



Practitioner's Guide to Monitoring Stealer Logs

By Flare Research



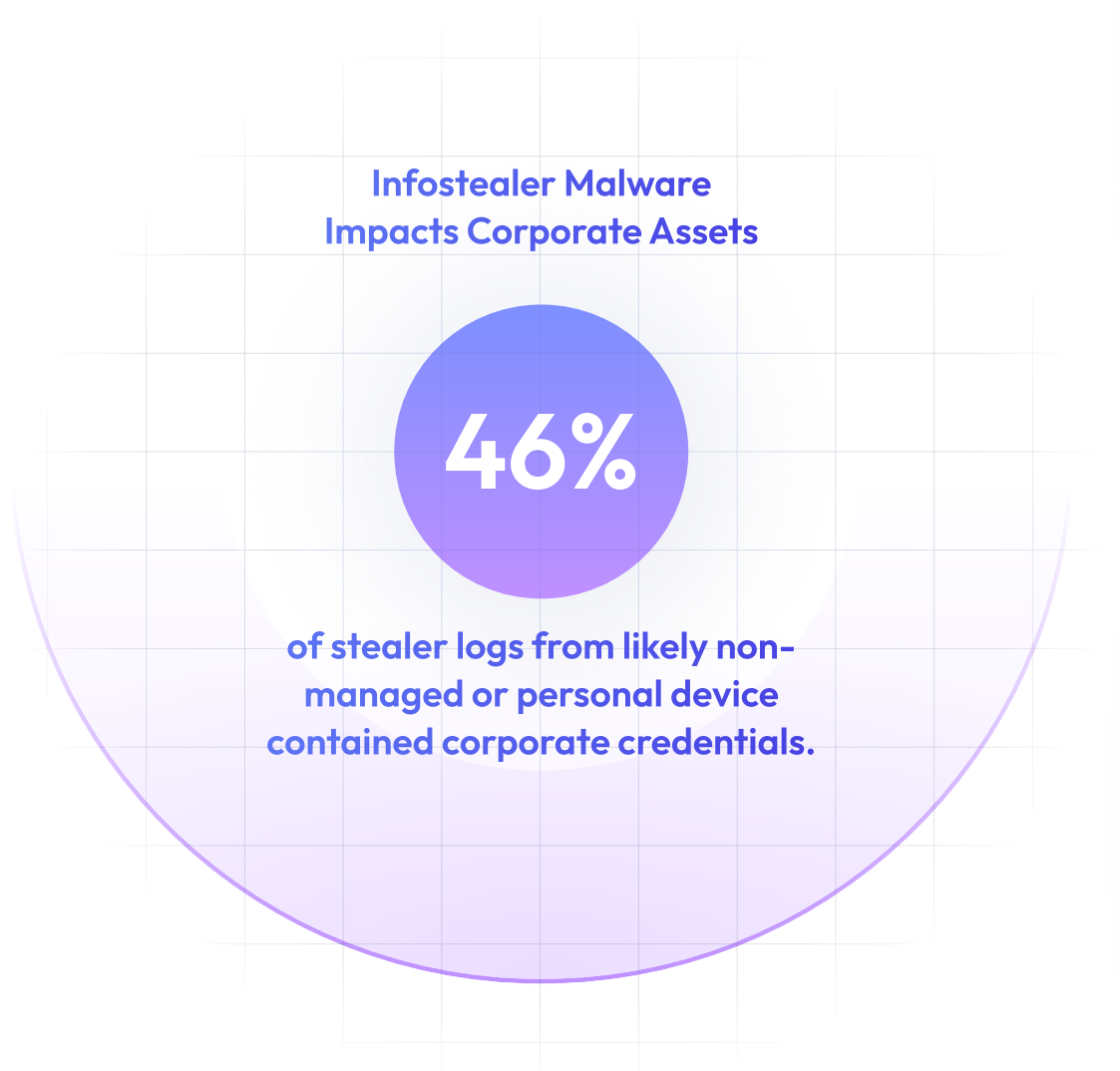
**Most guides tell you what information stealer logs are.
This is a practitioner's guide about monitoring stealer
logs and using them to better protect your environment.**

The intention of this guide is to act as a resource, but not to instruct practitioners on what to do. This reflects the reality that every organization is different in terms of their risks and requirements.

According to [Verizon's 2025 Data Breach Investigations Report \(DBIR\)](#), stealer logs enable corporate account takeovers and represent an external, unmanaged risk to organizations. Approximately 46% of stealer logs with corporate credentials are from likely non-managed or personal devices.

Flare Research found that exposed credentials and sessions of large productivity Software as a Service (SaaS) and cloud tools are growing at an estimated 29% annually.

Not all stealer risk matches an organization's size, even smaller firms are targeted.



