The Active Adversary Playbook 2021

news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/

May 18, 2021

Introduction

The challenge of defending an organization against cyberthreats can be considerable. Adversaries continuously adapt and evolve their toolsets and activity in order to seize new opportunities, evade detection and stay one step ahead of security teams. It can be hard for an organization to keep up with the latest approaches used by adversaries, particularly when it comes to targeted, active attacks that are orchestrated by human operators.

The Active Adversary Playbook 2021 details attacker behavior and impact as well as the tactics, techniques and procedures (TTPs) seen in the wild by Sophos' frontline threat hunters and incident responders.

Our aim is to help security teams understand what adversaries do during attacks and how to spot and defend against such activity on their network.

The findings are based on data from Sophos telemetry as well as incident reports and observations from the Sophos Managed Threat Response (MTR) and Sophos Rapid Response teams in 2020 and early 2021. The data is categorized according to the MITRE ATT&CK framework.

Adversary Tactics and Techniques

The starting point: how to get the most from security product signals

Security product detections are an invaluable source of potential warning signs. Just because something was blocked doesn't mean a threat has been fully neutralized. For instance, a detection for the Mimikatz credential stealer on a domain controller might be blocked, but the very fact that it exists means that a threat actor has already compromised the server and may try other techniques that aren't detected. It is always worth investigating suspicious alerts, even alerts for blocked threats.

Taking full advantage of security product telemetry comes down to understanding your organization's operating environment. As we discuss later in this post, adversaries are turning to tools that are commonly used by IT administrators and security professionals, making it harder to identify suspicious actions.

This is particularly the case when adversaries use legitimate tools such as Advanced Port Scanner, ADRecon, and others. Many of these tools are detected by security products as "potentially unwanted applications" (or PUAs) and are needed for everyday use by IT teams.

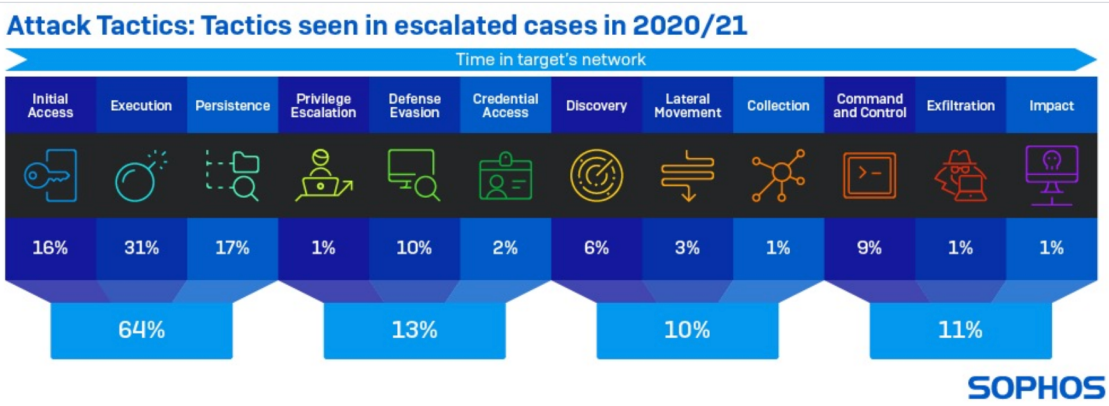
Defenders need to ask two important questions: (1) Do all my users need to be able to use these utilities? (2) Do these utilities need to be able to run on every device?

The answers to these questions will allow you to set appropriate exception policies for the use of such tools. It also makes it easier to spot suspicious use: is the person or device trying to run this tool authorised to do so? If the answer is no, investigate immediately.

Tactics

Early stage tactics are the highest value detections for defenders because if they are blocked they can neutralize and contain an attack before it has the chance to fully unfold and cause damage or disruption.

It is therefore not surprising that the attacker tactics most likely to spark an investigation are heavily weighted towards activity that happens early in the attack chain. For instance, out of all the tactics escalated by Sophos MTR for investigation, 31% were suspicious "execution" detections, 17% were "persistence" detections and 16% were "initial access" detections.



