



**MIDYEAR
UPDATE**

2024 Threat Detection Report

An in-depth look at the most prevalent threats,
MITRE ATT&CK® techniques, and identity
trends for the first half of 2024

introduction



Every March we publish the **Threat Detection Report**, our annual analysis of prevalent threats and techniques we've observed in confirmed threat detections and trends we've observed in those detections and beyond. Now, for the first time, we've supplemented the Threat Detection Report with a lightweight, midyear update examining the same data from the first six months of the current year. You can think of it as an addendum to the current Threat Detection Report or a preview of the upcoming one. In either case, you'll find analysis of pressing threats and techniques—and an in-depth look at how identity attacks are affecting the infosec community.

This report includes:

- an overview of identity trends that are shaping the threat landscape and driving change in the infosec industry
- an assessment of changes in threat and technique prevalence from the previous year into the first six months of this one
- analysis of emergent or otherwise interesting threats and techniques
- actionable guidance on preventive, mitigatory, or other security controls that teams can employ to better protect their organization against prevalent threats and techniques

A detailed explanation of the data we leveraged to produce this and the full Threat Detection Report is in the report's **methodologies section**. Put briefly, the report is the product of our analysis of confirmed threat detections across our customers, including the techniques adversaries abuse, the threats they leverage, and other insight gleaned from detections or observed across the industry.



key trend

Adversaries abusing identities

“Identity is the new perimeter.”

We’re not the first to say it, and we won’t be the last: *identity is the new perimeter*. This perhaps overused phrase is becoming cliché for a reason—it’s unquestionably true for most organizations, particularly those with a large cloud footprint and which leverage numerous SaaS applications. This sentiment is a driving force behind the burgeoning identity threat detection and response (ITDR) sub-industry. To that point, one sufficiently privileged identity can offer an adversary access to countless cloud systems, SaaS applications, or even the identity product itself. Even a less privileged identity—when it’s not inherently valuable as a target for internal reconnaissance or espionage—can serve as a beachhead for an adversary to conduct internal phishing or otherwise move laterally to a more privileged one.

Compromised identities have been a central component of countless costly breaches this year. Looking purely at Red Canary’s detection data, three of our top 10 techniques from the first six months of 2024 are cloud-native techniques that relate directly to identity: **Cloud Accounts**, **Email Forwarding Rules**, and **Email Hiding Rules**.

Identities are arguably among the most important assets for enterprise security teams to secure, and although there are many security solutions capable of effectively fortifying identities, these can be complex, expensive, and prohibitively difficult to implement.

In this section, we will explore:

- common identity threats and techniques
- organizational and IT problems related to identity
- strategies anyone can follow to harden their identity perimeter

Identity threats and techniques

“Three of our top 10 techniques from the first six months of 2024 are cloud-native techniques that relate directly to identity.”

Identities are a means to an end, and so isolated, identity-specific threats or threat groups are difficult to pin down. However, many adversaries are proving themselves adept at targeting identities, and there are numerous identity-related techniques that adversaries commonly deploy in the service of an intrusion. We’ll explore general threats to identities and techniques to help security professionals better understand the role identities play in an organization’s security posture.

The following is a non-exhaustive list of methods adversaries commonly leverage to gain access to identities and brief descriptions of what adversaries commonly do once they've compromised an identity.

How adversaries compromise identities

Stolen credentials and tokens

There are innumerable ways for an adversary to steal valid credentials that they can then use to gain access to identities and valid accounts. Some common methods include:

- **credential-stealing malware**
- phishing
- credential stuffing
- password spraying
- brute forcing
- leaked credentials/authentication tokens
- **vulnerability exploitation**

Adversaries also frequently target **session tokens** in order to gain access to identities. Methods of token theft include wide varieties of social engineering like adversary-in-the-middle (AitM) attacks or attacks in which adversaries otherwise leverage malicious applications to gain access to cloud-hosted systems and services (more on this below).

Adversaries can also steal tokens after compromising a cloud account or service. In Amazon Web Services (AWS) particularly, sufficiently privileged adversaries can extract **short-term security token service** (STS) tokens from Elastic Cloud Compute (EC2) instances by **targeting the EC2 Instance Metadata Service (IMDS)**. This service contains tokens associated with the roles granted to an EC2 instance, which an adversary can steal and potentially leverage to perform actions within the same cloud tenant.

