SOPHOS

Stopping Active Adversaries: Lessons From The Cyber Frontline

Learnings for IT and business leaders based on analysis of 232 major cyber incidents remediated by Sophos X-Ops incident responders

A Sophos Whitepaper. December 2023

Setting the scene

Background

This paper shares key findings from analysis of 232 cyberattacks remediated by Sophos X-Ops incident responders in 2022 and the first half of 2023. It consolidates learnings from the three Sophos Active Adversary reports of 2023 to provide a unique window into the tactics, techniques, and procedures employed by today's skilled, professional cybercriminals.

For a deeper dive into the findings shared in this report, see:

- Active Adversary Report for Business Leaders 2023
- Active Adversary Report for Tech Leaders 2023
- Active Adversary Report for Security Practitioners 2023

The Sophos X-Ops Incident Response team

Sophos Rapid Response is a dedicated team of incident responders who specialize in stopping active cyberattacks and preventing further damage. Any organization, whether a Sophos customer or not, can call on them for expert assistance when dealing with a live attack.

The team is available 24/7/365 and consists of 50 digital forensic specialists and 35 deployment engineers who are experts at hands-on-keyboard combat.

Sophos Rapid Response is supported by over 150 analysts in the Sophos Managed Detection and Response (MDR) Security Operations Center (SOC). These analysts provide real-time insights into what they are seeing and stopping across the many thousands of customer environments that they monitor and proactively secure every day. Further supporting the team are 400 Sophos Labs malware analysts who are experts at unpacking, understanding, and blocking malicious code.

Sophos incident responders' goal is to quickly triage, contain, and neutralize active threats and eject adversaries to prevent any further damage.

Analysis of 232 incident response cases

This study spans 232 cases from 2022 and the first half of 2023 that were remediated by Sophos incident responders covering organizations across 35 nations and 25 sectors.

83% of incidents occurred in organizations with fewer than 1,000 employees. This broad scope ensures a wide representation of adversary behaviors that everyone can learn from.

Countries represented in the dataset

Active adversaries

As this report looks at attacks executed by active adversaries specifically, it is important to understand who they are and what they do.

Who they are

Active adversaries are highly skilled cybercriminals, often equipped with sophisticated software and networking skills. They are generally very well paid, and often part of a professional cybercriminal network.

What they do

Active adversaries infiltrate organizations' systems, evade detection, and continuously adapt their techniques, using keystroke and AI-based methods to bypass preventative security controls and execute their attacks. Continuous adaptation is the key. They launch an attack, see what happens, and respond accordingly. If they don't succeed the first time, they try another option and another option until they achieve their goal.

Prevalence

Despite misconceptions that active adversaries only target larger organizations, the reality is that they impact organizations of all sizes. 24% of IT leaders in organizations with 100-250 employees report that they experienced an attack involving an active adversary in the last year[1].

It's worth noting that, with the occasional exception of very high value political targets, active adversaries rarely deliberately target a particular organization. Rather, they look for organizations with gaps in their security defenses and then go in for the kill.

1 The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos - Survey of 3,000 IT leaders across 14 countries

Step 1: Initial entry

Let us start by unpacking how adversaries are getting into organizations.

Attack vectors are evolving

In 2022, exploited vulnerabilities were the number one root cause of attacks, used in 37% of cases, followed by compromised credentials, used in 30% of cases.

These findings are reinforced by data from the Sophos State of Ransomware 2023 study, which reported that 36% of ransomware attacks in the previous year started with exploited vulnerabilities and 29% with compromised credentials.

Looking deeper into the 2022 attacks remediated by the Sophos Incident Response team, over half (55%) of those that started with exploited vulnerabilities were associated with just two vulnerabilities: ProxyShell and Log4Shell - both of which had patches available at the time of compromise.

Moving into the first half of 2023, the order switched and compromised credentials was the number one root cause, used in half of the incidents remediated by the team. Exploited vulnerabilities were used as the entry method in just under a quarter (23%) of cases.