1 The Challenges Around Monitoring Stealer Logs

One of the most significant challenges you face working with stealer logs is the sheer scale of the information that's out there. This is a classic example of the axiom in cybersecurity: attackers only need to be right once; you have to be right all the time.

Successful attacks leveraging stealer data only need one set of valid credentials, typically a single line out of a stealer log, to gain a foothold.

Preventing these attacks before they happen requires finding that one line in that one log. That single line could be hiding among tens of millions of entries, across millions of logs updated every week.

It's not looking for a needle in a haystack, it's looking for a single specific needle among millions of needles in millions of haystacks.

Another challenge in finding stealer data is where you go to find it. The forums and channels where stealer data is bought and sold are in some of the darkest corners of the dark web. Going to these locations to find this information represents serious security and legal risks; it isn't something to be undertaken lightly.

This challenge of "where to go" has intensified as the landscape shifted. Our research shows that approximately 90% of logs now appear on Telegram rather than traditional dark web markets, fundamentally changing both where defenders must look and how quickly they need to act.

Finding stealer data is only the start of the process. Once you find that data, you have to validate if what you've found is something that truly poses a risk to your organization. Not every piece of information in a stealer log is useful to attackers or a risk to you.

Information that's useful to attackers isn't binary: there are degrees of risk. Broad access to privileged systems represents an entirely different order of magnitude from access to a single low-value resource. Once you've found the information and validated it, you then have to prioritize it based on the contextualized risk it represents.

Time pressures compound everything. Stealer log information goes stale quickly: session cookies expire, credentials change, defenders (hopefully) detect and remediate. The pressures of time and speed are borne out in the data. According to Verizon's DBIR, stealers and ransomware are closely linked. On average, stolen credentials tied to ransomware victims surface just two days after the attack is publicly disclosed, giving security teams an extremely narrow window to act. And this is not a problem confined to smaller or less-resourced organizations. Models project [enterprise identity](#) exposure reaching 15–16% of all stealer infections by late 2026 under baseline assumptions.

Practitioners navigate all these challenges of scale, validation, and prioritization with limited time.

2 The Importance of Understanding Your Risk Profile in Context

When we talk about monitoring stealer logs, there's an important risk element that's frequently overlooked: understanding your organization's risk in the broader context of attackers and their goals.

When we talk about identity and access, no organization is an island. Organizations are interconnected. One organization's breach can easily become a partner's compromise. Your organization can be on either side of that equation.

Before moving forward in the following sections, it's strongly recommended that you first understand your full risk in context and apply it throughout this process.

In practical terms, this means your organization may be small and seem uninteresting to attackers, but if you have close relationships with larger, more strategic, and attractive targets, you inherit their risk profile by virtue of that connection.

A recent example of "inherited risk" is the [theft of information belonging to one of the world's largest and oldest automakers](#) that occurred after [the attacker targeted a small law firm working with them on a specific project](#). [The attacker found the law firm's information in stealer logs](#). The law firm itself wasn't the ultimate target, their client was. The law firm's risk profile wasn't based simply on itself but on who it was connected to: it inherited its customer's risk.

Another way context can affect your risk is when you have information or access that is disproportionately valuable in terms of quantity or quality. An example of this is the classic risk third-party technical support companies face. Third-party technical support companies have privileged access and information for their customers because they need it to do their work. Third-party support companies hold privileged access to many high-value clients in one place, making them an extremely attractive target for attackers looking to maximize the impact of stolen credentials.



3 Building Your Monitoring Program

With a fuller, contextualized understanding of your organization's risk, you can build out your stealer log monitoring program.

One key thing before starting: documentation is key throughout this process. Documentation makes processes scalable and repeatable so that others can pick up and contribute to the work.

The first step is identifying where to find stealer logs.

3.1 – IDENTIFYING AND PRIORITIZING SOURCES

Currently, there are two primary places to go hunting for stealer logs:

Telegram Dark web marketplaces like XSS, Russian Market, and others

There are several reasons for Telegram's ascendancy:

1. **Speed:** Telegram enables faster, more real-time transactions compared to more static forums.
2. **Freshness:** The speed of Telegram enables information to be posted, sold, and used more quickly, addressing the time-sensitivity for attackers' risks we discussed.
3. **Law enforcement takedown activity:** Law enforcement actions against specific forums and sites like [RAMP](#) and XSS show how these sites face risks around takedowns and disruptions that Telegram hasn't faced.
4. **Advantages of Telegram channels:** The way Telegram is structured as an application makes it particularly attractive and useful for the stealer log trade.
 - **Public channels:** Sellers can provide samples and advertisement logs in a public space to reach as many potential customers as possible.
 - **Private VIP channels:** Sellers can sell premium logs, often for US\$200-500/month for access in a more secure, invite-only environment.
5. **Network effect:** In a classic example of the network effect, the more Telegram is used for stealer log sales, the more it's used for stealer log sales. The network effect reinforces Telegram as the known "go-to" destination for stealer logs.