The tactics are generally identified through the techniques used to achieve them. The table below lists the top adversarial techniques associated with each attack tactic during 2020/2021.

The top 5 techniques observed with each tactic in 2020/2021

TA0001	Initial access
T1133	External Remote Services
T1190	Exploit Public-Facing Application
T1566	Phishing
T1078	Valid Accounts
T1195	Supply Chain Compromise

TA0002	Execution
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation
T1053	Scheduled Task/Job
T1569	System Services
T1204	User Execution

TA0003	Persistence
T1543	Create or Modify System Process
T1547.001	Registry Run Keys / Startup Folder
T1546.007	Netsh Helper DLL
T1547.010	Port Monitors
T1098	Account Manipulation

TA0004	Privilege escalation
T1059	Process Injection
T1047	Process Hollowing
T1053	SID-History Injection
T1569	.bash_profile and .bashrc
T1204	Security Support Provider

TA0005	Defense evasion
T1036	Masquerading
T1218	Signed Binary Proxy Execution
T1070	Indicator Removal on Host
T1562.001	Disable or Modify Tools
T1112	Modify Registry

TA0006	Credential access
T1552.002	Credentials in Registry
T1040	Network Sniffing
T1110	Brute Force
T1552.004	Private Keys
T1003	OS Credential Dumping

TA0007	Discovery
T1033	System Owner/User Discovery
T1007	System Service Discovery
T1016	System Network Configuration Discovery
T1046	Network Service Scanning
T1082	System Information Discovery

TA0008	Lateral movement
T1021.001	Remote Desktop Protocol
T1021.002	SMB/Windows Admin Shares
T1570	Lateral Tool Transfer
T1550.003	Pass the Ticket
T1550.002	Pass the Hash

TA0009	Collection
T1560.001	Archive via Utility
T1074	Data Staged
T1005	Data from Local System
T1039	Data from Network Shared Drive
T1409	Access Stored Application Data

TA00011	Command and control
T1105	Ingress Tool Transfer
T1090	Proxy
T1572	Protocol Tunneling
T1008	Fallback Channels
T1043	Commonly Used Port

TA0010	Exfliration
T1041	Exfiltration Over C2 Channel
T1048	Exfiltration Over Alternative Protocol
T1567.002	Exfiltration to Cloud Storage
T1567.001	Exfiltration to Code Repository
T1537	Transfer Data to Cloud Account

TA0040	Imapact
T1490	Inhibit System Recovery
T1486	Data Encrypted for Impact
T1485	Data Destruction
T1489	Service Stop
T1496	Resource Hijacking