It is too early to say that adversaries have definitively changed their tactics. It may be that in the first half of 2023 there weren't as many easily exploitable vulnerabilities for adversaries to take advantage of, or that initial access brokers had a lot of inventory that they were willing to sell off cheaply. However, what is certain is that compromised credentials are readily available on the dark web, often obtained through phishing attacks or previous data breaches.

Root cause of attack

	2022	2023 H1
Exploited Vulnerabilities	**37%**	**23%**
Compromised Credentials	**30%**	**50%**

Source: The Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Lack of multi-factor authentication (MFA) leaves the door open to adversaries

One thing that makes it easier for adversaries to abuse compromised credentials is the lack of multi-factor authentication (MFA) in many organizations. Well over a third (39%) of the incidents remediated in the first half of 2023 found that the victims did not have MFA configured.

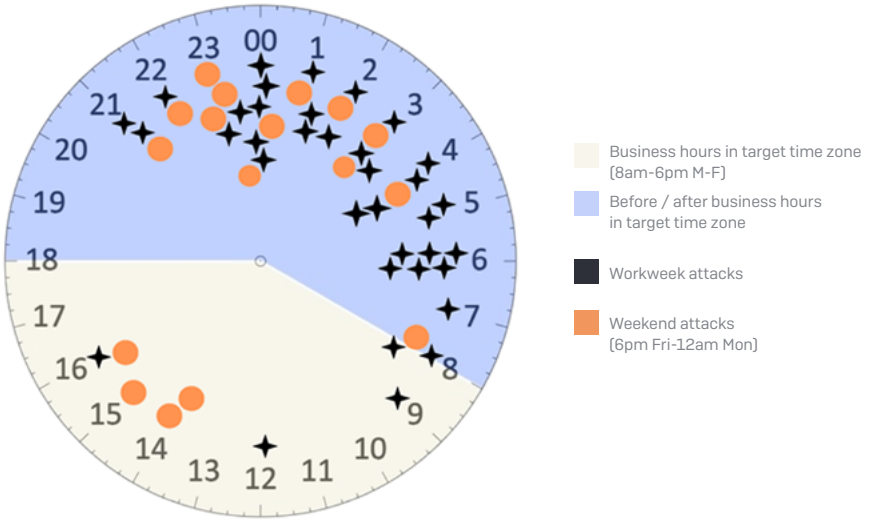
MFA is not a brand new, untested technology. It's well-established, readily available, and there's really no excuse for not having it in place. If you do not have MFA enabled, you are making it incredibly easy for attackers to infiltrate your organization.

Attackers target off-hours

Another key finding is that adversaries actively target organizations when there's a higher chance they won't be detected (for this analysis we have focused on ransomware attacks because they have the most reliable and objective indicators).

43% of ransomware attacks were launched on a Friday or Saturday in the victim's time zone. Adversaries deliberately launch their attacks on these days so that they can work on them over the weekend – when IT teams are less likely to be actively monitoring and responding to security alerts.

Diving deeper we see that 9 in 10 attacks (91%) start outside of normal working hours in the victim's time zone (i.e., outside of 8am to 6pm Monday to Friday).



The time of day ransomware attacks start

This 24-hour clock image shows the time of the attack in the victim's time zone. The orange dots are weekend attacks (6pm Friday – 12am Monday) and the black crosses are weekday attacks. The image makes clear that the vast majority of the attacks cluster between 11pm and 6am – demonstrating that adversaries are deliberately working at night.

How many people do you have actively monitoring and responding to alerts and suspicious activity outside of standard business hours? Not people who can be called up if needed, but rather analysts who are actively identifying and investigating suspicious activity? If you don't have anyone covering nights, weekends, and holiday periods, it's time to elevate your defenses.