While Telegram dominates the stealer log marketplace, there are also dark web marketplaces for stealer logs. Some of the best know and most useful [Russian-speaking cybercrime forums](#) for stealer logs include:

XSS.is Exploit.in WWHClub RuTOR LOLZTEAM Dark Money PROBIV DUBLIKAT

Telegram is the primary marketplace over dark web marketplaces. However, every organization is different, and if you have specific intelligence indicating dark web marketplaces that focus on your organization, sector, or industry, make adjustments appropriately.

You can carry out this monitoring through [Flare](#) without incurring the security, operational, and legal risks of visiting directly. Direct research is possible, but outside the scope of this guide.

3.2 – WHAT TO MONITOR FOR

Knowing where to look is only half the equation. The other half is knowing what you're looking for when you get there. Below is a list of things to look for in stealer logs in recommended order of priority.

Domains and subdomains

Enterprise identity providers

Session cookies and credentials combinations

VPN/RDP access credentials

Cloud console access

Check out a [sample of what stealer logs look like here](#).

3.2.1 – Domains and Subdomains

Focusing monitoring on domains and subdomains is recommended as your top priority to find quickly what you care about most. Including not only your organization's domains and subdomains but those of partners and customers is prudent to ensure you're covering your full risk exposure. Attackers can and do target attacks through weaker, less protected partners.

Depending on how organizations are structured, domain and subdomain information can also help with the triaging process. For example, if you find an entry for "finance.company.com" that can tell you immediately you're looking at a more serious risk scenario than an entry for "testserver.company.com."

3.2.2 – Enterprise Identity Providers

[Enterprise identity provider \(IdP\)](#) credentials represent the broadest exposure of multiple risks because it's a single point of failure. Unlike other credentials that give access to a single application or service, these credentials can give attackers access to all applications that use that identity provider. In most situations, this effectively means all the organization's applications and services since the goal of single-sign on (SSO) is to enable one set of credentials to access all applications and services.

For your program, you'll want to ensure that you're looking for the provider(s) you use for your organization, as well as providers your organization uses with your partners and customers. For example, if you use Entra ID in your organization but use Google Cloud with a partner, be sure to look for both.

The top four providers are: [Microsoft Entra ID \(formerly Azure AD\)](#), [Okta](#), [AWS IAM/IAM Identity Center](#), [Google Cloud Identity](#). However, there are many enterprise IdPs out there, and you'll want to focus monitoring for the specific providers used by the organizations you're monitoring for.

3.2.3 – Session Cookies and Credentials Combinations

When stealers infect devices, they attempt to capture both session cookies and saved credentials. Understanding how these work together explains why finding both in the same log entry represents a greater risk than credentials alone.

Stolen credentials alone still require an attacker to authenticate. That authentication attempt can be logged, enabling detection and possible blocking by defenders.

With a session cookie, the attacker bypasses that risk entirely. They already have the authorization they need and can use it directly in a replay attack using the session cookie: there is no authentication required.

The combination of both session cookies and credentials is particularly potent because it gives attackers the means to carry out attacks using the session cookie and renew those attacks using the stolen credentials after the cookie expires.

Cookie lifetime matters here. The shorter the lifetime of the cookie, the shorter the attack window using it, but it also leads to user frustration with more frequent re-authentication prompts.

When MFA isn't present, attackers can renew their access using those stolen credentials. The credentials are the fallback that enable the attack to continue after the cookie expires.

Where MFA is in place, in most cases the valid session cookie bypasses it because the MFA trigger was cleared when the cookie was issued. However, MFA does limit the attacker's ability to renew access once the cookie expires, since re-authentication will trigger MFA again.

3.2.4 – Remote Access Credentials (VPN/RDP)

Another priority for your stealer log monitoring should be remote access credentials like Virtual Private Network (VPN) and Remote Desktop Protocol (RDP) credentials.

Remote access credentials can be used to gain access to your networks or systems. As such, they're very attractive to attackers and another valuable piece of information they look for in stealer logs.

When monitoring for remote access credentials, you can look for specific hostnames for remote access connection points in your environment (e.g., vpn.company.com) as a starting point.

3.2.5 – Cloud Console Access

"Console access" is another form of administrative access, sometimes also called "admin" or "root." Regardless of the specific term, they all mean the same thing: complete, unfettered privilege and control of the resource.

Cloud console access specifically is an administrative privilege and control over cloud resources. This access comes in two specific forms:

Login credentials for human users

API Keys and tokens for applications

Both are useful to attackers, stealers go after both; it makes sense to prioritize looking for both in your monitoring.