“Organizations that enforce MFA across their cloud accounts and SaaS applications significantly complicate adversary attempts to compromise identities.”

Multi-factor authentication (MFA) abuse

Organizations that enforce MFA across their cloud accounts and SaaS applications significantly complicate adversary attempts to compromise identities. However, there are various methods of overcoming MFA. **MFA fatigue attacks**—where an adversary obtains legitimate credentials and then bombards their victim with MFA requests—are among the simplest of these.

Adversaries also leverage AitM attacks to bypass MFA, by setting up a website that looks like a legitimate login page and luring the victim into entering their credentials into it. The adversary relays those credentials in

real time, often cloning the login details of the captured session and attempting to log into the legitimate account, before presenting the victim with a secondary webpage in which to enter their MFA code. If the victim uses push notifications, then the secondary page may not be necessary. AitM attacks are commonplace and numerous AitM toolkits lower the barrier of entry for adversaries conducting AitM attacks.

Other common tactics for bypassing MFA include adversaries reaching out to help desk technicians or mobile service providers in an effort to conduct SIM swap attacks or even register their own MFA devices. Help desk social engineering, SIM swaps, and other techniques for resetting an MFA device are also crucial for adversaries to establish persistence, since tokens gleaned from an AitM or similar account takeovers are short lived, and the adversary will need to bypass MFA again in short order to maintain access to their victim's account.

Role and application abuse

Adversaries also abuse application access and role assignments to gain access to identities. Application consent phishing and device code phishing are two examples of this. Application consent phishing involves an adversary registering a malicious application and then tricking their victim into granting it permissions that will allow the adversary to access systems and data within their cloud environment and potentially beyond. Device code phishing, on the other hand, abuses the **OAuth 2.0 Authorization Framework specification**, which allows devices without browsers (such as TVs or internet-of-things devices) to authorize themselves on behalf of users. In this case, the adversary requests a user code from the cloud or identity provider that will offer certain permissions to their own malicious application. They then send that login link to the victim, who may unwittingly login and grant permissions to the adversary-controlled application.

How adversaries leverage compromised identities

Business email compromise (BEC)

“BEC remains a clear frontrunner among identity-centric threats—let alone threats in general.”

BEC remains a clear frontrunner among identity-centric threats—let alone threats in general. In fact, two of the top 10 techniques we detected in the first six months of 2024 are driven largely by BEC-related activity:

- Email Forwarding Rules
- Email Hiding Rules

We discussed both techniques in the **Email Forwarding Rules** section of

“Adversaries often attempt to hide their communication by creating a rule to forward emails from a particular sender to an email folder that the victim is unlikely to open.”

the 2024 Threat Detection Report, as the line between these two techniques is blurry and subject to interpretation. Both schemes typically involve an adversary compromising an email account and using it to monitor communications and/or surreptitiously communicate with the victim’s contacts—often a contact that engages in financial transactions with the victim, such as a vendor or a payroll department. **Email forwarding incidents** may involve routing emails to an external or internal email address. Adversaries often attempt to hide their communication by creating a rule to forward emails from a particular sender to an email folder that the victim is unlikely to open. Alternatively, we also often see adversaries simply marking messages as spam, blocking senders, or otherwise hiding email messages. The ultimate goal of these attacks may be to reroute payments from legit bank accounts to accounts controlled by the adversary, reconnaissance, or for reconnaissance or espionage.

Other post-compromise activity

Outside of BEC, much of what an adversary does once they compromise an identity is procedural. They’re merely using the identity to support whatever their ultimate objective is, which could range from cryptocurrency mining to **ransomware** to espionage and include essentially anything in between. Some activity to be aware of includes:

- abusing OAuth apps
- additional credential stuffing, password spraying, and brute forcing
- internal phishing
- reconnaissance for passwords or other valuable information
- resetting victim passwords
- adding new MFA devices
- third-party account creation
- adversary service creation
- consenting to new applications
- privileged role assignments
- reconnaissance of directory users and applications

Identity challenges

“Outside of BEC, much of what an adversary does once they compromise an identity is procedural.”

As we noted earlier, many of the prominent threats and risks organizations face in the identity space are mitigatable via controls that are available to most organizations. Unfortunately, these controls can be complex to implement in practice, particularly at scale. As such, we will list some of the challenges that organizations might encounter as they attempt to fortify their identity infrastructure.