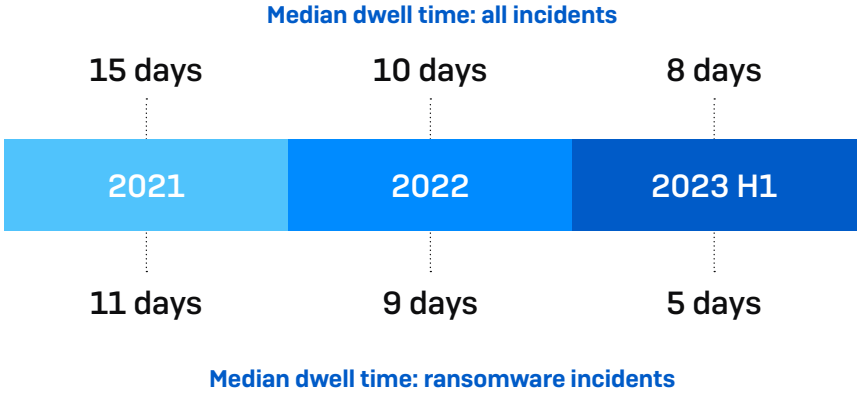
Step 2: Internal activity

Now let's unpack what adversaries do once they're inside your network - and how long it takes them.

Adversaries are speeding up

Once adversaries infiltrate your network, they move quickly. In the last two and a half years, we've seen adversaries pick up the pace. This is partially due to improvements in defense capabilities that have necessitated faster attacks. In addition, adversaries are simply getting well-practiced – the more attacks they carry out, the faster they get.

Dwell time is the time an adversary spends in your environment before being detected. In successful cyberattacks, adversaries typically remain undetected until the point at which they detonate their attack, for example, when they launch their ransomware and start encrypting files. As a result, shorter dwell time means faster overall attack execution. Dwell time also represents your opportunity to detect and neutralize an active adversary before they can achieve their goal.



Source: Active Adversary Playbook 2022, Sophos (n=144); Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

In the diagram, the top row shows the median dwell time for all types of cyber incidents and the bottom row shows the median dwell time for ransomware incidents.

- In 2021, dwell time was 15 days for all incidents and 11 days for ransomware.
- In 2022, dwell time dropped to 10 days for all incidents and nine days for ransomware.
- In the first half of 2023, dwell time shrunk yet further: eight days for all incidents and just five days for ransomware.

Combining this learning with our previous findings around attack timings makes clear the challenges facing organizations that lack 24/7 security operations coverage. If an adversary starts their ransomware attack at 9pm Friday night but you don't see the suspicious activity and alerts until 9am Monday morning, you have already lost half of your window of opportunity to detect the attacker and eject them from your environment.

Dwell time varies by attack type

Digging a little deeper, the chart below shows dwell times for several popular attack types. We've explored the ransomware number, so let's focus on a few other areas of note.

