

WHITE PAPER


Understanding Today's Threat Actors

Insights from Incident Responders and Tips for Protecting Your Organization



Executive Summary

The cyberthreat landscape constantly changes, posing significant challenges for security professionals. Threat actors often evade traditional prevention-oriented security controls. In the first half of 2023, threat actors utilized valid credentials most often to gain entry to a corporate network and then disabled defenses to remain hidden.¹ This offered them plenty of time for network discovery, lateral movement, and data collection before exfiltrating and encrypting that data. While attackers' increasingly sophisticated activities should sound alarm bells, that same sophistication provides organizations ample opportunity to stop these attacks before a threat actor can achieve their objectives.



In the first half of 2023, two-thirds of cybercriminals used valid credentials to gain initial entry into a network.²

The Evolving Threat Landscape Keeps Security Practitioners Up at Night

In a survey conducted by Enterprise Strategy Group, participants were asked what makes security operations more difficult today than two years ago. The top response was the rapidly evolving cyberthreat landscape.³

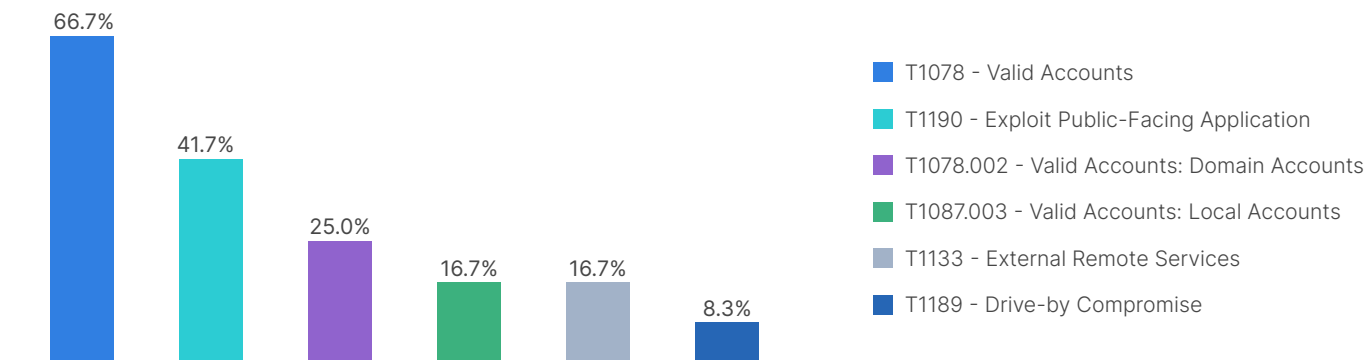
To provide defenders with insights into the most common tactics threat actors use, Fortinet recently published its [Fortinet FortiGuard Incident Response Report 1H 2023](#). In the report, we shared the most common ways adversaries could gain and maintain access to organizations, what they typically did after gaining that access, and the most common threat actor objectives we observed.

We present key findings from that report here to help organizations assess their current cybersecurity capabilities, identify gaps, and prioritize measures and investments to close those gaps and manage their cyber risk.

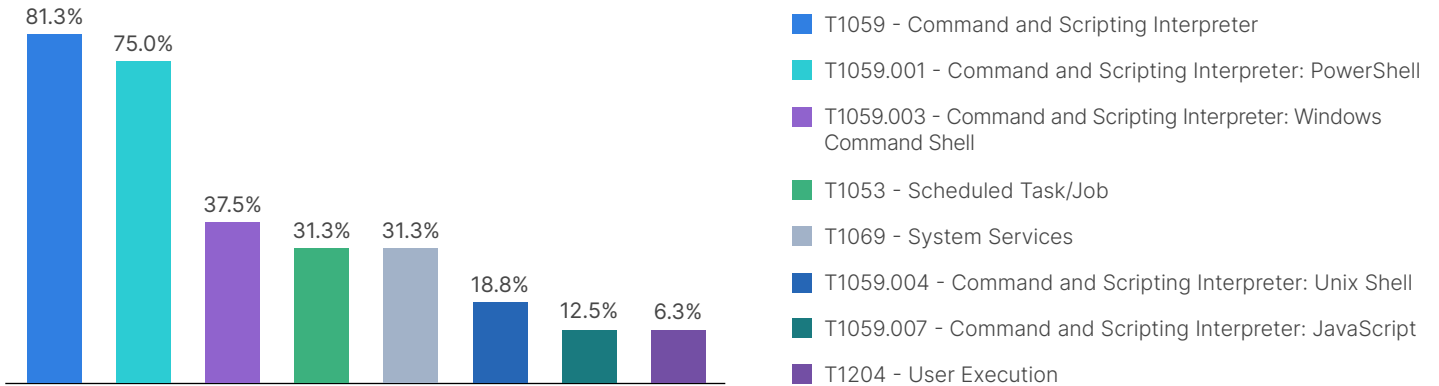
How Threat Actors Gain and Maintain Access to Your Network