MFA adoption

Implementing MFA across an organization presents numerous challenges. For one, an organization needs dedicated technical staff capable of actually setting up and enforcing MFA. Further, MFA requires third-party devices—often mobile devices or additional IT equipment—to work. As such, an organization either needs to allocate budget to procure these devices or it must assume that employees have access to their own mobile devices that they are willing to use for MFA. This effectively creates a de facto bring-your-own-device (BYOD) policy that can have a wide variety of knock-on consequences that may discourage the adoption of MFA. Further, this doesn't account for scenarios where employees may not have personal devices, may be unwilling to use them for work, or may lack the technical savvy required to use MFA.

Additionally, some organizations have multiple workers leveraging shared accounts and devices. Think of a convenience store chain where employees use a shared account to access the point-of-sale terminal. How does an organization set up MFA for this kind of shared account?

Permission sprawl and dangerous role assignments

Permission sprawl is another problem that many organizations may face in the identity space. Maintaining an inventory of users is challenging on its own, but understanding the permissions granted to those users—and the implications of different permissions across different tools—is immensely complex. Similarly, organizations must understand role assignments since it's easy to assign overly permissive or privileged roles to applications.

Beyond understanding permissions and roles, it's worth considering the trustworthiness of the applications you grant these roles and permissions to. Taking **Microsoft Azure** as an example, an application from the Azure Marketplace might be reasonably trustworthy whereas an application from elsewhere might deserve more scrutiny. Similarly but on an individual level, you might be willing to grant full read-write permissions from Microsoft Exchange to the Apple mail client but not to some lesser known calendar orchestration app. Take this simple example and expand it out across all the users and applications in a given organization to understand the scope of this challenge.

Alert overload

Most identity and cloud providers will generate alerts for suspicious login activity. Unfortunately, these alerts can be extremely voluminous, particularly for remote workers, people who are working while traveling, and large enterprises, especially ones with complex internet gateways. The criteria these providers apply in determining that a login is suspicious can be based on anomalous characteristics of the logon as defined by

“Beyond understanding permissions and roles, it's worth considering the trustworthiness of the applications you grant these roles and permissions to.”

the vendor itself, but an anomaly in a login is not necessarily malicious or even suspicious. As an example, if an alert tells you that a user logged in from an unusual location or IP space (and that's all it tells you), how do you know whether or not that login was malicious or benign? Many identity providers generate unmanageably high volumes of false positive alerts, discouraging security teams from investigating suspicious logins, even when the logins are successful.

Identity solutions

For all the risks and challenges associated with identity, defenders can choose from a wide array of solutions available for improving identity security.

MFA

Implement and enforce MFA as far and as wide as possible. If feasible, implement phish-resistant MFA, but any MFA is better than none.

Conditional access policies

Conditional access policies effectively allow administrators to permit or deny access to a resource based on attributes of the login. For example, you can use conditional access policies to deny access to resources from unmanaged devices or require that devices use MFA to access a resource. Implementing these to whatever extent is possible across your identity infrastructure can mitigate a wide array of identity risks arising from improper configuration, implementation, and elsewhere.

Passwordless solutions

Passwordless solutions like hardware tokens, hardware-based authentication devices, biometrics, and more that require a user to plug a keycard or USB fob into a device—or prove their identity via a biometric measure—make it extremely difficult for an adversary to compromise an account. Unfortunately, these phish-resistant solutions can be hard to implement and administer. However, implementing them on a smaller scale, for example if you only want them to protect your most secure identities (e.g., your Okta admin accounts), can be much more manageable and significantly shore up the security of your identity infrastructure.

Short-term access

AWS STS and **privileged identity management (PIM) for Microsoft Entra ID** are great examples of short-term access, although similar technologies likely exist across other cloud and identity providers.

“Many identity providers generate unmanageably high volumes of false positive alerts, discouraging security teams from investigating suspicious logins, even when the logins are successful.”