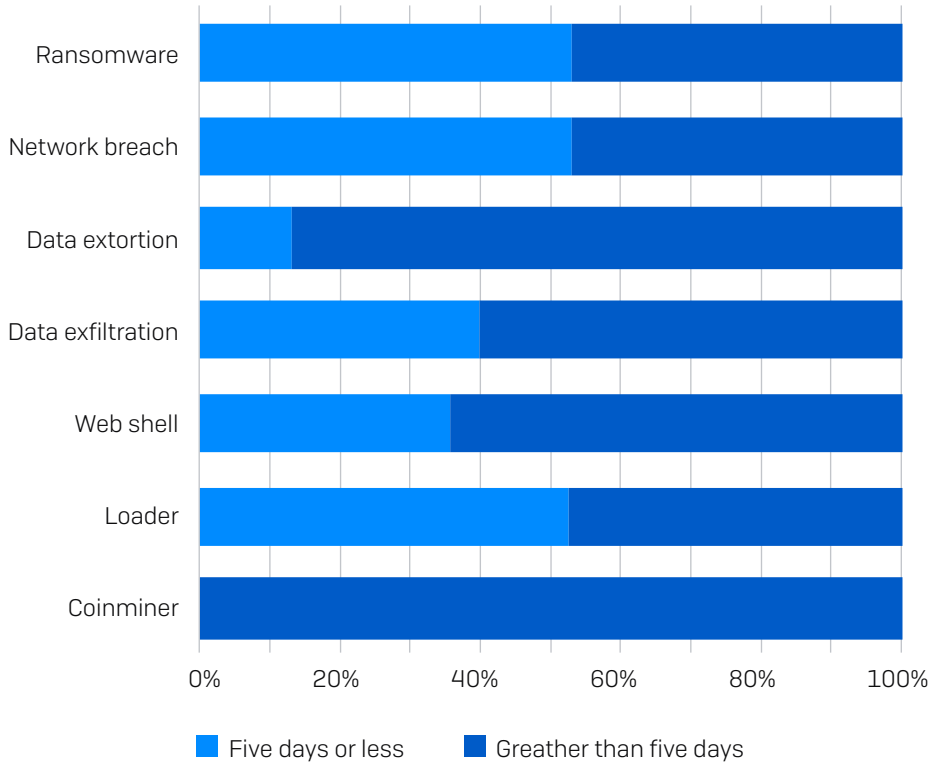
Coinminers have a very long dwell time, but they are meant to be long running. Coinminers will happily squat on a server, accruing fractions of a cent per month, in perpetuity.

Data extortion. Most, but not all, attacks fell into the "slower" attack dataset. In an extortion attack, the threat actors tended to stay on the network longer than in cases where data is simply exfiltrated, but no extortion was attempted.

It is likely that, because there is no encryption component to these attacks, the threat actors are able to operate more silently, and therefore more slowly and deliberately.

Data exfiltration is a variant of data extortion (all extortions involve some form of exfiltration, but not all exfiltrations involve extortion) and also leans slightly toward longer attacks for similar reasons. ("Data exfiltration" in our dataset indicates cases where it is confirmed that data left the affected network, but no further information is available about what the attacker did with that data.)

Dwell Time by Attack Type, 2022 -1H23



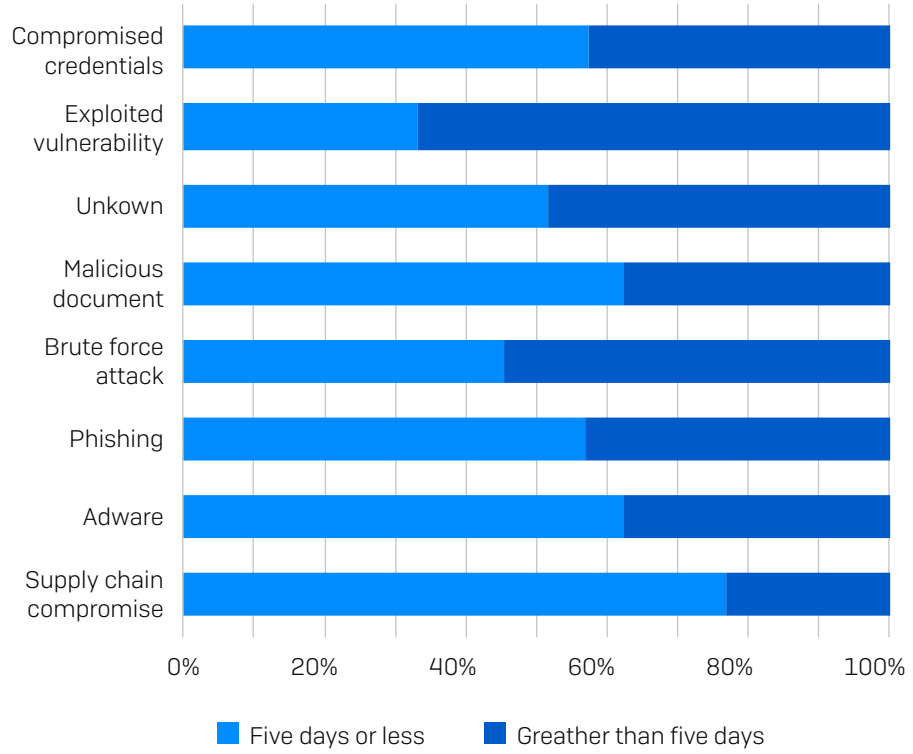
Dwell time varies by root cause

We saw earlier that the most common root causes of attacks were compromised credentials and exploited vulnerabilities. Now let's look at how dwell time varies by root cause.

