SOPHOS NEWS

The Active Adversary Playbook 2022

Cyberattacker behaviors, tactics and tools seen on the frontline of incident response during 2021

JUNE 07, 2022

Introduction

The challenge of defending an organization against rapidly evolving, increasingly complex cyberthreats can be considerable. Adversaries continuously adapt and evolve their behavior and toolsets, leverage new vulnerabilities, and misuse everyday IT tools to evade detection and stay one step ahead of security teams.

It can be hard for an organization's IT and security operations professionals to keep up with the latest approaches used by adversaries. This is true particularly when it comes to targeted, active attacks that involve more than one perpetrator, such as an initial access broker (IAB) breaching a target and then selling that access on to a ransomware gang for use in their attack.

The Active Adversary Playbook 2022 details the main adversaries, tools, and attack behaviors seen in the wild during 2021 by Sophos' frontline incident responders. It follows on from the Active Adversary Playbook 2021and shows how the attack landscape continues to evolve.

The 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 incidents investigated by the Sophos Rapid Response team during 2021. Where possible, the data is compared against the incident response findings outlined in the Active Adversary Playbook 2021.

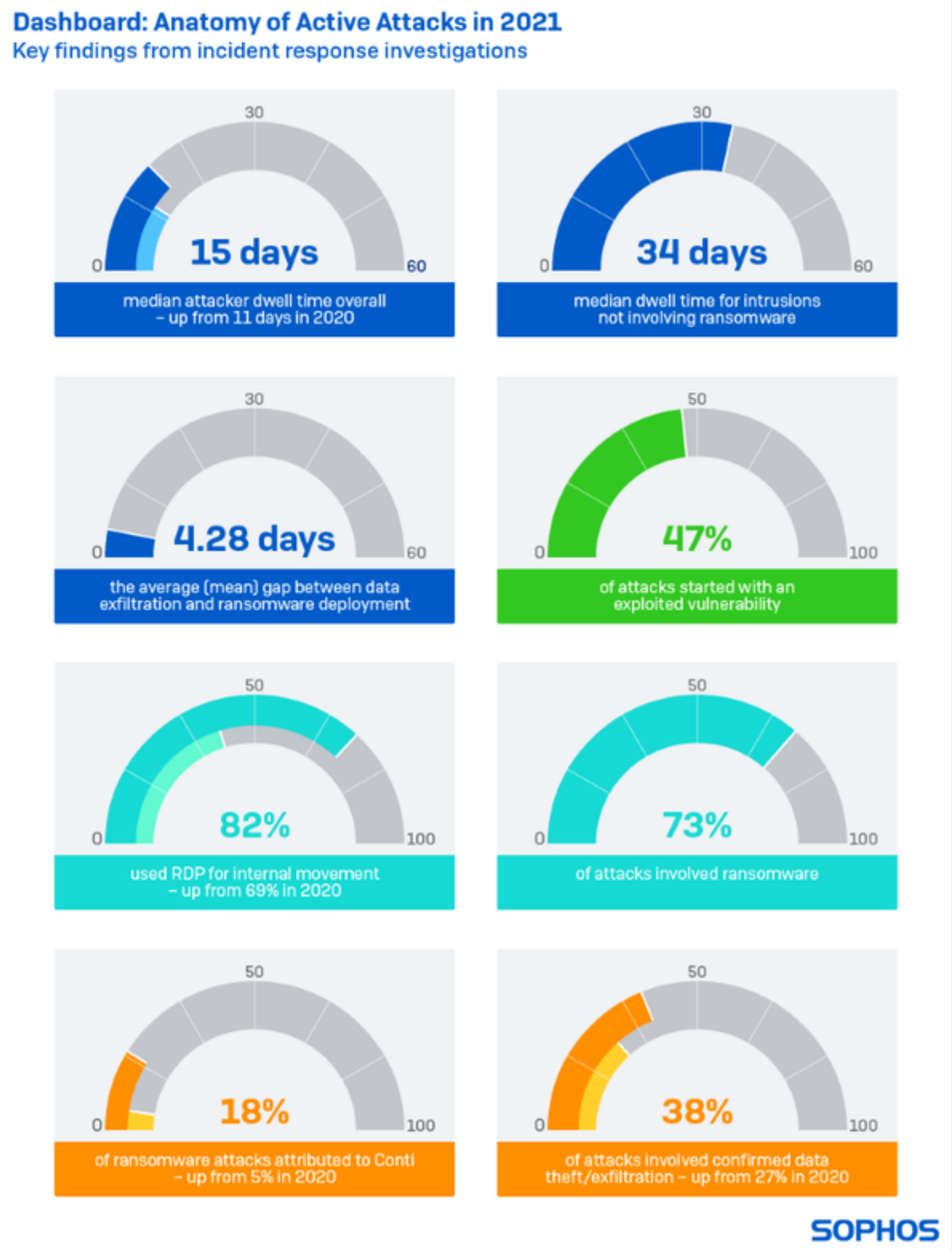
Incident Response Demographics 2021

The report is based on 144 incidents targeting organizations of all sizes, in a wide range of industry sectors, and located in the U.S., Canada, the U.K., Germany, Italy, Spain, France, Switzerland, Belgium, Netherlands, Austria, the United Arab Emirates, Saudi Arabia, the Philippines, the Bahamas, Angola, and Japan.

The most represented sectors are manufacturing (17% of incident response cases were in this sector) followed by retail (14%), healthcare (13%), IT (9%), construction (8%), and education (6%). Additional profile information can be found in the data tables at the end of this report.

Dashboard: The Anatomy of Active Attacks in 2021

Two of the most influential cyberthreat developments of the year occurred in March and August 2021, with the reporting of the ProxyLogon and ProxyShell vulnerabilities in Microsoft Exchange servers. As noted recently by CISA and other government security agencies, the ProxyLogon/ProxyShell bugs have been extensively exploited by adversaries. Not surprisingly, they feature in a significant number of the incidents investigated by Sophos during 2021.