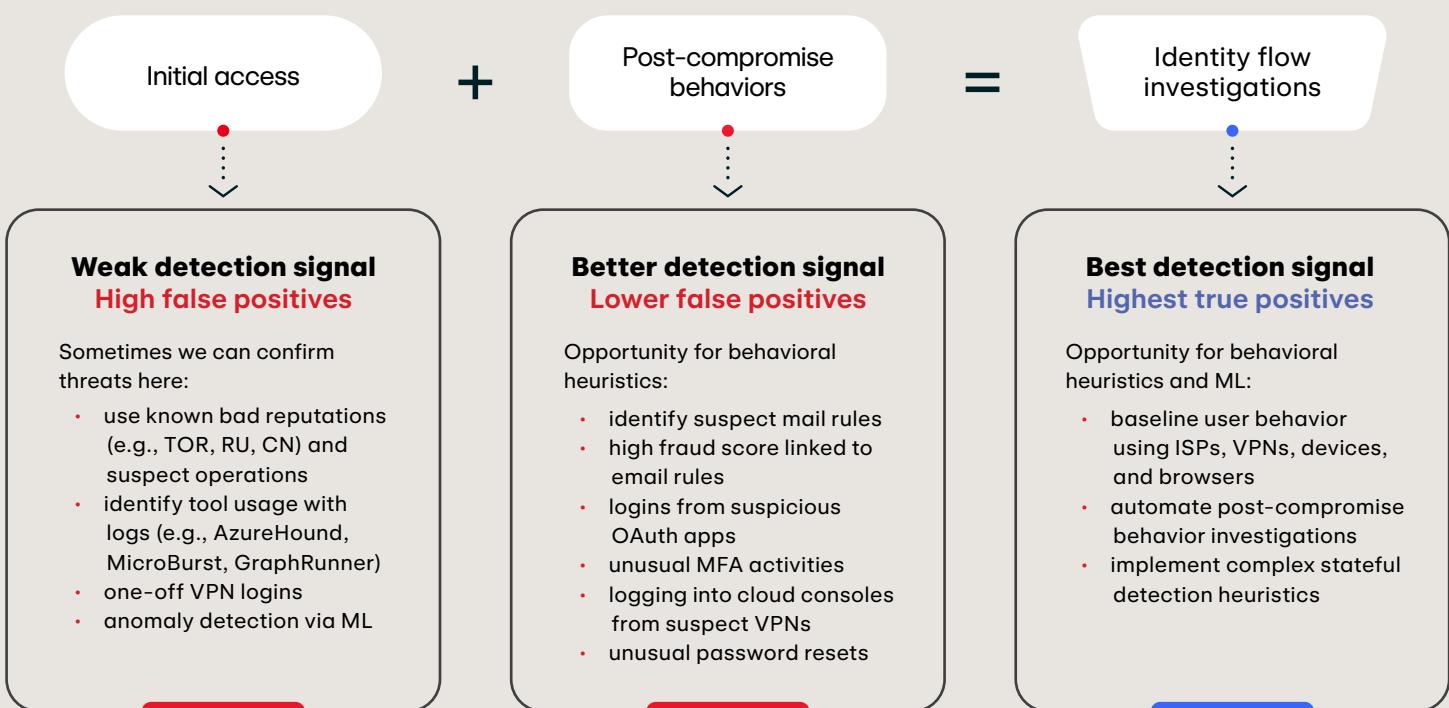
Short-term access allows organizations to issue short-lived tokens that grant temporary access to resources in lieu of long-standing permissions or credentials for users or roles. Tokens only last for a matter of minutes or hours, limiting the amount of damage an adversary can do with a stolen token. Further, since these tokens are generated dynamically and not stored by the user, they are phish-resistant and difficult to steal.

Identity threat detection and response (ITDR)

ITDR solutions collect telemetry from your identity, cloud, and other IT infrastructure and perform detection and response specifically for identity-related activity. This can include looking for logins occurring from unusual VPNs but also enriching identity telemetry with related signals from other tools like **endpoint detection and response** (EDR), user entity behavior analytics (UEBA), **certificate information**, and more.

The following graphic demonstrates the identity threat detection workflow that we've found most effective at detecting threats across our customers' identities.

Stages of identity threat detection





threats

Our 10 most prevalent threats from the first half of this year bear a striking resemblance to the top 10 from 2023. Not much has changed, which is to be expected since there tends to be a decent number of holdovers from year to year. You've got the dual-use tools that show up almost annually in **Impacket** and **Mimikatz**; long-time threats that have been prevalent for years in **SocGholish**, **Gamarue**, and **Gootloader**; and the **Charcoal Stork-ChromeLoader** pairing that helped shape the top 10 threats in 2023.