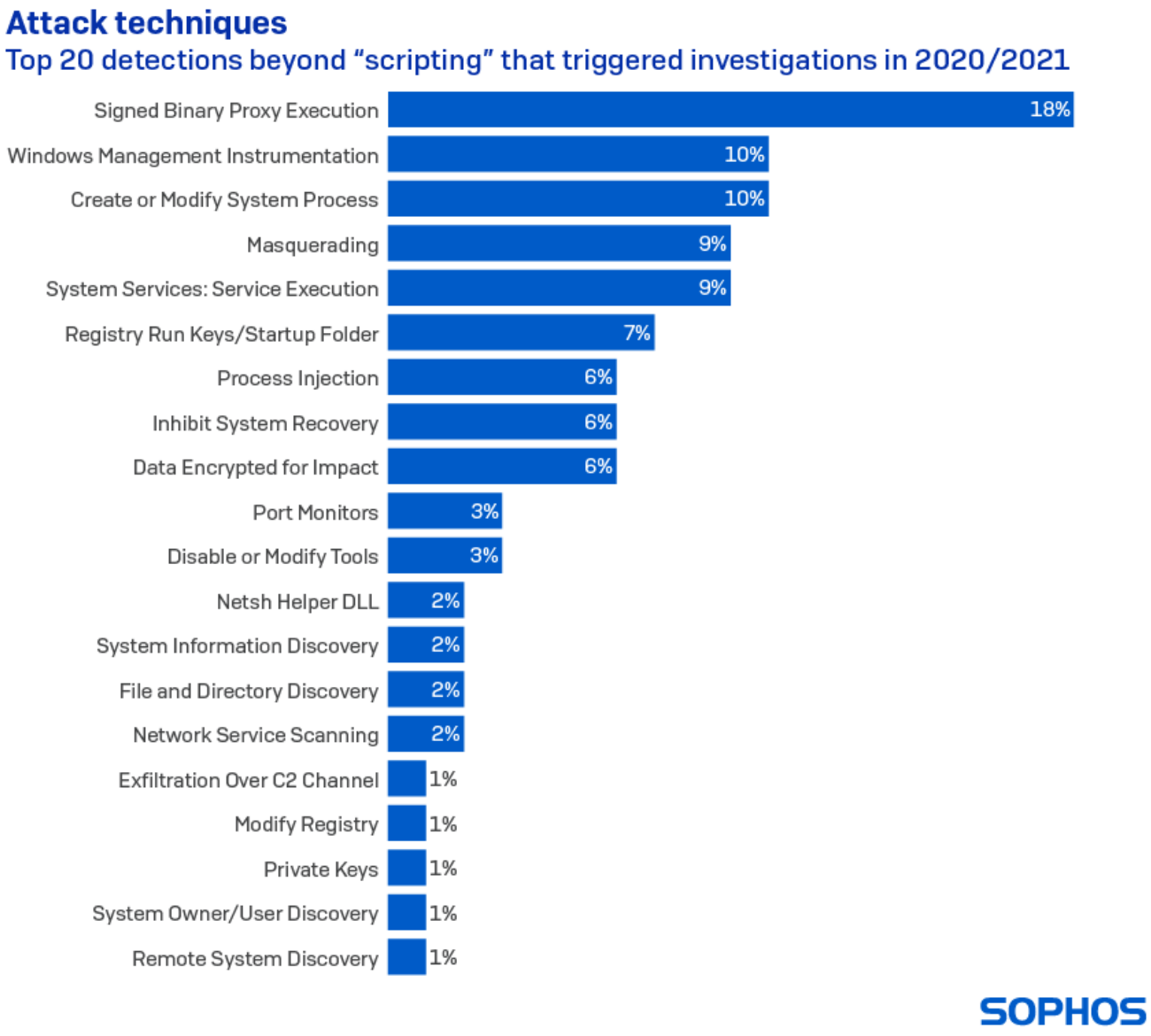
SOPHOS

Techniques

The table below lists the techniques most likely to trigger a deeper investigation and to signpost an active threat.

The overall leader, “Command and Scripting Interpreter,” which includes such things as PowerShell, Cmd, etc., was excluded from the list because its dominance overshadows and obscures other important techniques. Scripting is the most used technique across all MITRE categories, and most MITRE techniques are achievable via script.

After scripting, the list is led by techniques that involve proxying the execution of malicious content with signed binaries ("signed binary proxy detections.") One in six (18%) of all detections that sparked investigations involved this technique. Windows Management Instrumentation detections were in second place, accounting for 10% of investigations.



Adversary Behavior and Impact

The data and observations in this section are based on 81 incidents targeting organizations of all sizes (the largest organization involved had 13,500 employees,) in a wide range of industry sectors, located as far afield as the U.S., Canada, the U.K., Australia, Switzerland, Germany, Belgium, Hong Kong, and Austria.

The most hit sector was manufacturing (the target for 16% of attacks) followed by healthcare, retail and IT (each a target for 9% of incidents,) and then financial services and business services (5% each.) Non-profit organizations were the target for 4% of attacks.