With all the investments made in prevention-oriented cybersecurity capabilities over the years, organizations often question how threat actors continue to find their way into corporate networks. Were the established security controls ineffective? Were there gaps between those controls that let adversaries slip through the cracks? Were employees tricked into downloading files that allowed a cybercriminal to access the network?

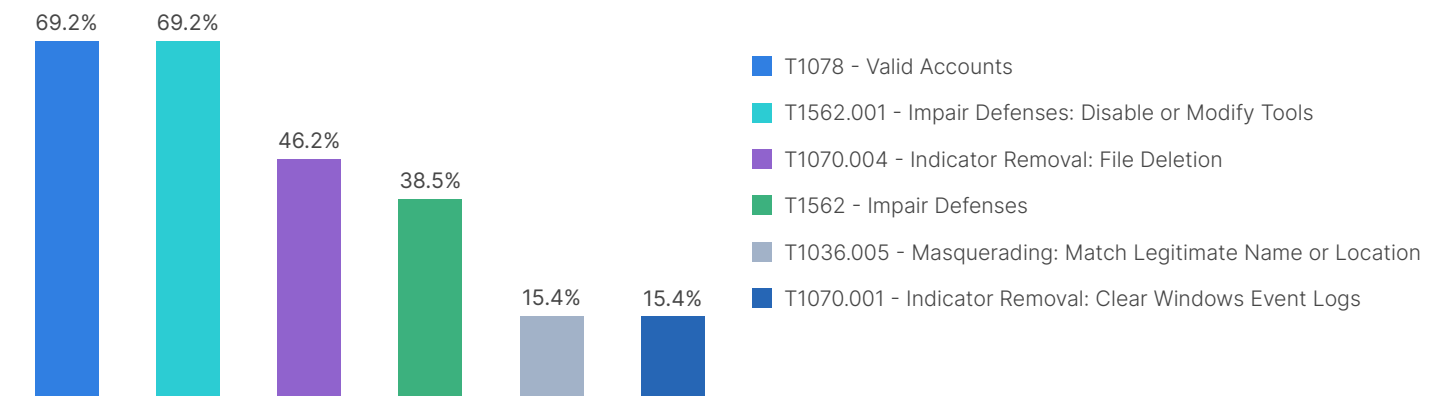
While the answer to these questions is sometimes “yes,” threat actors often used valid credentials as their entry mechanism, followed by exploiting public-facing applications. In fact, in the past six months, more than two-thirds of breaches we investigated resulted from adversaries using valid accounts to gain access.⁴ Valid credentials are readily sought and made available on the dark web for this purpose. There is a whole category of “initial access brokers” providing means of entry, including credentialed access.



Not only that, when malicious code was executed, it was primarily triggered automatically using scripting, such as PowerShell or command shell. While your initial instinct may be to blame the end-users, user execution did not make the list of top compromise methods.