However, it's interesting to see that ChromeLoader has moved dramatically up the charts and overtaken the number one slot. **Scarlet Goldfinch** is a newcomer to the top 10, never before featured in the Threat Detection Report's annual top 10 (but something of a mainstay in our monthly **Intelligence Insights** rankings in recent months). Atomic Stealer warrants mention given that it targets macOS devices, which represent a small percentage of the endpoints we monitor, and so its appearance in the top 10 here suggests that this threat is extremely prevalent on macOS devices.

The following compares the 2023 top 10 threats featured in the 2024 Threat Detection Report to the top 10 threats from the first six months of this year. Refer to the [methodologies section](#) to learn more about where these data come from.

TOP 10 THREATS DETECTED

RANK	2023	H1 2024
1	Charcoal Stork	▲ +5 ChromeLoader
2	Impacket	Impacket
3	Mimikatz	SocGholish
4	Yellow Cockatoo	Mimikatz
5	SocGholish	Gamarue
6	ChromeLoader	Gootloader
7	Gamarue	NEW Scarlet Goldfinch
8	Qbot	Charcoal Stork
9	Raspberry Robin	NEW Atomic Stealer
10	SmashJacker	NetSupport Manager

In this section, we're going to briefly explore:

- ChromeLoader and its relationship with Charcoal Stork
- Scarlet Goldfinch and how it's different from SocGholish
- Atomic Stealer and macOS threats generally

ChromeLoader (with special guest Charcoal Stork)

What is it?

ChromeLoader is a malicious browser extension that reads and hijacks browser traffic by modifying victims' browser settings and redirecting their traffic to advertisement websites—likely to perform some kind of pay-per-click ad fraud. While the threat is admittedly more innocuous than the ransomware precursors in our top 10, it is nonetheless extremely prevalent and we consider it malicious (and not mere adware) because of its use of persistence mechanisms, ability to read and redirect searches, and potential for exposing sensitive information that could be used for targeted phishing campaigns. Furthermore, while ChromeLoader currently seems to serve the purpose of perpetuating some kind of advertising fraud, it could be readily adapted to deliver more overtly malicious code in the future.

ChromeLoader is closely related to another threat in our top 10: Charcoal Stork. A suspected pay-per-install provider, Charcoal Stork was our number one threat in the most recent Threat Detection Report following a dominant run of infections in 2023. Adversaries typically deliver Charcoal Stork via malvertising that promotes malicious installers masquerading as cracked games, fonts, or desktop wallpaper.

ChromeLoader intrusion lifecycle

Initial Access

- ChromeLoader delivery via Charcoal Stork or other PPI
- Malvertisement drops variously named file
- Masquerades as PDF editor

Persistence & Defense Evasion

- Persistence via LNK to NodeJS app in Startup folder
- Also persists via a Registry run key
- Time delay between install and activity

Execution

- Obfuscated PowerShell on Windows
- Retrieves code over network

Collection

- Gathers and exfiltrates browsing data

What can you do about it?

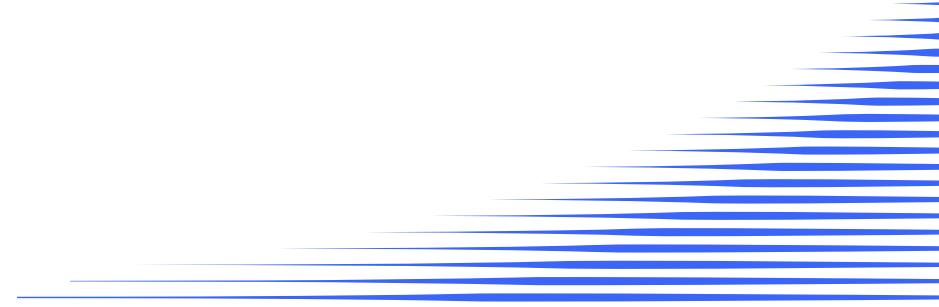
There's **extensive guidance** on how to defend an organization against ChromeLoader (and Charcoal Stork) in the 2024 Threat Detection Report that remains viable, so we won't retread all of that here. However, there are two relatively simple preventive strategies that nearly any security team can implement to diminish the risk posed by these threats.

1. Forcing the installation of ad blockers across your organization may prevent the malicious advertisements that deliver Charcoal Stork (and by extension ChromeLoader) from rendering in the first place. Google has **relatively simple instructions** on how to do this from the Admin console in Chrome, and **similar controls exist for Edge** as well. Alternatively, more complex solutions for ad blocking may be available to organizations via their firewall configuration settings.
2. Additionally, you can establish block and allow lists for extensions across an enterprise, potentially blocking users from ever installing the ChromeLoader browser extension in the first place. Google has **simple instructions** on how to do this in Chrome.