Dashboard: Anatomy of Active Attacks in 2021

Key findings from incident response investigations

15 days median attacker dwell time overall – up from 11 days in 2020

34 days median dwell time for intrusions not involving ransomware

4.28 days the average (mean) gap between data exfiltration and ransomware deployment

47% of attacks started with an exploited vulnerability

82% used RDP for internal movement – up from 69% in 2020

73% of attacks involved ransomware

18% of ransomware attacks attributed to Conti – up from 5% in 2020

38% of attacks involved confirmed data theft/exfiltration – up from 27% in 2020

There are likely to be many more ProxyLogon/ProxyShell breaches that are currently unknown, where web shells and backdoors have been implanted in victims for persistent access and are now waiting silently until that access is used or sold.

This leads to another major development shaping the cyberthreat landscape in 2021: the growing influence and power of initial access brokers (IABs).

The success of IABs depends on being the first to breach a target and achieve access they can sell on. As a result, IABs are often quick to appear on the scene of newly reported bugs, hoping to compromise targets before widespread patching has taken place. Their aim is to secure a foothold in a victim and possibly do some initial exploratory movement to get a sense of the value of the asset – before selling it on to other adversaries, such as ransomware operators, to use in attacks, sometimes months after the initial intrusion.

As highlighted in the Sophos 2022 Threat Report, the rise of IABs reflects the growing "professionalization" of attacks in a cyberthreat market that features a growing number of specialized service suppliers. The thriving ransomware as a service (RaaS) industry is another example of this trend.

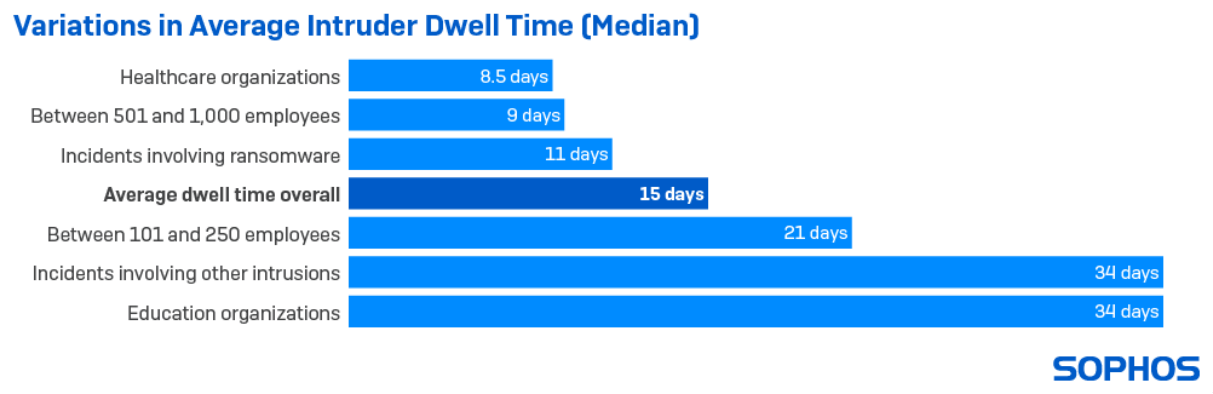
Last but not least, forensic evidence uncovered during incident response investigations in 2021 revealed instances where multiple adversaries, including IABs, ransomware gangs, cryptominers, and occasionally even multiple ransomware operators, were targeting the same organization simultaneously. This is a development that will continue to shape the cyberthreat landscape in 2022 and beyond.

The length of time intruders spend in victim networks is increasing, likely due to such activity. Other adversaries that are in victim networks for the long haul, sometimes concurrently, include botnet builders and malware delivery platforms or droppers.

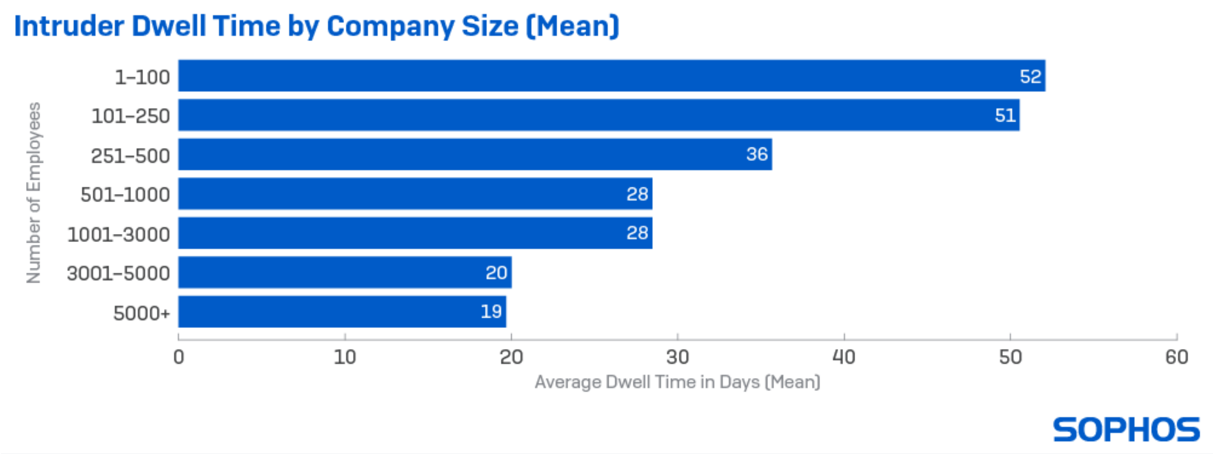
These developments are discussed in more detail below.

The Invisible Intruders

The incident data shows that the median average dwell time increased by about a third between 2020 and 2021, from 11 days to 15. There was considerable variation, with attacks that culminated in ransomware having shorter dwell times, on average around 11 days (down from 18 in 2020), and those involving other intrusions lasting significantly longer, with a median dwell time of 34 days.