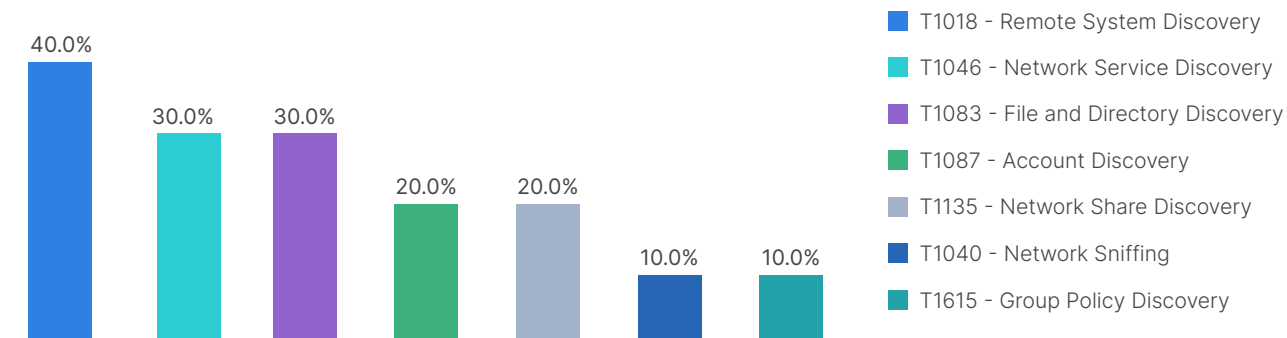


Finally, once inside an organization, threat actors typically took steps to remain unnoticed for an extended period—26 days on average—as they went about their business.⁵ This is a result of using valid accounts, turning off defensive tools, and removing signs of the initial intrusion.

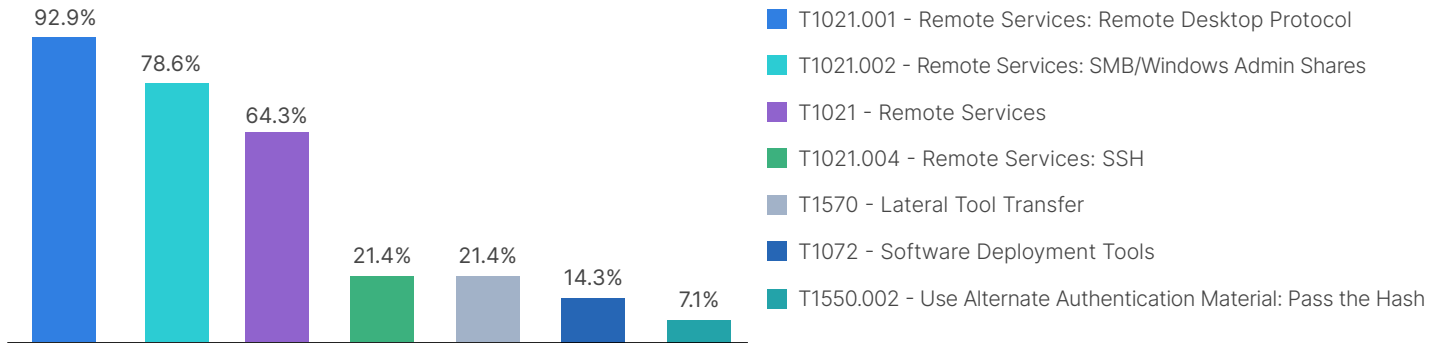


A Closer Look at Discovery, Lateral Movement, and Further Instruction

Once inside, with an expectation of remaining undetected for an extended period, threat actors typically took their time to plan the next move, focusing on discovery: discovery of remote systems, network services, files, directories, accounts, and even network shares.⁶



With this insight, often reported back to the threat actor via command-and-control (C&C) communications, campaigns would move laterally to maximize their reach within the organization. Most often, this was conducted using the remote systems and services that threat actors discovered once they were inside the network.