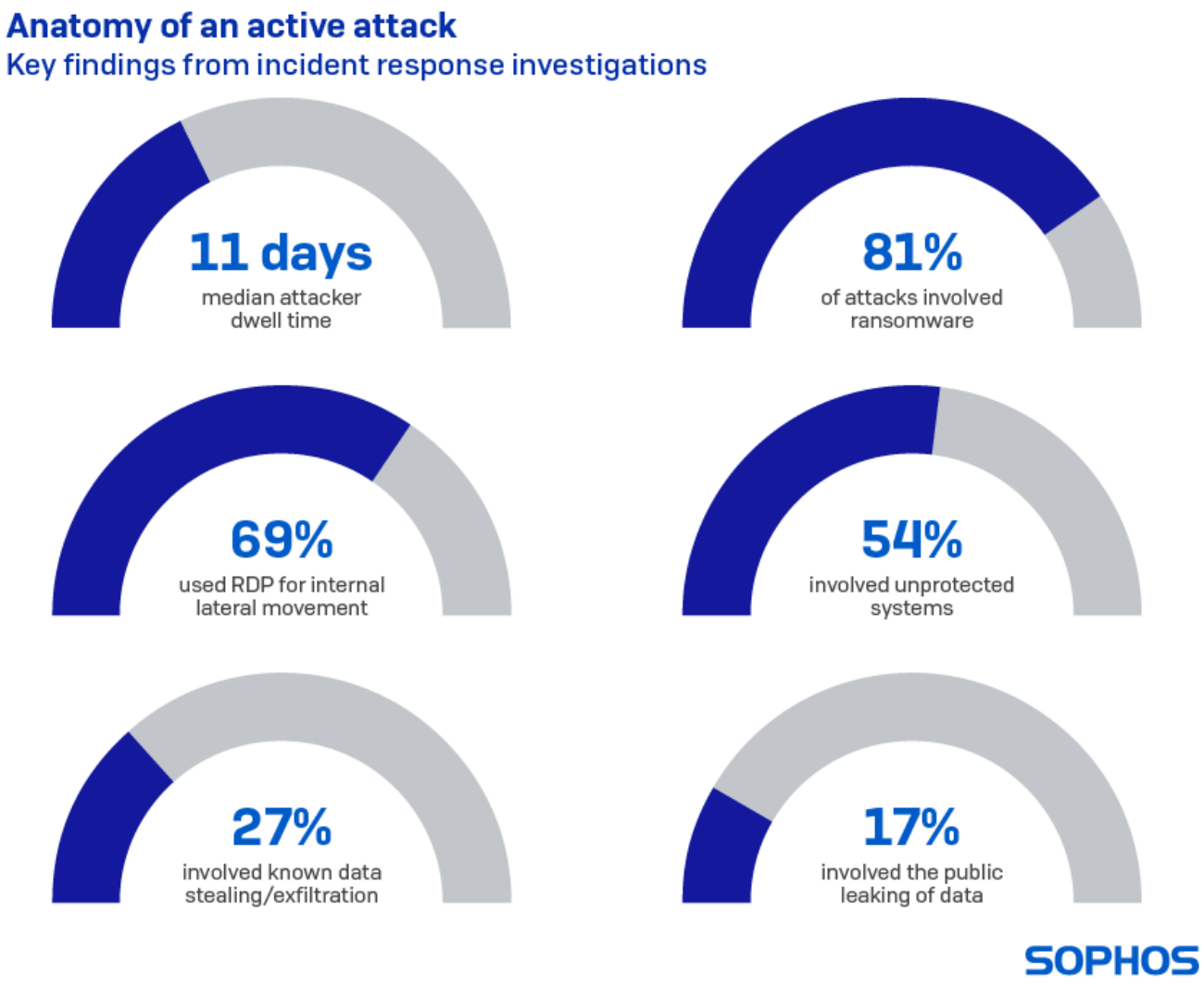
Anatomy of an active attack

The median time that attackers were able to remain in the target network before detection – dwell time – was 11 days. The longest intruder dwell time observed by rapid responders was 439 days (more than 15 months.)

To put this in context, 11 days potentially provide attackers with approximately 264 hours for malicious activity, such as lateral movement, reconnaissance, credential dumping, data exfiltration, and more. Considering that some of these activities can take just minutes or a few hours to implement, 11 days provide attackers with plenty of time to do damage.