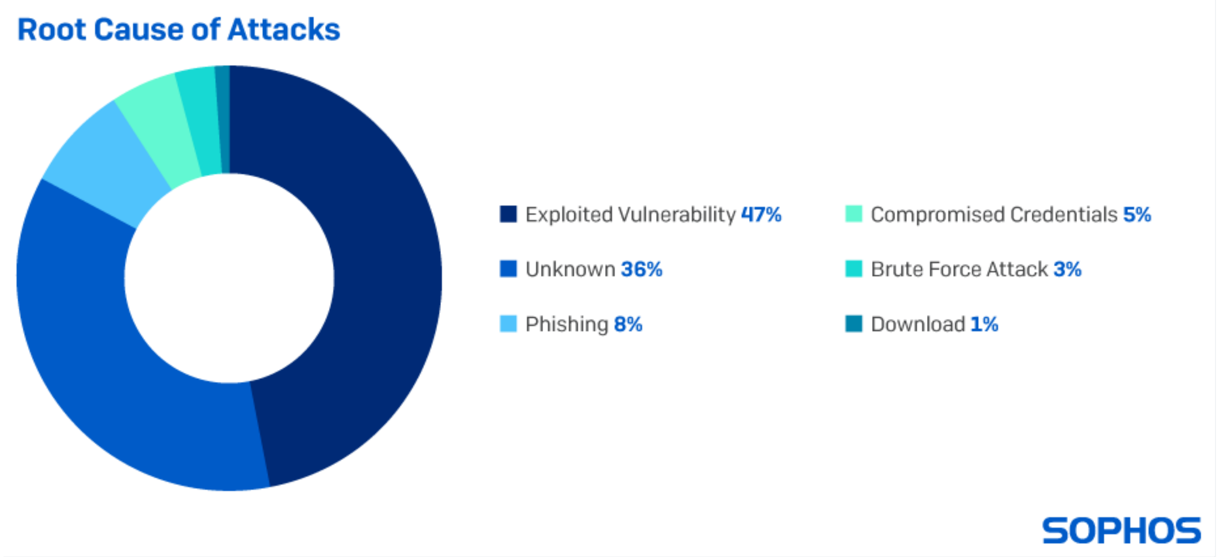


As suggested above, longer dwell times may reflect the involvement of an IAB. For smaller businesses or industry sectors such as education (average intruder dwell time 34 days), the longer dwell times also reflect how hard it can be for in-house IT security staff to proactively hunt for, investigate, and respond to suspicious alerts and potential threats.



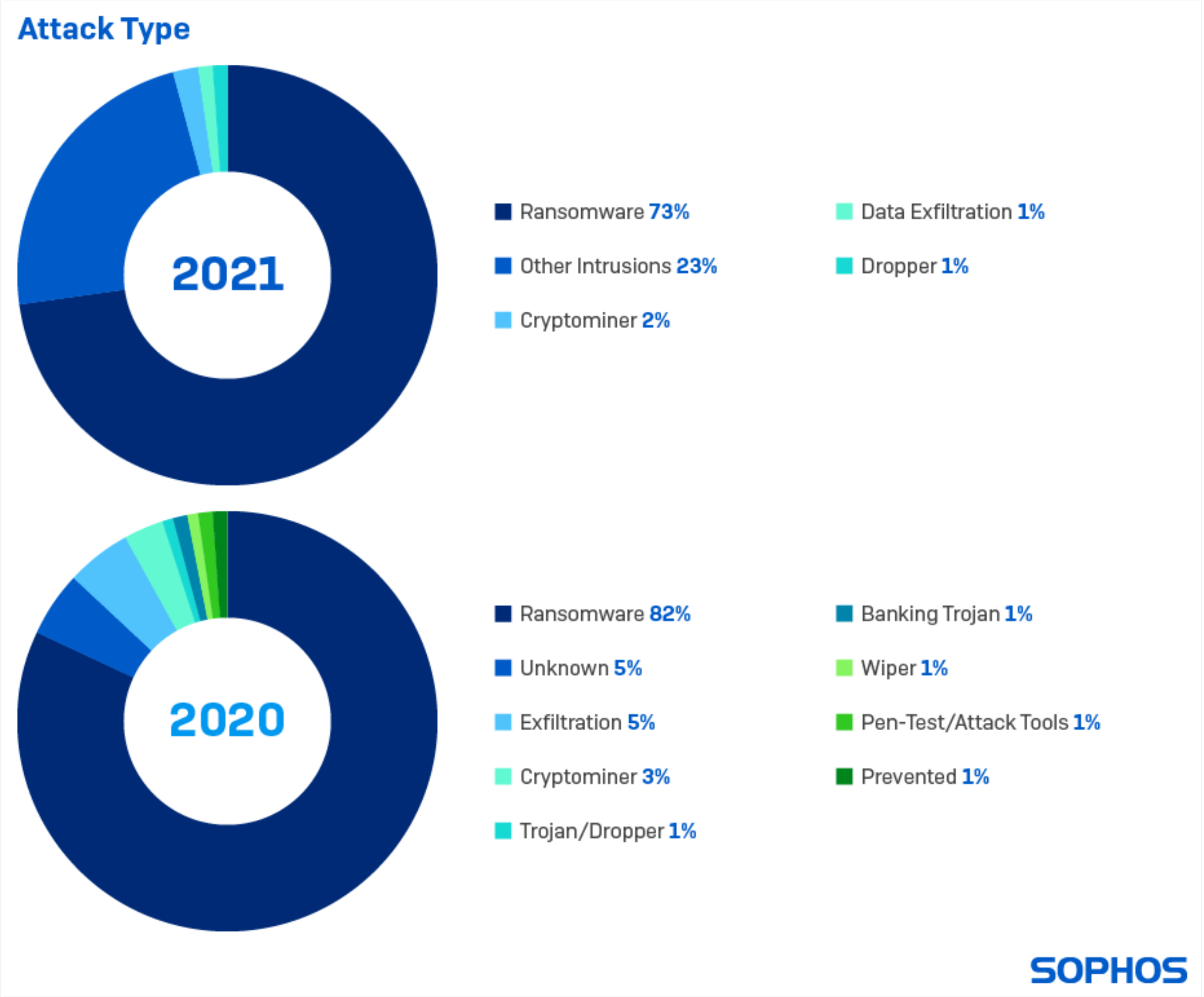
The Root Causes of Attacks

It is not always possible, or easy, to identify the root cause of 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. Despite this, the evidence shows that among the incidents investigated by Sophos, the exploitation of unpatched vulnerabilities – such as ProxyLogon or ProxyShell – were the root cause for almost half (47%) of cyberincidents investigated in 2021.