The differences between the two will be relevant to your monitoring. Each of these look differently in stealer logs. Login credentials will generally be easier to monitor: you can look for credentials for specific privileged users tied to specific cloud specific hosts (e.g., admin@company.com and app.cloudcompany.com).

API keys and tokens will be much more specific to the apps in question. Conferring with the builders and maintainers of your apps that use cloud API keys and tokens can help you understand what to look for.

3.3 – SETTING UP DETECTION PARAMETERS

With this understanding of what to look for and how you should prioritize it in your monitoring, it helps to discuss some tips and guidance on setting up parameters in your detection.

Here are three specific detection parameters to consider in your monitoring:

- 
- ☒ **Domain-based searches:** Domains and subdomains are recommended as the top priority for your monitoring. You can monitor for specific exact matches as well as substrings. Another element to consider here are specific hostnames for remote access points, critical systems, or other high value, high risk assets.
 - ☒ **Email pattern matching:** Similar to domain-based searches, you can focus on looking for specific high-value, high-risk accounts. This is also a good way to catch personal devices that are using your organization's credentials.
 - ☒ **Infrastructure identifiers:** Similar to domain-based searches, you can focus your monitoring on information that is specific to your environment. Some examples are machine names, tenant IDs, and organization-specific subdomains (especially those that serve as a bridge between your organization and others').

4 Separating Signal from Noise: A Triage Framework

We've covered where to look and what to prioritize looking for in stealer logs. Next comes building a process for what to do once you think you've found something actionable.

It's recommended that you plan to review and update your triage process regularly. Both at a regular calendar cadence (e.g., quarterly) and after major incidents.

We propose you consider a simple three-step triaging process:

1. Perform the initial assessment
2. Score the potential risk against criteria
3. Validate the threat

The results of the triage process will enable you to determine whether to move the potential issue on for further investigation and at what speed and severity.

4.1 – PERFORM THE INITIAL ASSESSMENT

When your stealer log monitoring uncovers a potential issue, an initial assessment gives you information you can use to score the potential risk it poses to your organization. This is something you want to do right away, in the first 60 seconds, given the potential risks.

It's recommended that you use your monitoring prioritization to inform your initial assessment. For example, continuing an earlier example, if your prioritized monitoring turns up a hit for "finance.company.com" you can give it a higher risk score in the next step than if you found "testserver.company.com."

In addition to the information from prioritized monitoring, additional elements you can assess for risk scoring include checking:

- **The stealer log metadata:** Does the metadata itself tell you anything you can use? Examples of information include when the data was stolen, where the stolen information is coming from and what operating system is involved. This information can help you understand more about the attack.
- **Scope of credentials in the log:** How many of your organization's credentials are in this log? Only one set of credentials can indicate a single event, many can indicate a broader, systemic attack.
- **Session cookie presence:** Does the log include active sessions? Active session cookies represent a particularly high risk since they can be used for replay attacks.

Remember, this is an assessment for triage, not a full investigation. You're aiming to gather information to fill out a matrix like below.

4.2 – SCORE THE POTENTIAL RISK AGAINST CRITERIA

The purpose of scoring the potential risk against criteria is to take information from the triage phase and use it to determine the priority of moving forward into validating the issue and launching an investigation and possible remediation.

Below is an illustrative, basic framework you can use to build your own risk scoring matrix based on your needs, policies, and procedures. The examples are specifically designed to illustrate possible ratings, your matrix may vary. Use this to set severity, note the criteria triggering that severity, set the SLA response time, and note the risk. For more details, check out the [NIST cybersecurity framework](#).

SEVERITY	CRITERIA TRIGGERED	SERVICE LEVEL AGREEMENT (SLA) RESPONSE TIME	RISK
Critical	Enterprise identity credentials + session cookies	<1 hour	Possible immediate MFA bypass
High	VPN/RDP access + multiple corporate credentials	<4 hours	Lateral movement potential
Medium	Single corporate SaaS credential without session cookies	<24 hours	Access to specific resources but limited in scope
Low	Consumer credentials on personal device with no other indicators	<72 hours	Security hygiene risk, pointer to possible other issues

4.3 – VALIDATION TECHNIQUES

The final step in triage is to validate the potential issue. As this is a triage phase, the goal is NOT to completely investigate the issue, it is to determine if the issue is valid enough to warrant moving on to the investigation phase where more resources can be spent on a fuller investigation. Issues that move on to investigation from triage can and do end up being non-issues sometimes: that is not a failure of triage and shows the investigation process is working.

The goal in triage is to eliminate obvious non-issues and assess the risk of potential issues appropriately to move them on with the right prioritization like we've shown with the risk scoring.