Scarlet Goldfinch (with special guests SocGholish and NetSupport Manager)

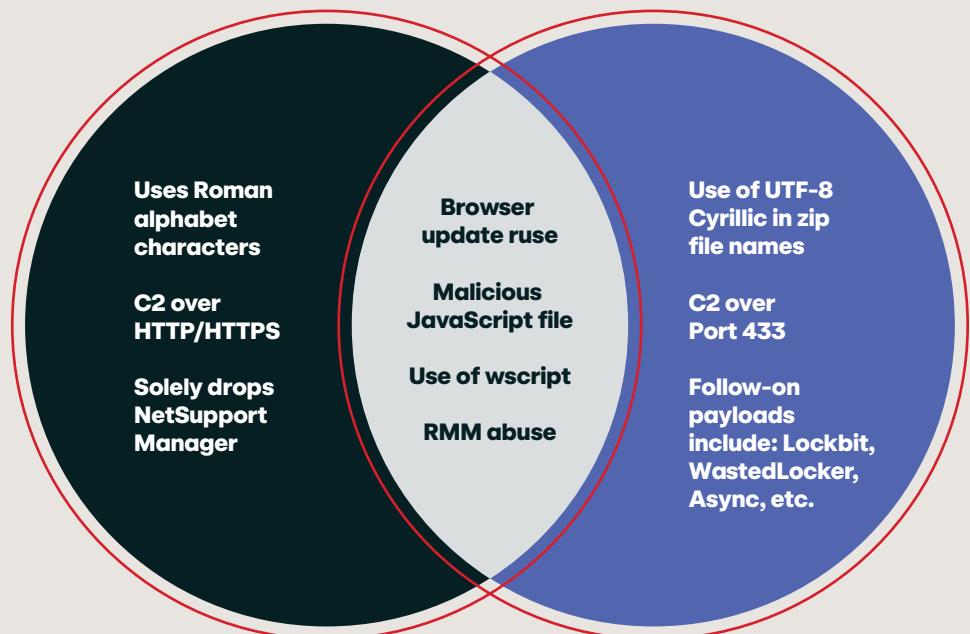
What is it?

Scarlet Goldfinch is an activity cluster defined by Red Canary that uses fake browser updates to trick users into downloading NetSupport Manager, a legitimate **remote management and monitoring (RMM) tool** that adversaries commonly abuse in intrusions. Another of the many examples in our prevalence list of web-based threat delivery, Scarlet Goldfinch is similar to SocGholish (hence the "S" and the "G"), but we started tracking it as a distinct threat in 2023 after observing conspicuous differences in tradecraft between the two threats.



The following image briefly illustrates what separates SocGholish from Scarlet Goldfinch:

Scarlet Goldfinch vs. SocGholish



The crucial differentiator here is that Scarlet Goldfinch delivers NetSupport Manager—an RMM tool with the veneer of legitimacy—as its follow-on payload, whereas SocGholish typically delivers more overtly malicious or suspicious malware. Further, NetSupport Manager, the 10th most prevalent threat in the first six months of 2024, is a dynamic administrative tool offering a robust array of remote administration features that many organizations leverage to apply updates, manage assets, and deploy software. Adversaries often use this tool maliciously (and those are the instances where we detect it) because it simultaneously blends in while also giving adversaries a great deal of flexibility as they attempt to accomplish whatever their ultimate objectives are.

The following shows a rough timeline of a Scarlet Goldfinch infection.

Scarlet Goldfinch intrusion lifecycle

Initial Access

- JSInject posing as browser update
- Update 124.0.6367.158.js

Persistence

- Registry “Run” key
- Usually named “divxx”, “officec”, or “vcarts”

Execution

- PowerShell commands for downloading
- Downloads and unpacks ZIP archive

Collection & Control

- Downloads additional malware
- NetSupport Manager RAT
- LummaC2 Stealer

What can you do about it?

There are multiple relatively straightforward ways to mitigate the threat posed both by Scarlet Goldfinch and its primary follow-on payload. We'll start with the former.