The Main Attack Types

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 73% of the incidents Sophos responded to in 2021 involved ransomware. Ransomware was also the most prevalent attack type in 2020, at 82% (the higher number likely reflecting the smaller data set). In the case of data exfiltration, accounting for 1% of incidents, the incident responders believe these would probably have unfolded into ransomware attacks but were caught and neutralized in time.



The second most prevalent type of attack uncovered by incident response investigations was the broad category of "other intrusion," which accounted for 23% of incidents. For the purposes of this report "other intrusions" are defined as intrusions that have not resulted in ransomware or other tracked attack type.

An intrusion is often the result of an exploited unpatched vulnerability, such as ProxyLogon and ProxyShell, but also includes the misuse of remote access services or insecure VPNs, stolen account credentials or security oversights (such as leaving entry points open to the internet).

The key thing is that the intrusions were detected and neutralized before a major malicious payload was delivered to the target. It is reasonable to assume that some, if not most, of these intrusions were excess inventory belonging to IABs: "banked" access that had not yet been sold to another adversary. If the intrusions had not been detected it is probable that a significant number would have gone on to become ransomware attacks.

Cryptominers were the main attack type in 2% of the incidents investigated. The presence of malicious cryptominers is often detected through their impact on system performance, as the illicit coin mining draws processing power from computers. It can be tempting to dismiss cryptominers as a lower-level, nuisance threat, but the fact that they are in the network at all proves there is a vulnerable entry point somewhere, and they can be a harbinger of more serious threats to come.

The same applies to droppers and malware delivery systems in general, which are designed to deliver, load, or install other malicious payloads to a target system. They are enablers for an unfolding attack, providing a platform for additional malicious modules such as backdoors and ransomware. Defenders therefore need to treat the presence of droppers and malware delivery systems, including Trickbot, Emotet and others, with the same seriousness as a major ransomware group since they are often the precursors to bigger attacks.

A Crowded Playground

Attack types are not mutually exclusive. As mentioned earlier, multiple adversaries, including IABs, ransomware gangs and cryptominers, can be found in an individual target network at the same time.

For instance, while cryptominers were the *main* attack type in just 2% of incident response cases, they were also present in 7% of ransomware incidents. Cryptominers often scan for and remove other miners in infected networks but can coexist comfortably with other threats, such as ransomware.

Simultaneous attack incidents reported by Sophos in 2021 include one involving Atom Silo ransomware and two cryptominers, and a dual ransomware attack involving Netwalker and REvil. This trend is continuing into 2022.

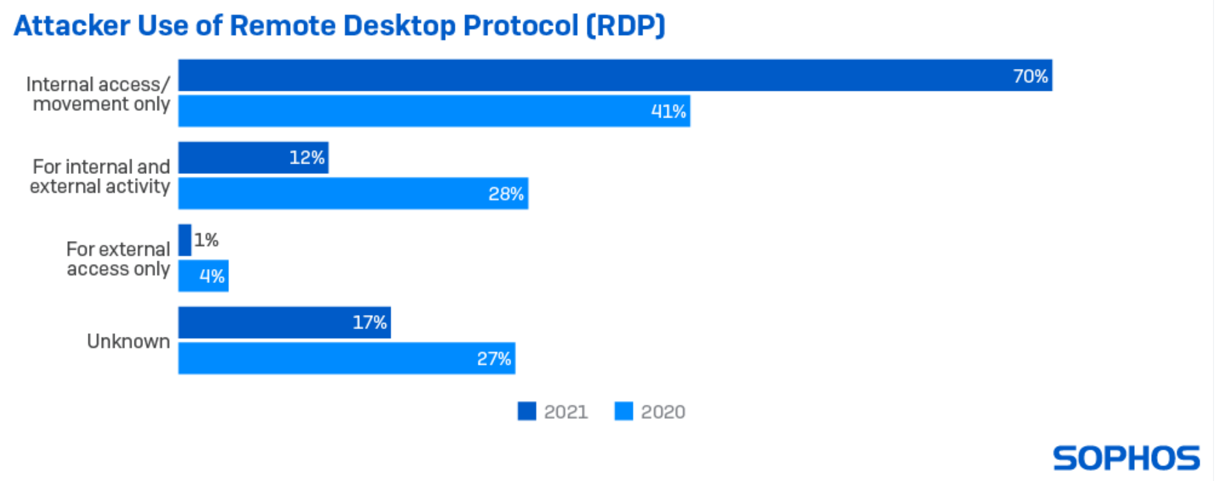
The Adversary Toolbox

Remote Desktop Services are a Major Internal Threat

RDP played a part in at least 83% of attacks, an increase from 2020 (when it featured in 73% of attacks). Internal use featured in 82% of cases and external use was seen in 13% of cases. This is against 69% and 32% respectively for 2020.

However, the way in which attackers used RDP is worth noting. In under three quarters (70%) of incidents that involved RDP, the tool was used *only* for internal access and lateral movement – a significant increase from 41% in 2020.

RDP was used for external access *only* in just 1% of cases, down from 4% in 2020; and just 12% of attacks showed attackers using RDP for both external access and internal movement, less than half the proportion from 2020 (when it was 28%).