This final validation serves as a proverbial "sanity check" to help you make a final assessment of the validity of the issue and the SLA response time you've assigned it.

Below are some suggested validation checks you can consider. Once again, you should adapt for your specific needs.

- **Determine if the information has been used in attacks:** cross-reference with your IDP logs for failed and/or successful authentication attempts with the information you've found.
- **Determine if the information is stale and possibly useless for attackers:**
 - Check the last password change date, if the password has changed already, it's likely invalid.
 - Check the session cookie age assessment: if it has expired, that session cookie is likely unusable.
- **Compare geographic information:** Check geographic information in the stealer log and compare with the employee's location: information in the log that points to known areas of threat actor activity, points away from locations where your organization is or travels, or shows multiple employees outside their expected locations can all be pointers to malicious activity.

5 Investigation Workflow

Once an issue has been validated in triage and assigned an SLA response time, you're ready to move forward on the investigation itself.

Below are some recommended practical steps to follow in your investigation. The goal in the investigation is to gather enough information accurately and quickly to inform the next "Response" phase where you take action.

Key elements in any investigation include:

Analyzing the log and extracting information

Scoping the compromise

Determining session cookie viability

Identifying attack attempts

5.1 – ANALYZING THE LOG AND EXTRACTING INFORMATION

This initial step of the investigation builds on and extends work from the triage. In that stage, you gathered enough information to perform triage, and in this stage you're focused on more thorough analysis and data extraction.

It is important to think of this phase as an iterative one. Investigations are not simple linear processes. Sometimes, information from a later stage will bring you back for new analysis and extraction.

Good investigations don't rule anything out for analysis and extraction: the below are meant to be a starting point, not an ending. You can and should follow the investigation where it takes you.

1. **Browser fingerprint data:** This information can be useful for session cookie replay detection, where attackers are using already-valid cookies for access. This can be a pointer to an active, in-progress attack.
2. **Saved credential inventory:** This information is useful in the next stage of the investigation by giving you the full scope of stolen exposure in this stealer log.
3. **System information:** We mentioned operating systems during triage, this is a deeper, more thorough look into what system this information is coming from. In addition to helping identify if this was a personal system or your organizations, it can also help identify issues like unpatched systems in your environment.
4. **Additional artifacts:** This is a broad category and can include things like cryptocurrency wallets, VPN configurations, SSH keys and other information that the stealer has taken. Each specific artifact you find should raise these questions: Is this applicable to my environment? How can an attacker use this information to further their attack?

5.2 – SCOPING THE COMPROMISE

This process extends the work done in triage and the previous step to more fully understand the full scope of what's happening and at risk. In this step, you're seeking to answer "what is the potential impact," so you can use that to direct the response process.

1. **Identify the employee from email, username or other information:** You may have already done a preliminary identification, but at this point you want to do a full and complete identification. This is necessary not just for this investigation but also for any legal, regulatory, or human resources actions that may need to be taken later. Be sure to carry this step out in accordance with your organization's privacy policies.
2. **Determine affected user's access:** This is a key step in understanding what's at risk. Understanding what systems and data were potentially impacted is absolutely critical in differentiating a minor incident from a major one.
3. **Check authentication logs for suspicious activity:** This is one of the largest steps in an investigation because being thorough can involve accessing authentication logs from multiple systems. Your guide for what to look at will be information from step two—what systems they have access to. Information from analyzing the log and extracting information steps two and four also will provide guidance on possible systems you need to check logs on. If faced with a large list to check, you should engage in a separate specific triage and prioritization exercise for those logs so you can review the most critical ones soonest.
4. **Determine infection vector:** This is a step focused less on the specific risk posed by the information in the log and more by the possibility that the means by which this information was stolen is affecting your organization more broadly. In this step, you're seeking to understand if it was a personal device or one of your organization's endpoints, was it a single event, part of a larger event, or even part of a larger coordinated event. This information is useful for guiding the broader response and shape remediation plans to ensure no additional attacks succeed.

5.3 – DETERMINING SESSION COOKIE VIABILITY

We've talked about the risk that session cookies represent: depending on the session cookie's lifetime, it may represent an active "open door" to the resources it has access to making it a "clear and present danger" for your organization. We've already recommended checking for active session cookies during triage. At this stage, a more thorough check on session cookie viability makes sense. Given the risks around session cookies, making this focus on session cookie viability specifically is highly recommended early in the investigation. Three things to look for around active session cookies:

- **When does the session cookie expire:** this is helpful for understanding the risk window.
- **What is the last-used timestamp:** this is helpful for understanding how recently the session was active. A recent last-used timestamp may suggest the session is still active, in use and usable by the attacker. An older last-used timestamp may suggest the session has been invalidated by the server, is no longer active and thus not useful for the attacker. Checking this with cookie expiration gives you a more complete picture of whether the cookie is actually viable for the attacker.
- **"Remember this device" token identification:** the presence of "Remember this device" tokens can indicate an active session cookie that has a longer lifetime than normal and that bypasses MFA as discussed. The presence of these tokens, especially for MFA environments, can indicate a heightened risk of replay attacks with the active session cookie.