Since Scarlet Goldfinch is delivered in the form of a JavaScript payload, defenders can effectively stop this threat before it starts by changing the default program that opens and executes JavaScript files from `wscript.exe` to something innocuous like `notepad.exe`. You can do this relatively easily by creating a Group Policy Object (GPO), which [we described in-depth in a blog in late May](#).

The most concerning component of Scarlet Goldfinch is its follow-on payload, NetSupport Manager. Broadly speaking, the first thing you may want to know is whether anyone—benign or otherwise—is using NetSupport Manager in your environment. Fortunately, [Surveyor](#) is a free and open source tool that works with supported EDRs to baseline environments for the presence of certain tools. Surveyor contains a definitions file that will search across an environment for the presence of NetSupport Manager (and a long list of other RMM and other tools) based on the presence of its process name (`client32.exe`), internal name (`client32`), domain connections to `geo.netsupportsoftware.com`, and its digital signature publisher (`NetSupport Ltd`).

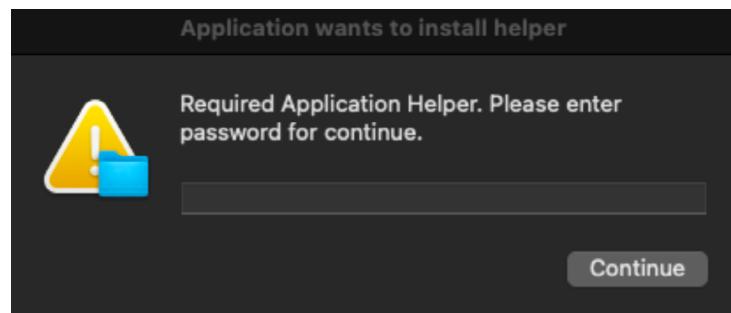
Perhaps most importantly, security teams can leverage application control solutions to ensure that only approved RMM tools are used in their environment.

Atomic Stealer (and macOS threats generally)

What is it?

Yet another web-delivered threat in our top 10, Atomic Stealer is an infostealer that targets macOS systems—and it's part of a general proliferation of **stealers** that target macOS systems along with threats like Banshee, Cthulu, and Poseidon. Specifically, Atomic Stealer targets credentials, payment card data, cookies, keychain details, and information related to cryptocurrency wallets. It's delivered via pirated or cracked software and malicious advertisements that prompt the end user to download the malware.

Downloading Atomic Stealer and other malware on macOS is relatively straightforward and can seem legitimate to unsuspecting users as it's often nearly indistinguishable from downloading legitimate software from the internet. In fact, the malware often coaches users through the process of installing the malware.



"To say we protect 10 times more Windows machines than macOS machines is probably a dramatic understatement, so Atomic Stealer's presence on this list is a testament to just how prevalent it is in organizations with a significant macOS footprint."

That macOS malware would make our top 10 most prevalent threats at all is noteworthy. Like most infosec vendors, the majority of machines we protect are not macOS machines. To say we protect 10 times more Windows machines than macOS machines is probably a dramatic understatement, so Atomic Stealer's presence on this list is a testament to just how prevalent it is in organizations with a significant macOS footprint.



The following shows the rough timeline of an Atomic Stealer infection:

Atomic Stealer intrusion lifecycle

Initial Access

- Pirated or cracked software
- Malicious advertising downloads

Collection

- Keychain duplication
- Browser data duplication
- AppleScript file grabber

Exfiltration

- Exfil data over HTTP/HTTPS in ZIP archive

Credential Access

- AppleScript input prompt

Privilege Escalation

- Request TCC permissions

What can we do about it?

The most common initial access for these threats is through users searching for software and obtaining it from malicious sources instead of trusted ones. Educating users about how and where to source software is critical, especially for macOS, where application control solutions are less common and complicated to use. However, providing ways for users to obtain software from safe, trusted sources can be massively beneficial. This can be as simple as a spreadsheet of known good links to approved software or as complex as a device management solution with software deployment options that put the burden of software installation on the IT department. We also strongly recommend proactively implementing some kind of ad-blocking technologies where possible.

“Educating users about how and where to source software is critical, especially for macOS, where application control solutions are less common and complicated to use.”

