As part of their command-and-control infrastructure, they establish SSH tunnels using scheduled tasks for persistence.

## Mitigation Strategies

To protect against Storm-0216, organizations should implement strong email security measures, including spam filters and phishing detection. Regular audits of user privileges and implementation of least privilege policies can help prevent lateral movement. Regularly reviewing and updating firewall policies, limiting the use of RDP, and securing it with strong credentials and multi-factor authentication can also help. Regularly changing and strengthening passwords and considering the implementation of a password manager can help protect against credential theft. Implementing network segmentation, using a robust endpoint protection platform, conducting regular user awareness training, regularly patching and updating all systems, software, and firmware, and regularly backing up critical data and ensuring that

systems, software, and firmware, and regularly backing up critical data and ensuring that recovery procedures are in place and tested can all help mitigate the damage caused by a successful ransomware attack.

Building an understanding of a threat actor, specifically one that may be exploiting a ubiquitous vulnerability or one that delivers ransomware, requires expertise, access to quality intelligence and most importantly, time. The Threat Actor Profile Promptbook in Security Copilot, paired with Defender Threat Intelligence, saves analysts hours of work and gives them a stronger foundation to operate from. Generative AI brings an actionable component to this information and allows for the reporting to be tailored to your organization.

One way to operationalize this Promptbook would be to identify which threat actors commonly target your industry and attach this Promptbook to run on a weekly basis. Results from the Promptbook could be reformatted to meet your needs and merged into a knowledge base for future reference. You can leverage the out-of-the-box Security Copilot version of this Promptbook or design your own to match your specific needs.

What I enjoy most about this Promptbook is the fact that it of course runs well on any Microsoft named threat, but it will also take alternative aliases from other company naming conventions and function on those as well. Years ago, when I did espionage research, I had to use a spreadsheet as a "rosetta stone" of threat actor names. I am hopeful that solutions such as this can begin to replace those older methods and allow defenders to focus on what matters most in their organization.