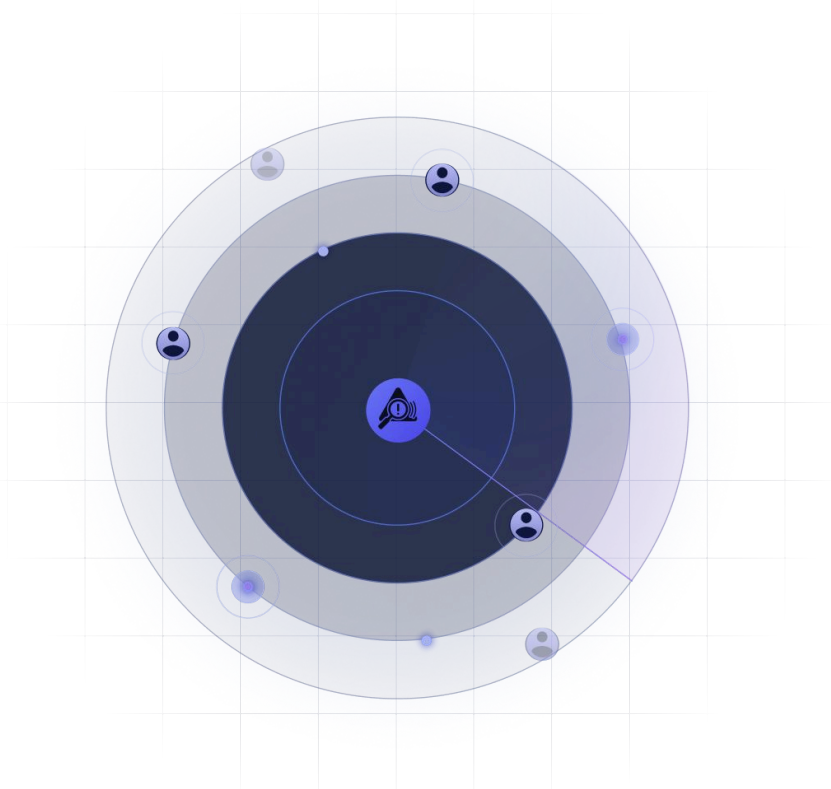
5.4 – IDENTIFYING ATTACK ATTEMPTS

The investigation steps covered so far focus on what has happened or what could happen: this step focuses on what is happening.

Because this step can be preventative rather than just forensic, it's also a stage of the investigation you may consider tackling sooner, especially depending on the guidance of your SLA response times.

In this stage of the investigation, you're monitoring for malicious activity using the information that you've found in the stealer logs. As part of a broader response, this monitoring can kick off additional triage and investigations as new attacks are discovered. Flexibility in investigation and response is key once again. Items you can monitor for in this stage include:

- **Authentication from new geographic locations:** Just as geographic information in the stealer log can point to threat actor activity, this is a similar and related indicator.
- **Access to resources outside normal user behavior:** An understanding of who the compromised user is and their role in the organization can help to understand what "normal user behavior" would be. This is an area where organizational awareness and human instinct can play an important role. In an investigation if something "feels" off, it's worth further investigation.
- **Bulk data access or downloads:** This is a classic marker of malicious activity. In many organizations, perimeter monitoring can be put in place to check for activity like this. However, attackers are aware of it, so it's important to be on the lookout for attempts to move large amounts of data in multiple small batches as well.
- **Password reset attempts and changes to security settings such as new MFA devices:** These can be indicators of attempts by the attacker to consolidate their presence and/or attempt lateral movement within your organization. In essence, these are actions by an attacker to make the compromised account more fully "theirs."



6 Coordinating Response

This step is about coordinating response, not about building a full response process: that is outside the scope of this guide.

In this step, we provide guidance on immediate steps a typical analyst handling these cases can take and suggest ways to coordinate with other groups in the organization. Every organization is different: you should adapt based on your specific needs.

6.1 – RECOMMENDED IMMEDIATE ACTIONS

The recommended immediate actions below are all focused on closing the attacker's window of opportunity, halting any active attacks, and preventing future attacks. These are steps most organizations will want to carry out quickly, as informed by the SLA response time. In some cases, there may even be merit to taking these actions first out of an abundance of caution and then performing full triage and investigation.