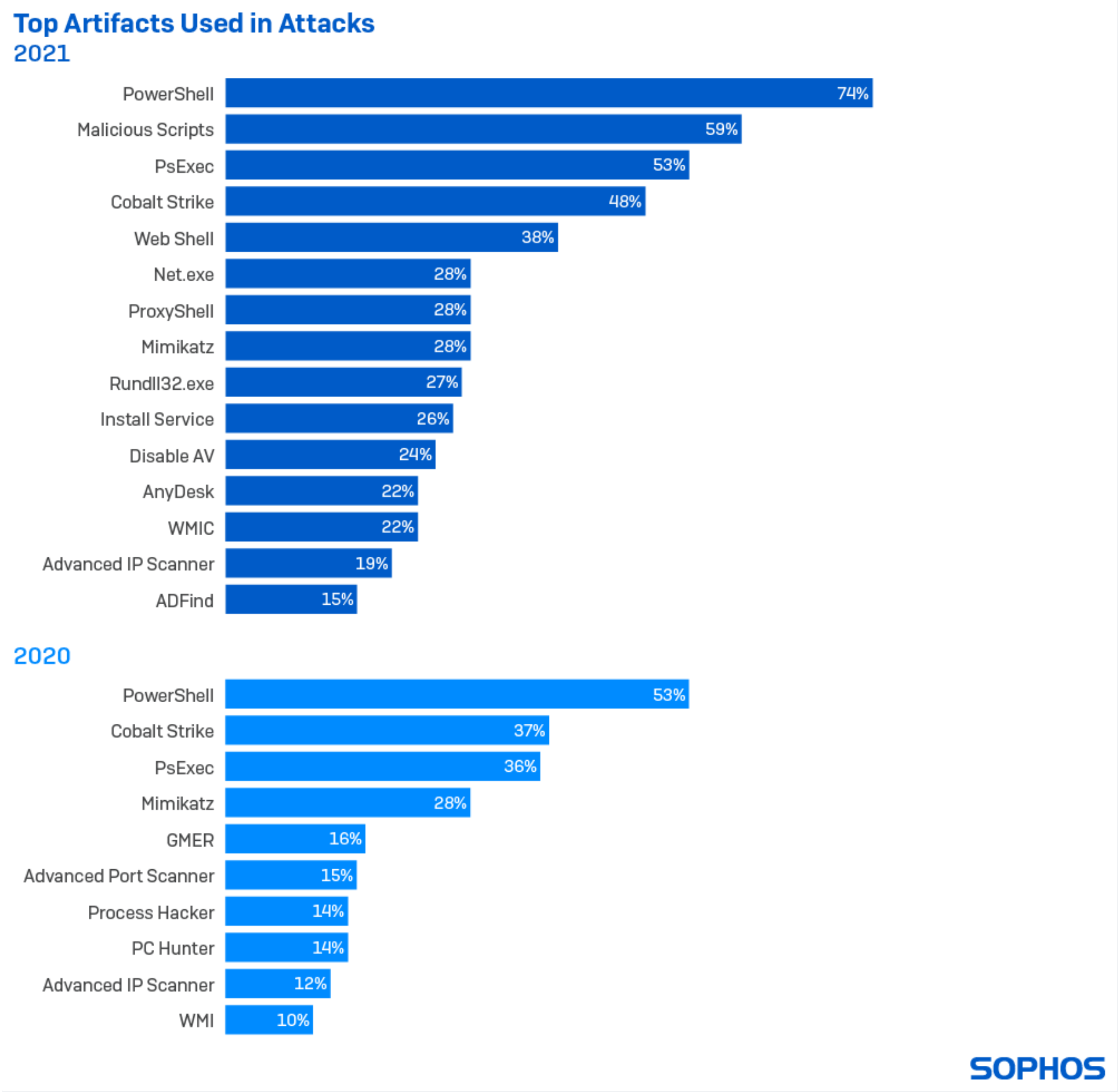


The decline in the use of RDP for external access is likely to reflect improved security, including disabling the service. However, RDP remains widely accessible inside the perimeter, and hardening this access should be a key focus for security teams.

The Attack Toolset in 2021

The chart below shows the “artifacts,” including tools, techniques, and services, most likely to be found in an attacker’s toolset in 2021. Many of these can also be used by IT professionals for benign purposes. They are popular with adversaries because they allow them to conduct activities 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 artifacts highlight the challenge defenders face in differentiating between malicious and legitimate activity on the network.



A deeper look at the most popular items used in attacks reveals the typical playbook for cyberattacks in 2021.

The Artifacts That Make Up Toolsets

The artifacts identified during incident response investigations can be divided into three categories: legitimate and hacking tools, Microsoft binaries, and additional artifacts (scripts, techniques, services, and more).

The incident response investigations found 525 different artifacts overall, up from from 132 in 2020 (although the base sample size was also larger), comprising 209 legitimate and hacking tools, 107 Microsoft binaries, and 209 additional artifacts.

Legitimate and Hacking Tools

These include software that was used to assist in an attack. Cobalt Strike (48%) and Mimikatz (28%) retain the top two spots from 2020, followed by AnyDesk (22%), Advanced IP Scanner (19%), and ADFind (15%). Compared with 2020, Cobalt Strike has increased its share (up from 37%), Mimikatz has remained steady (holding at 28%), and three new tools have cracked the top five.

Cobalt Strike is a commercially produced exploitation tool suite designed to help security teams recreate a wide range of attack scenarios. Attackers try to establish a Cobalt Strike "beacon" backdoor on an infected machine. Beacons can be configured to execute commands, download, and execute additional software, relay commands to other beacons installed across a targeted network, and communicate back to the Cobalt Strike server. Any detection of Cobalt Strike on the network should be immediately investigated.

The second most widely seen tool, **Mimikatz**, was also originally designed as an offensive security tool, and can steal passwords and other account credentials to leverage in an attack.

Legitimate network scanners like **Advanced Port Scanner** and **IP Scanner** are used to generate a list of IP and device names, which enables attackers to home in on the victim's most critical computing machines and infrastructure.