In general, attacks that started with compromised credentials moved faster than those that started with an exploited vulnerability. More than half of the attacks that started with compromised credentials had a dwell time of five days or less, compared to a third of the attacks that started with an exploited vulnerability.

The notable outlier in this view of the data is supply chain attacks, where more than three quarters had a dwell time of less than five days. Supply chain compromises are the ready-made meal kits of threats: all the ingredients are provided and ready –to go, and it's just a matter of making it happen.

Dwell Time by Root Cause, 2022 -1H23



Adversaries race to Active Directory

Findings from incident analysis suggests that once adversaries get inside an organization, they make a concerted effort to move laterally to Active Directory (AD) servers as quickly as possible. In fact, the median time-to-AD for attacks in the first half of 2023 was just 0.68 days – approximately 16 hours.

Median Time-to-Active-Directory for attacks in 2023 H1

0.68 days = 16 hours

Source: Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Combining this finding with the earlier data around attack timing makes clear that AD can easily be compromised during off-hours.

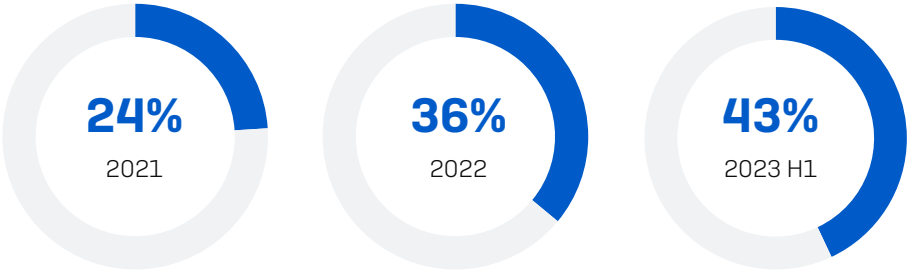
There are many operational reasons for an adversary to focus on Active Directory. Establishing a foothold on an AD server greatly enhances an attacker's capabilities. An AD server is typically the most powerful and privileged asset on a network, one that's capable of controlling identity and policies across an entire organization. Attackers can exploit highly privileged accounts, create new accounts, or disable legitimate accounts.

Attackers can also use the AD server to distribute their malware from a trusted source. Plus, when attackers get to AD, they find that most servers are protected with only Microsoft Defender, and sometimes are not running protection at all.

Disabling protection is now commonplace

In recent years, adversaries have become very adept at disabling cybersecurity protection: we now see this approach used in almost half of the attacks remediated by Sophos incident responders.

Percentage of compromises where adversaries disable protection



Source: Active Adversary Playbook 2022, Sophos (n=144); Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Living off the Land (i.e., exploiting legitimate IT tools)

Adversaries often exploit legitimate IT tools when carrying out their attacks to avoid triggering protection technologies.This chart shows the most commonly exploited legitimate IT tools (or Living off the Land Binaries to use the technical name) used in the attacks.

Top 10 Living off the Land Binaries (LOLBins) observed in the dataset

RANK	5 DAYS OR LESS	GREATER THAN 5 DAYS	RANK
1	RDP	RDP	1
2	PowerShell	PowerShell	2
3	PsExec	cmd.exe	3
4	cmd.exe	PsExec	4
5	Task Scheduler	Net.exe	5
6	net.exe	Task Scheduler	6
7	rundll32.exe	rundll32.exe	7
8	ping.exe	WMI	8
9	reg.exe	ping.exe	9
10	vssadmin.exe	whoami.exe	10

We've split them between fast attacks (five days or less) and slower attacks (greater than five days). Remote Desktop Protocol (RDP) is the number one most abused IT tool in both fast and slow attack categories, followed closely by PowerShell.