- **Invalidate compromised sessions immediately:** this step renders current sessions invalid and useless and is an effective countermeasure for the risks posed by active session cookies.
- **Force password reset for affected accounts:** Similar to invalidating compromised sessions, this step seeks to render the stolen information useless and inert.
- **Add geographic restrictions:** Geographic restrictions can be a low-impact-to-the-user high-impact-to-the-attacker countermeasure. It's similar to countermeasures banks take to prevent credit card fraud. If users' geographic locations are regular and predictable, this can be an easy step that they will never see or be impacted by. This is a step to consider especially if you've seen geographic activity in your triage and investigation.
- **Elevate monitoring on affected identity:** This is a prudent proactive step to increase protections against a now-known high-risk identity. This can be particularly useful in cases where the investigation shows that organizational credentials have been used on personal systems. Those systems are outside your control, and the risk of re-infection and new compromise can be high.

Taking actions like these can have significant user impact. If a legitimate action looks malicious and the analyst intervenes, business processes break. Being forced to re-authenticate may not be a major issue to some, but others can have a significant repercussion.

6.2 – COORDINATING WITH OTHER DEPARTMENTS LIKE IT AND SECURITY OPERATIONS

Some response activity will need to be carried out by other groups. The handoff between groups represents its own organizational risk that should have specific countermeasures in place. These risks are best countered through the establishment of regular processes and regular communications. Communication templates are particularly effective to help with this.

Some examples of information that needs to be handed off to other groups and should be very clearly and explicitly provided, ideally in templated fashion includes:

- **What was exposed:** Be specific, include the accounts, credentials, sessions, resources, and more
- **The risk assessment:** This can be done using the risk scoring matrix built earlier to help convey the risks and the SLA response time expected.
- **Actions taken, actions requested, additional recommended actions** with information from the risk scoring matrix already discussed.

6.3 – WHEN TO ESCALATE

Not every finding requires the same response path. Some issues you can resolve independently; others require escalation to other teams, senior security staff, legal, HR, executive leadership, or even law enforcement.

Ideally, the decision on when to escalate is made by the process, policies, and procedures. The risk scoring matrix can provide guidance: you can use that to build additional processes around escalation and notification. For example, anything that is of critical severity automatically requires notification to senior security staff, legal, HR and executive leadership.

Ultimately, escalation is a business decision and should be decided by leadership.

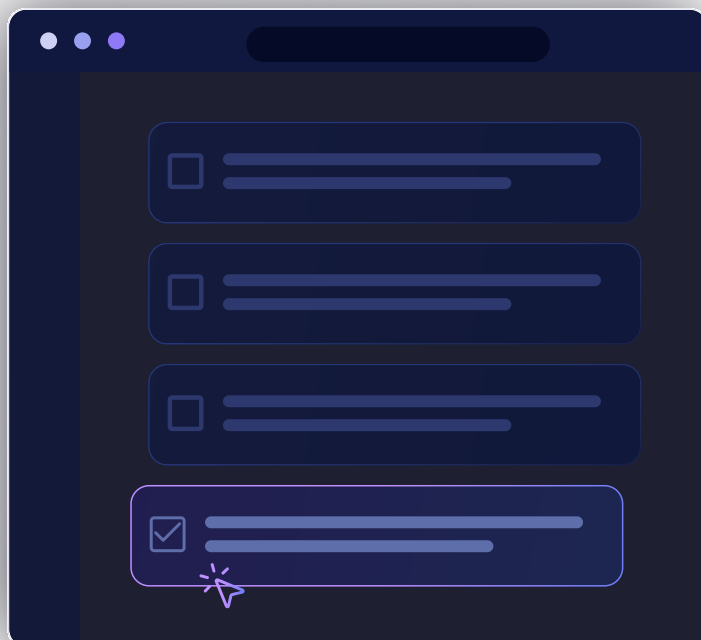
6.4 – DOCUMENTATION REQUIREMENTS

We've discussed documentation before and how it should be used throughout this process. Documentation in an event serves three purposes:

1. It provides a record of the investigation that can be used throughout the investigation and afterwards.
2. It creates a record that can be used for any legal, regulatory, or HR processes.
3. It builds the institutional knowledge that makes your program better over time through continuous improvement.

At minimum, document what you found, when you found it, how you found it, what actions you took and why, and the outcome.

For all incidents, documentation should be treated as potentially legally discoverable and written accordingly. Consult your document retention policy, if applicable, for guidance on where and how long to maintain these records.



7 Continuous Improvement

Documentation brings us to the final part of this guide: continuous improvement.

One of the reasons to document processes and specific, individual incidents is to be able to learn from them to refine and improve the process.