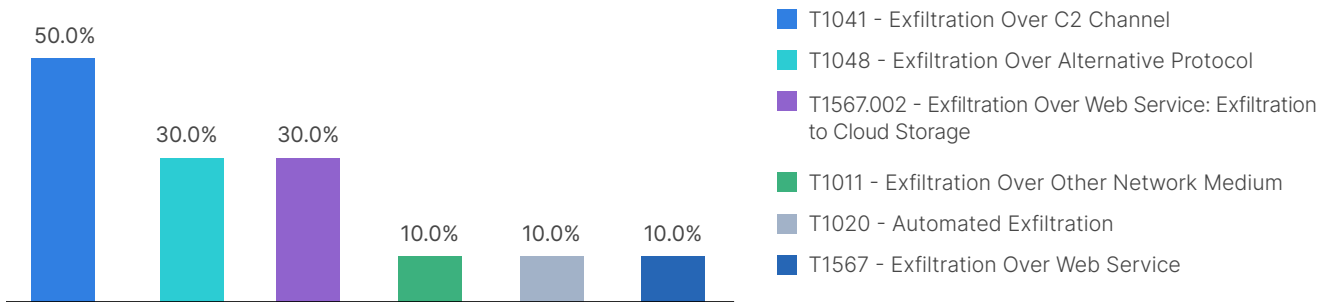


Interestingly, while there's discussion in the security community of threat actors often using encrypted traffic to bypass security inspection, half the time C&C traffic utilizes standard application layer protocols. The use of encrypted channels was only observed in 15% of instances.⁷

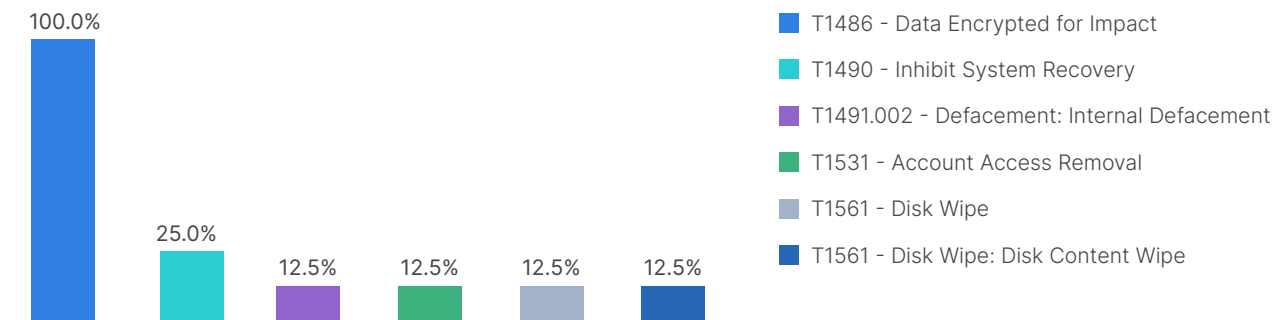
In 25% of cases, cybercriminals encrypted data and impaired recovery systems.⁹

A Closer Look at Collection, Exfiltration, and Impact

With an in-depth understanding of the organization, its systems, and data, threat actors were routinely able to collect data from both network share drives and local systems (70% and 50%, respectively) before exfiltrating it over those same C&C channels, or even via alternate protocols or web services.⁸



Interestingly, in all cases when Fortinet was called in to investigate, data was encrypted to maximize impact and, in a quarter of cases, system recovery was impacted as well.¹⁰



Conclusion

What does this mean for defenders?

First, stop blaming installed security controls for failing to protect the organization's assets. When attackers use valid accounts to gain entry to a network, you need the ability to identify abnormal or unauthorized activity of valid users and their credentials. Therefore, organizations must invest more in detection and response technologies and services to safeguard their enterprise effectively.

Additionally, the signs of activity after intrusion are often available but only for the teams and tools prepared to identify them. Activity logging and monitoring tools can pinpoint automated installation, evasion, discovery, lateral movement, C&C communications and more when properly configured and monitored.

Lastly, to maximize their return on intrusion, threat actors often progress through multiple stages of action. This is good news for defenders, as they need only to detect and disrupt that activity at one stage to thwart the attack. However, this is only possible if the organization has defined the processes and trained its teams to execute them, which will turn individual signals into higher-fidelity incident indicators and trigger containment and remediation actions. Ideally, this takes the form of documented, repeatable, and practiced playbooks to guide staff who may lack expertise, time, or diligence in handling a constant stream of often mundane alerts. That said, this information often does paint an important picture of attacks in progress.

For more insights on attacker activities and recommendations for effectively protecting your organization, [download a free copy](#) of the full report.

¹ [FortiGuard Incident Response Report, 1H 2023](#), Fortinet, October 17, 2023.

² Ibid.

³ [SOC Modernization and the Role of XDR](#), Enterprise Strategy Group, October 24, 2022.

⁴ [FortiGuard Incident Response Report, 1H 2023](#), Fortinet, October 17, 2023.

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.

⁸ Ibid.

⁹ Ibid.

¹⁰ Ibid.