The misuse of the legitimate **AnyDesk** IT management tool is increasingly popular, as it offers attackers direct control of the target computer, including control over the mouse/keyboard and the ability to see the screen. Legitimate remote access services such as **TeamViewer**, **Screen Connect**, **Atera RMM**, and **Splashtop** also make the top cut in 2021.

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.

Microsoft Binaries

Separating Microsoft tools from generic tools shows how attackers are living off the land. These tools are all digitally signed by Microsoft. **PowerShell** (74%) unsurprisingly tops the list, followed by **PsExec** (53%), **"net.exe"**(28%), "**rundll32.exe"** (27%), and the **WMI Command-line** (WMIC) tool (22%). The use of PowerShell, PsExec, and WMIC all increased in 2021, compared to 2020.

The tool "net.exe" was used in many phases of an attack, most commonly as a discovery tool, while "rundll32.exe" was used extensively for execution and defense evasion.

Other Microsoft tools that could point to an attacker lurking in the network are **"whoami.exe,"** **Task Scheduler**(to maintain persistence), and **"schtasks.exe"** (to execute malicious code.) The use of any such tools should be closely monitored.

Additional Artifacts

This category includes both tools and techniques, such as trying to disable protection, vulnerabilities such as ProxyShell, use of cloud services such as **Mega.io**, additional malware found, secondary infections, and transport protocols used.

Malicious scripts (excluding PowerShell) were seen in 59% of the incidents investigated. Malicious scripts are software code that enable malicious activity. Examples of scripts misused by attackers include DOS/CMD batch and command line scripts, Python scripts (a collection of commands in a file to be executed like a program) and VBScripts (Visual Basic scripts that can be executed in Windows or Windows Explorer.)

Web shells were the second most common type of threat found (in 38% of incidents), with ProxyShell (28%) and ProxyLogon (11%) featuring prominently. Installing services, disabling protection, dumping LSASS, creating rogue accounts, modifying the registry, and clearing logs round out the top 10.

Data Exfiltration

In 2021, **Rclone** entered the list of top artifacts used for exfiltration. Rclone is a command line tool that connects to a wide variety of cloud storage providers, such as Mega, and in 2021 it was the tool most widely used in data exfiltration. Other cloud storage providers seen in this year's data include **Dropbox,** **DropMeFiles**, **M247**, **pCloud**, and **Sendspace**.

In addition to Rclone, tools found in incident investigations that aided data exfiltration include **Megasync**, **FileZilla**, **Handy Backup**, **StealBit**, **WinSCP**, and **Ngrok**.

The appearance of exfiltration tools in the top list in 2021 is not surprising considering the fact that 38% of all incidents investigated involved the exfiltration of data, up from 27% in 2020. A number of other incidents (8% overall) showed signs of data being collected and staged for possible removal. In cases where exfiltration took place, the evidence suggests that the stolen information was subsequently leaked in 46% of incidents.

Attackers generally remove information as the final stage before deploying the ransomware. Sophos' incident analysis shows that in 2021 the median gap between data exfiltration and the deployment of the ransomware was around 44 hours. The mean average gap was just over four days (4.28 days) and the median gap was under two days (1.84 days).

Regardless of which average is used, the important message here is that after exfiltration there is a potential window of opportunity for defenders to prevent the final and most damaging stage of the attack from unfolding. Any detection of tools known to be used in data exfiltration should therefore be investigated as a priority.

Tool Combinations

The incident investigations revealed a pattern of tool combinations on victim networks that provide a powerful warning signal for IT security teams (comparative data for 2020 was available in some cases):

- In 2021, PowerShell and malicious non-PS scripts were seen together in 64% of cases
- PowerShell and Cobalt Strike combined in 56% of cases, compared to 58% in 2020
- PowerShell and PsExec were found in 51% of cases, compared to 49% in 2020
- PowerShell, malicious scripts and Cobalt Strike were seen in 42% of cases
- PowerShell, malicious scripts and PsExec were observed in 38% of cases
- PowerShell, Cobalt Strike and PsExec occur in 33% of cases, up from 12% in 2020
- Cobalt Strike and Mimikatz were seen together in 16% of cases

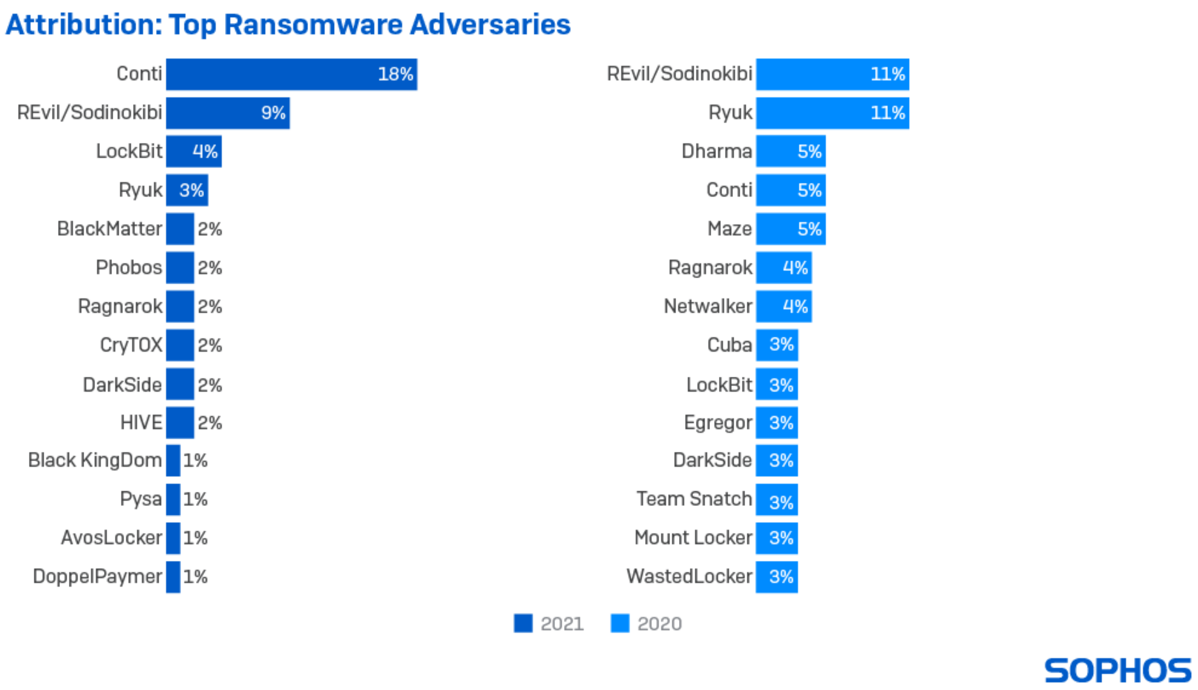
Such correlations remain as important this year as they did last year, because their detection can serve as an early warning of an impending attack or confirm the presence of an active attack.