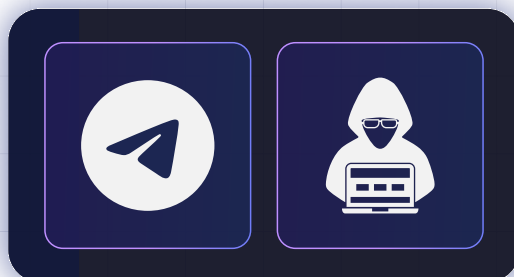
Threats are continually evolving, and no two incidents are alike. Without documentation, each response has to be built from scratch, reinventing the wheel. With documentation, each response builds on the previous one, learning, growing and adapting.

In addition to the documentation already outlined, here are some further recommendations to incorporate into your after-action reports and continuous improvement process.

7.1 – TRACKING EXPOSURE PATTERNS

Understanding the exposure patterns can help you get ahead of the curve by focusing your monitoring and protections more closely. Things that can help you understand exposure patterns include:

- **Which distribution channels affect your organization most:** One of the biggest challenges is knowing where to look for stealer log information. Learning what Telegram channels and dark web marketplaces affect your organization most directly can enable you to stay focused most closely where you need to be.
- **Employee populations at highest risk:** Risk is not created equal. Understanding the unique context risk of your users is also important. In addition to the context you can provide based on what you know of your employees, documenting what you find about your employees in the wild can help you build a more accurate risk picture.
- **Malware families targeting your sector:** Threat actor groups, especially ransomware groups, are known for specializing in targeting specific industries. Understanding what malware specifically targets your industry helps you focus both your defensive posture and understand places distribution channels to look at.
- **Geographic attack and infection patterns:** Similar to how malware families target your sector, there are geographic patterns to attacks and infections. Understanding this provides additional specificity that enables better protection and response.



7.2 – MEASURING PROGRAM EFFECTIVENESS

To improve a program, you have to know what's working and what's not working: you have to measure the program's effectiveness. Some common program effectiveness elements that you can and should measure in your documents for use include the following.

- **Time-to-detection metrics:** This measures how long it took for the compromise to be detected. In the case of searching stealer logs for information, it will be how long it took to find and identify the compromise once it happened. Ironically, the stealer log can help you with this, as the timestamp information in the log can give a reasonable indicator of compromise.
- **Time-to-remediation metrics:** This measures the effectiveness of your response process. It tells you how long it took to remediate the issue after it was detected.
- **Time-of-exposure metrics:** This combines the time-to-detection and time-to-remediation metrics to give you a full picture for how long your organization was at risk of attack. This measure is sometimes necessary also for regulatory findings.
- **Attack rate:** This is a measure you can gather from the logs in your investigation. This measure helps you understand how what you've found in the stealer logs translated into actual attacks against resources. In gathering this information, you can also understand what resources are being attacked and look for patterns there.
- **Repeat exposure tracking:** This is an important measure for understanding who may pose a great risk to your organization and may need additional user training as well as protections. Patterns in this can also point to departments in need of better, more specific training and possible technical countermeasures.

7.3 – FEEDING DETECTION INTO PREVENTION

A final area where the learnings from actual incidents provides important information for continuous improvement is in the area of prevention. Past events provide strong indicators of where future events can occur. It is also worth noting that threat actors tend to follow the rule of “nothing succeeds like success.” Here are some areas where learnings from handling stealer log incidents can be used to drive improvements for prevention.

- **Security awareness training priorities:** Part of tracking exposure patterns can uncover areas where users and groups of users may be in need of additional training and education.
- **Endpoint protection tuning:** Understanding the threat specific to your industry, geography, and attacks you've experienced can help you better understand how your endpoint strategies should be optimized.
- **Policy enforcement:** Patterns that emerge around personal systems being compromised can play their most positive role. Ultimately, that is more a human problem than a technological one, and the countermeasure in this case is through enforcement of policies and procedures.
- **Identity provider configuration hardening:** Lessons learned about MFA and session cookie expiration from attacks can provide guidance. It can also provide justification because changes around that area can have a direct and inconveniencing impact on users. Being able to point to hard evidence to justify the change can ease the path to users accepting the need for those changes.

Figuring Out Your Organization's Approach to Stealer Log Monitoring

Today, to protect your environment, you increasingly need a program to monitor for and act on data found in stealer logs.

This is a relatively new operational requirement. Until recently, actively searching for stolen credentials and sessions lived mostly in specialized circles, not in day-to-day security practice. As with any emerging tactic, there is still a lot to learn.

There's no one-size-fits-all approach. The right answer is the program you build to fit your risk profile, policies and procedures, users, business constraints, and leadership expectations and then refine over time through disciplined triage, investigation, response, and continuous improvement.

Check out what information stealer logs contain about your organization:

[Start a Free Trial](#)