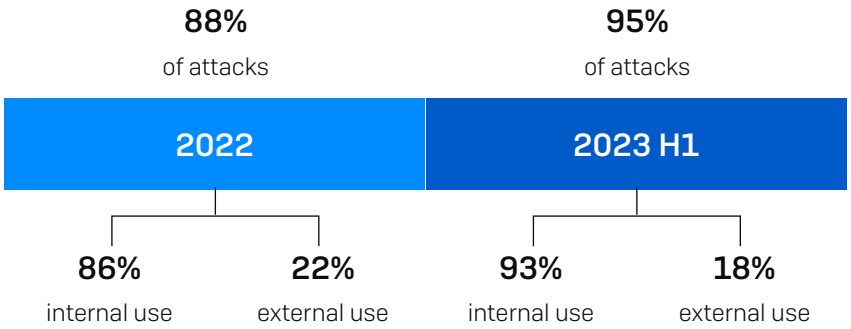
Furthermore, eight tools feature on both sides of the chart and, if we expand the list to look at the top 20 binaries, 90% appear on both the fast and slow lists.

If you see signsof suspicious activities involving these tools, investigate without delay.

Ubiquity of RDP in attacks

As evidenced by the chart below, adversaries love to use RDP. In fact, in the first half of 2023, RDP played a role in a staggering 95% of attacks, an increase from 2022, when it played a role in a previous all-time high of 88% of attacks.

Use of RDP in attacks



Source: Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Many people think of RDP as a way for adversaries to get into organizations. And that's true - they do use it for external access. But most often, they use it to advance their attacks once they are inside.

In the first half of 2023, RDP was used for internal movement in 93% of incidents and externally in 18% of incidents. This compares to 86% and 22% respectively in 2022.

As the data makes clear, there were a number of incidents where RDP was used for both internal and external access. However, it is rarely used for external access only - both in 2022 and in the first half of 2023, RDP was used solely for external access in just 2% of cases.

This means that if you only focus on looking for RDP abuse as a means to infiltrate your organization, you're missing the main adversary use case.

Removing the evidence

Another common approach used by active adversaries is to remove evidence of their activities in order to cover their tracks. In 82% of cases where telemetry logs were missing, cybercriminals had disabled or deleted it.

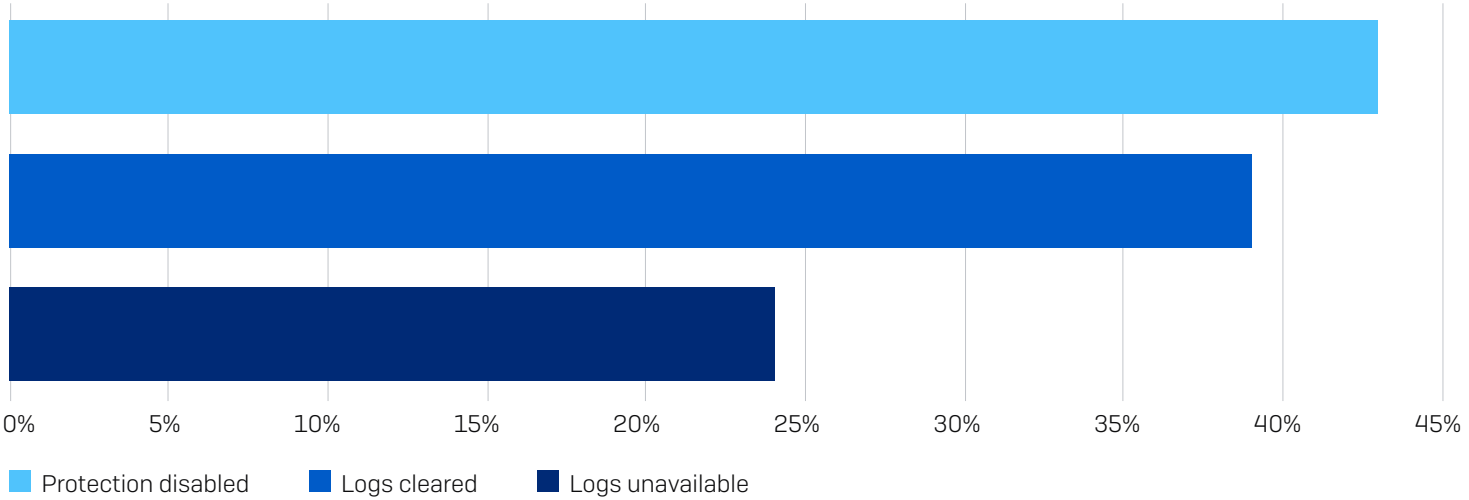
Time is of the essence when responding to an active threat: the time between detecting the initial access event and fully mitigating the threat should be as short as possible.