The release of ransomware is often the point at which an attack becomes visible to the IT security team. It is therefore not surprising that 81% of the incidents Sophos responded to involved ransomware. Ransomware attacks tend to have shorter dwell time than "stealth" attacks, because they are all about destruction.

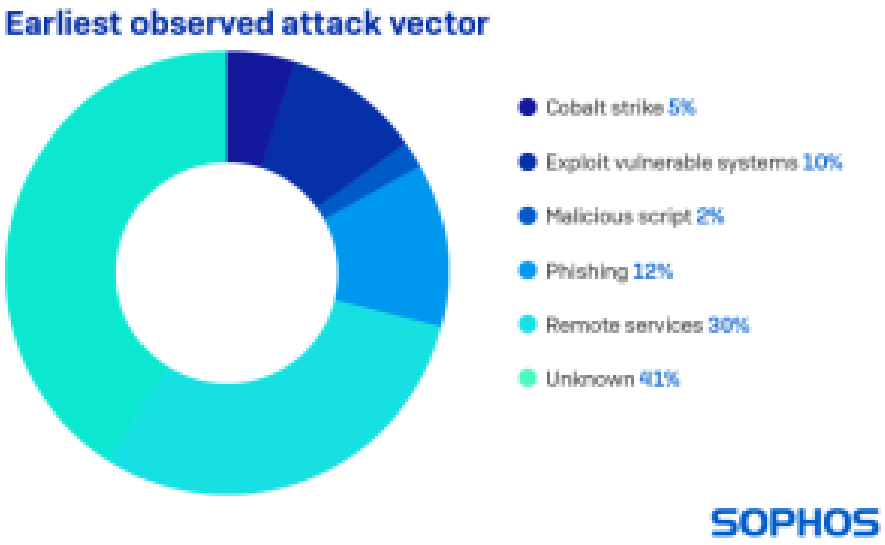
Other attack types included exfiltration-only, cryptominers, banking trojans, wipers, droppers, pen test/attack tools, and more.



Earliest observed attack vector

Remote access services such as Remote Desktop Protocol (RDP) were involved at the start of almost one in three (30%) attacks. Phishing was the starting point for around one in eight (12%) attacks, followed by the exploitation of vulnerable systems in about one in 10.

Cobalt Strike was the earliest identified part of the attack in around 5% of cases, but its prevalence across many different stages of an active attack suggests that the presence of Cobalt Strike is among one of the most valuable indicators of active malicious activity.



Why “unknown” matters

Threat investigators can’t always retrace every step intruders take in an attack. Sometimes the attackers have intentionally deleted evidence of their activity and sometimes the IT security team has already wiped or re-imaged compromised machines by the time the responders arrive. The result can be the loss of important forensic information that could reveal security gaps in the target’s IT environment and provide valuable insight on attacker behavior.

A quick note about RDP

RDP played a part in 90% of attacks. However, the way in which attackers used RDP is worth noting. In incidents that involved RDP, it was used for external access only in just 4% of cases. Around a quarter (28%) of attacks showed attackers using RDP for both external access and internal movement, while in 41% of cases, RDP was used only for internal lateral movement within the network.