The Main Ransomware Adversaries in 2021

There were 41 different ransomware adversaries identified across the 144 incidents included in the analysis. Of these, around two thirds (28) were new groups first reported during 2021. Eighteen ransomware groups seen in incidents in 2020 had disappeared from the list in 2021, a clear indication of how very crowded, dynamic, and complex the cyberthreat landscape has become, and how difficult this can make life for defenders.

In many ways, 2021 “belonged” to Conti, a prolific RaaS operator that was behind just under one in five (18%) of the incidents investigated by Sophos. It is worth noting, however that REvil ransomware accounted for one in 10 incidents overall, despite apparently stopping operations in July 2021 (reappearing briefly in September, 2021, and again in 2022).

Other prevalent ransomware families during 2021 included DarkSide, the RaaS behind the notorious attack on Colonial Pipeline in the U.S., and Black KingDom, one of the “new” ransomware families to appear in March 2021 in the wake of the ProxyLogon vulnerability.



Around a quarter (24%) of incidents in 2021, and 25% in 2020, were attributed to other ransomware groups, while the remaining incidents couldn’t be attributed with confidence to any known group.

Sophos has reported at length on Conti ransomware. A comprehensive list of articles on Conti and other prevalent ransomware families, including LockBit, Ryuk, and more, can be found in Sophos’ Ransomware Threat Intelligence Center.

Conclusion

Every organization is a target for an adversary somewhere, and, increasingly, for more than one. From phishing and financial fraud, to botnet builders, malware delivery platforms, cryptominers, IABs, data theft, corporate espionage, ransomware, and more – if there's a vulnerable entry point into a network, the chances are that attackers are looking for it and will eventually find and exploit it.

Until the exposed entry point is closed and everything that the attackers have done to establish and retain access is completely eradicated, just about anyone can walk in after them. And probably will.

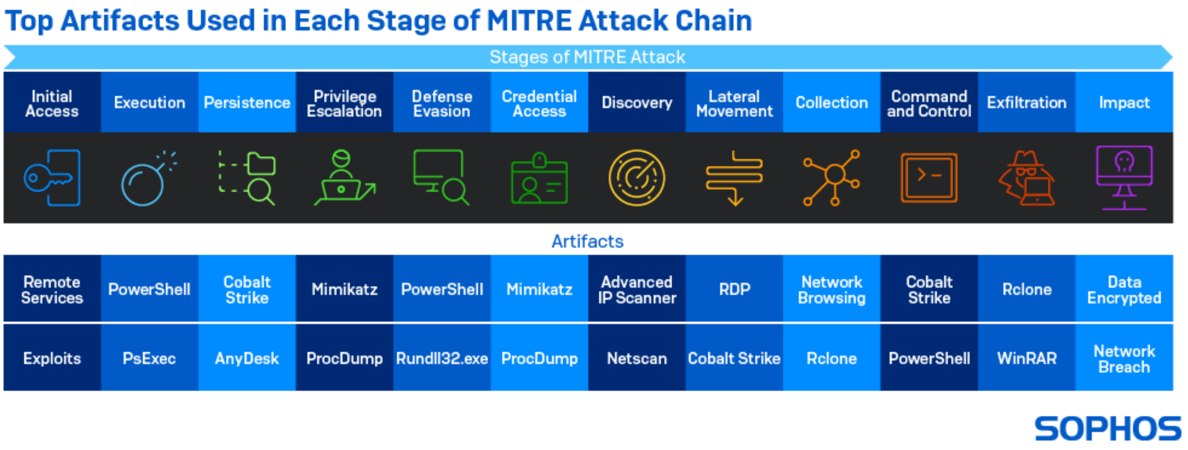
Security teams can defend their organization by monitoring and investigating suspicious activity. The difference between benign and malicious is not always easy to spot. Technology in any environment, whether cyber or physical, can do a great deal but it is not enough by itself. Human experience and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

The big incident response lessons of 2021 are how quickly and extensively easy-to-exploit, widespread vulnerabilities are seized upon by adversaries, contributing towards longer intrusions and multiple adversaries. For defenders, these lessons mean that detecting, investigating and responding to the red flags of known adversary toolsets and techniques are more critical than ever.

Additional Data Tables

Incident Investigation Artifacts Mapped to the MITRE Attack Chain

The tools, techniques, and other artifacts observed during incident investigations were mapped against the MITRE ATT&CK framework. Further details will be published in a companion article on Sophos News.