The further along in the attack chain an attacker gets, the bigger the headache for responders. Missing telemetry only adds time to remediation that most organizations can't afford. That is why complete and accurate logging is essential.

Now that Microsoft has begun making logging free and available for basic licenses (as of September 2023), there's no reason for your organization to not take full advantage of it.

And like many other types of data, logs should be securely backed up so that they can be used in the event that forensic analysis is required.

Causes of Missing Telemetry, 1H23



Reasons telemetry was not available to investigators from incidents in the first half of 2023.
As more than one reason can be true in any given attack, the percentages add up to over 100 percent

Key takeaways for defenders

Based on the insights from incidents remediated by Sophos incident responders, we recommend adopting the following steps to help enhance your resilience against active adversaries.

Increase friction for attackers wherever possible

If your systems are well maintained, attackers have to do more to subvert them. This takes time and increases the window of detection. Fancy techniques like "bring your own vulnerable driver" (BYOVD) attacks are fourth or fifth on most attackers' list of options – after everything else fails and they have to go nuclear.

Robust, layered defenses, including automated, adaptive protection creates friction for attackers and increases the skill level they need to bring to the table. Many simply won't have what it takes and will move on to easier targets.

Protect everything

Attackers will take advantage of any weak spot they can find to penetrate your environment and then move around as they escalate their attacks. Make sure your entire environment is protected – you're only as strong as your weakest link. Plus, strong defenses also provide valuable telemetry, which can help to accelerate threat detection and response.

Maintain 24/7 vigilance

If you're only doing security operations during working hours, you'll miss important signs of adversary activity until it's too late.

Be ready to investigate and respond promptly

Having a response plan is important, but you also need to be ready to respond promptly. Timely response can mean the difference between cleaning up a nuisance issue and rebuilding your entire environment from backups. Be sure to have response plans for the types of attacks most likely to affect your organization and practice implementing them with both your security practitioners and the other company stakeholders on whom you'd need to rely in a crisis.

How Sophos can help

Sophos X-Ops

Sophos X-Ops brings together deep expertise across the attack environment to defend against even the most advanced threats. The team publishes materials designed to provide expert insights and advice that helps defenders secure their organizations.

Resources published by the X-Ops team can be accessed by visiting news.sophos.com/category/threat-research/.

Alternatively, you can follow X-Ops on X with the handle @SophosXOps. The team utilizes the same handle on InfoSec Exchange.

Sophos services and products

Sophos has a range of best-in-class solutions designed to detect and stop active adversaries in their tracks. These include a 24/7 managed detection and response service, adaptive endpoint protection, and incident response support.

To learn more, start a free trial or speak to our team.

For more information on Sophos solutions click here

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2023-12-15 (WP-NP)

SOPHOS