Top attack droppers

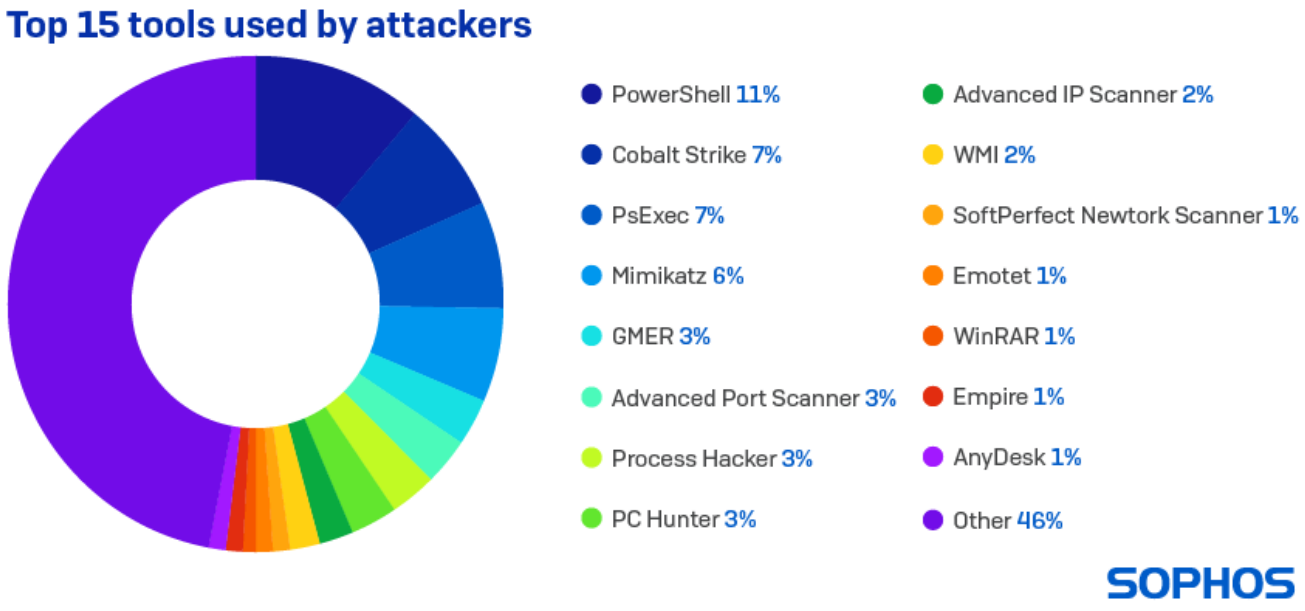
A dropper is a kind of delivery malware – or trojan – designed to load or install other malware to a target system. The payload is either carried inside the dropper or the dropper downloads it when it is activated. Droppers are enablers for an unfolding attack, providing a platform for additional malicious modules such as backdoors and ransomware.

Malicious scripts were by far the most prevalent dropper seen by incident responders and were involved in a third of all attacks. They were followed by a broad category of tools used both by attackers and penetration testers ("grey hat" tools, such as those seen in the artefact table below, accounting for 9% of attacks.) Trickbot (seen in 3.7% of incidents) and QBot (seen in 1.2% of cases) are two widely used types of "secondary malware" often seen in ransomware attacks. Valak, a malware dropper now believed to be evolving into a more advanced multi-stage modular malware and Cobalt Strike were each seen in 1.2% of cases. The dropper used was unknown in 47% of investigations.

Tools used in attacks

The pie chart shows the items most likely to be found in an attacker's toolbox. The full list of tools seen in attacks totalled 405. Most of them are distinct, identifiable tools and many can also be used by IT professionals for benign purposes. They appeal to attackers because they allow them to implement activity such as credential stealing, discovery, lateral movement and malware execution, and more, while blending in with harmless everyday IT activity.

The number and nature of the tools seen highlight the challenge defenders face in differentiating between malicious and legitimate activity on the network.



For example, Process Hacker, PCHunter and GMER are all legitimate tools that include kernel drivers. If an attacker gets the right kernel driver installed they can often disable security products. The fact that attackers are now routinely trying to do this is a testament to how good security products are at disrupting the attack kill chain. In other words, if you can't beat them, try to break them.

It is good security practice to ensure the use of these tools is blocked except for specific circumstances, and to investigate what is going on if they are spotted being used at any other time.