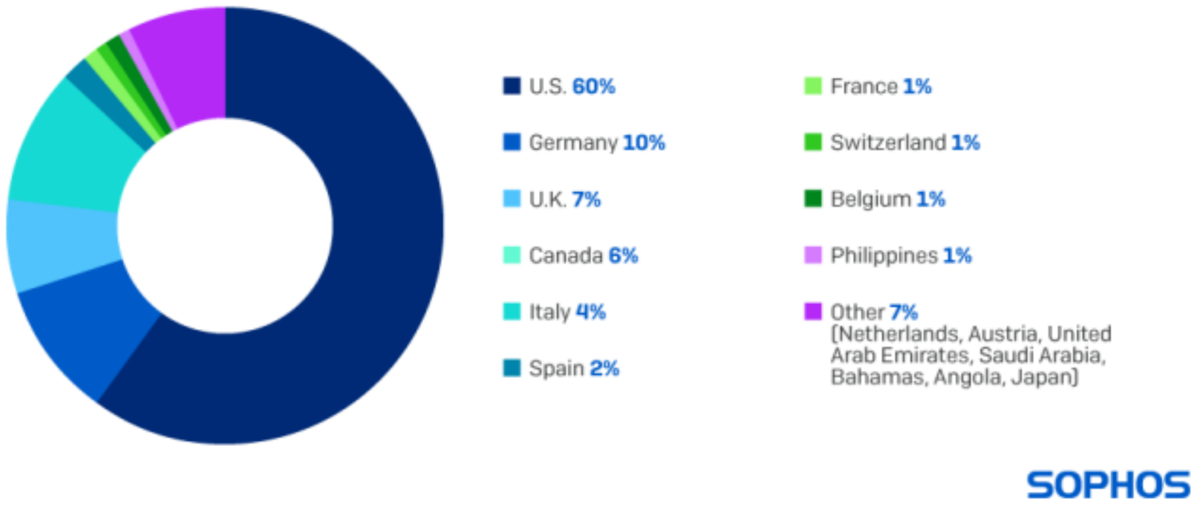
Top Artifacts Used in Each Stage of MITRE Attack Chain

Stages of MITRE Attack

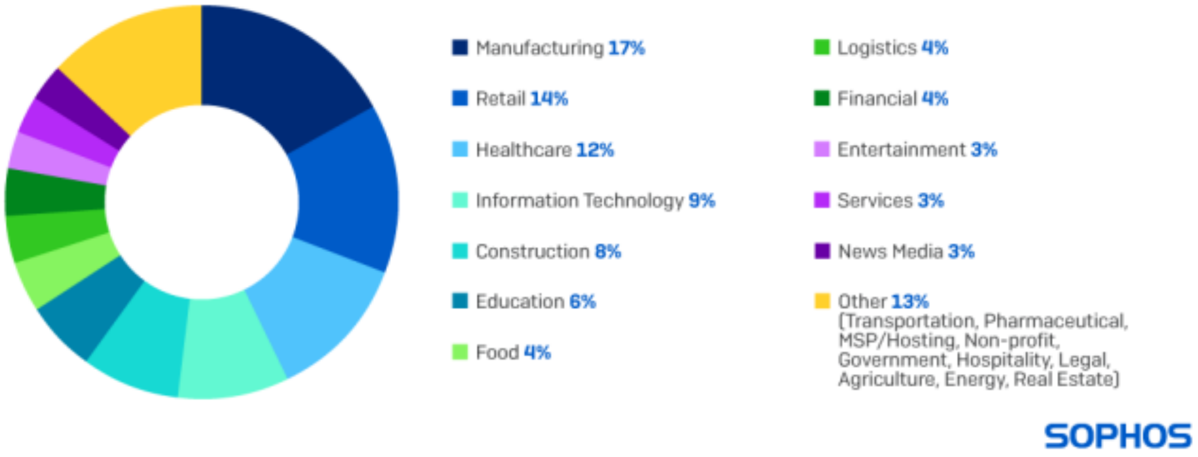
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Artifacts											
Remote Services	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Network Browsing	Cobalt Strike	Rclone	Data Encrypted
Exploits	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Network Breach

Incident Response Demographics 2021

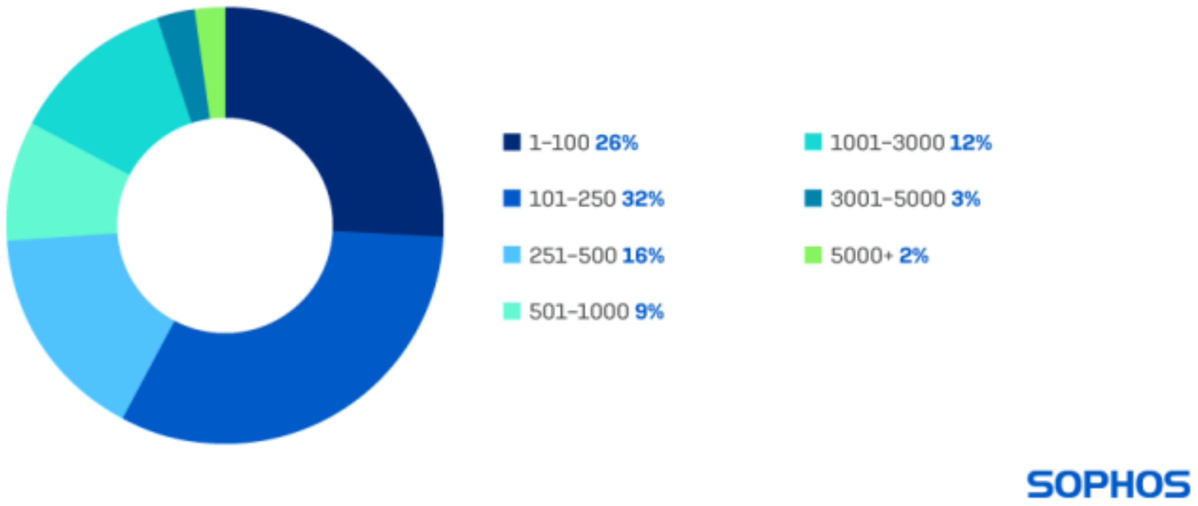
Incident Response Cases by Country



Incident Response Cases by Sector



Incident Response Cases by Organization Size (Number of Employees)



Sophos Rapid Response ***helps organizations facing an active threat to contain, neutralize and investigate the incident. You can contact Sophos Rapid Response for emergency support 24/7.***

Don't miss any important report check webpage:
https://www.cybercrimeinfo.nl/rapporten