The red flag of tool combinations

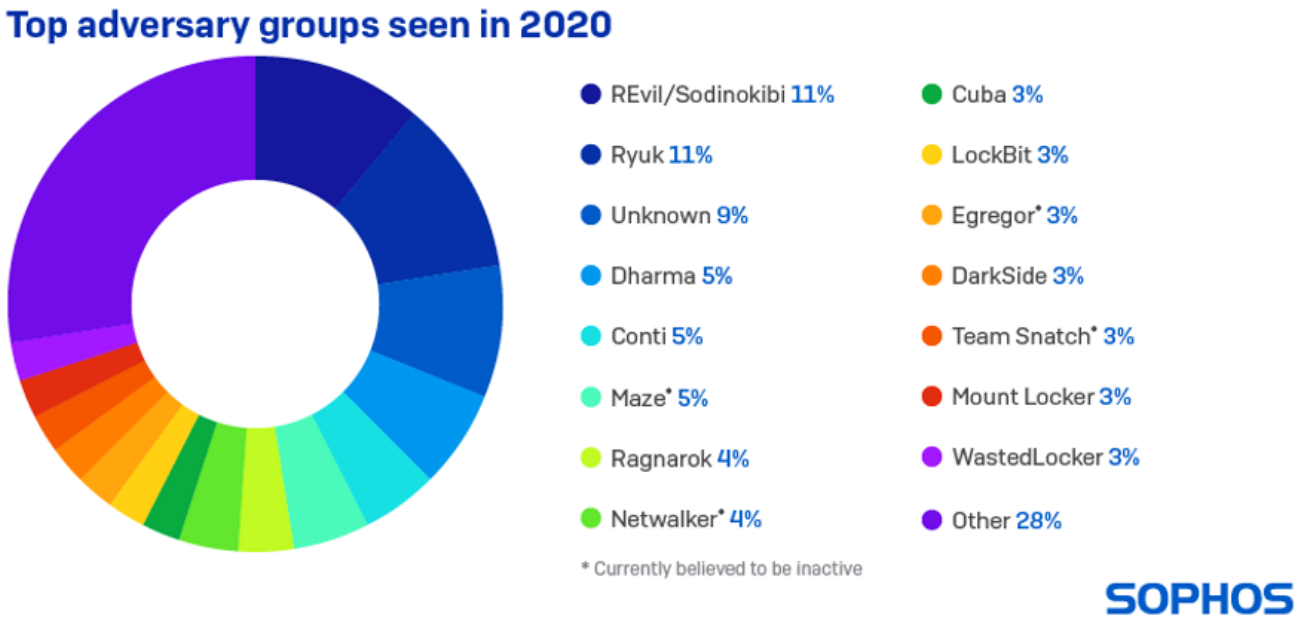
Some interesting correlations emerge among the top five tools found in victim networks.

For instance, when PowerShell is used in an attack, Cobalt Strike is seen in 58% of cases, PsExec in 49%, Mimikatz in 33%, and GMER in 19%. Cobalt Strike and PsExec are used together in 27% of attacks, while Mimikatz and PsExec occur together in 31% of attacks. Lastly, the combination of Cobalt Strike, PowerShell and PsExec occurs in 12% of all attacks.

Such correlations are important because their detection can serve as an early warning of an impending attack or confirm the presence of an active attack.

The main attack groups seen

The list of attack groups seen is dominated by ransomware families, but also includes cryptominers and suspected nation-state attackers, among others. In some cases, the attack group involved is unknown because the attack was detected and contained before the release of the final payload. There were 37 different attack groups identified in all, a clear indication of how very crowded and complex the cyberthreat landscape has become, and how difficult this can make life for defenders.



Conclusion

Every organization is a target for someone. It could be for business email compromise, cryptominers, data exfiltration, corporate espionage or a headline-hitting large scale ransomware attack. Cybercrime is a lucrative business.

Security teams can defend their organization by monitoring and investigating suspicious activity. The difference between benign and malicious is not always easy to spot. Technology in any environment, whether cyber or physical, can do a great deal but it is not enough by itself. Human experience and the ability to respond are a vital part of any security solution.

Sophos Managed Threat Response and Rapid Response

The Sophos Managed Threat Response (MTR) team provides 24/7, worldwide threat hunting, detection, and response capabilities, delivered by an expert team as a fully managed service. For more information on the Sophos MTR service, visit our website. If you prefer to conduct your own threat hunts, Sophos EDR gives you the tools you need for advanced threat hunting and IT security operations.

Sophos Rapid Response helps organizations facing an active threat to contain, neutralize and investigate the incident. If you need immediate assistance, you can contact Sophos Rapid Response for support 24/7.