It’s also important to keep your macOS systems updated. The built-in macOS XProtect YARA engine (their equivalent to Windows Defender) gets updated regularly and may get new detection rules for stealers. In addition, new updates may also improve controls such as **Gatekeeper**, which is supposed to protect users from threats downloaded from the internet.



techniques

As is the case with threats, the list of 10 **MITRE ATT&CK®** techniques we detected most frequently in the first half of this year isn't a dramatic departure from the top 10 in 2023. In fact, **Email Hiding Rules** is the only technique we've never covered explicitly in a previous Threat Detection Report, although we discussed it in passing in the **Email Forwarding Rule** section. Since you can find extensive analysis of all of these techniques either in the **2024 Threat Detection Report** or in **our archive of previous Threat Detection Reports**, we're going to focus this update on a few techniques that have been most emergent in recent years and months.

To that point, **Cloud Accounts**, **Email Forwarding Rules**, and **Email Hiding Rules** stand out since they've only managed to break into the top 10 in the last year. This stands in contrast to techniques like **PowerShell**, **Windows Command Shell**, **Windows Management Instrumentation**, **OS Credential Dumping**, and **Rename System Utilities**, which are among our 10 most prevalent threats nearly every year, and **Modify Registry** and **Service Execution**, which bounce in and out of the top 10 depending on the year.

TOP 10 TECHNIQUES DETECTED

RANK	2023	H1 2024
1	PowerShell	Windows Management Instrumentation
2	Windows Command Shell	▲ +2 Cloud Accounts
3	Windows Management Instrumentation	Windows Command Shell
4	Cloud Accounts	PowerShell
5	Obfuscated Files or Information	▲ +1 Email Forwarding Rule
6	Email Forwarding Rule	NEW Email Hiding Rule
7	OS Credential Dumping	OS Credential Dumping
8	Rundll32	Modify Registry
9	Ingress Tool Transfer	Service Execution
10	Rename System Utilities	Rename System Utilities

In this section, we're going to briefly explore:

- Cloud Accounts
- Email Forwarding Rules and Email Hiding Rules

Cloud accounts

What is it?

Cloud Accounts is the MITRE ATT&CK technique for when an adversary abuses a legitimate account in an intrusion into an organization's cloud environment. The technique is extremely broad in the context of the cloud,

since legitimate accounts are among the only ways that an adversary can interact with their victim's cloud. **APIs** are the crucial knobs and dials that allow an adversary to accomplish their goals in the cloud, whatever they are, and a valid cloud account is the essential prerequisite for accessing APIs. In this way, cloud accounts are more of a means to an end than a standalone adversary technique. They're also inextricably bound to the major trend (identity) covered earlier in this report, as accessing a valid cloud account almost always entails compromising an identity. Further, accessing cloud-hosted emails is one of the ends that an adversary may seek when exploiting valid cloud accounts, which is why it should come as no surprise that Email Hiding Rules and Email Forwarding Rules are also in our top 10.

Most confirmed threat detections that are associated with the cloud accounts techniques in our dataset arise from a mix of alerts from identity providers, custom detection analytics leveraging identity telemetry, and malicious activity occurring in cloud-hosted email services (more on this in the following section). In addition to these, we also detect activity emanating from valid cloud accounts based on alerts from cloud service providers and custom detection analytics built on top of logging capabilities provided by the cloud providers.

In general, upon gaining access to a cloud account, adversaries typically perform various **Account Manipulations**, like gathering long-term credentials, gaining new permissions, or taking advantage of misconfigurations to maintain persistence or elevate their privileges. They may also perform discovery actions to enable pivoting to resources of interest such as email, internal company chat resources, document storage, Git resources, and more.

The precipitous rise of cloud account abuse in our detection dataset is the result of five interrelated factors:

1. technique broadness (as discussed above)
2. increased adoption of cloud technology among businesses
3. internal security teams emphasizing cloud security in response to increased adoption
4. security vendors emphasizing cloud security to help internal security teams meet their newfound cloud security needs
5. adversaries following enterprises into the cloud

As such, the data and systems that adversaries have always sought are increasingly moving to the cloud. At the same time, there's increased visibility from defenders into the cloud, both internally and from third-party vendors. As a result (and as an industry), we're seeing a lot more malicious and suspicious cloud activity than we have in years past.

The broadness of this technique makes it difficult to succinctly summarize what exactly adversaries are doing in the cloud, but, in a general sense,

“APIs are the crucial knobs and dials that allow an adversary to accomplish their goals in the cloud, whatever they are.”

“You don’t necessarily need to know what an adversary’s ultimate objective is in your cloud to reduce the risk associated with its compromise.”

“Nearly every malicious or suspicious action that an adversary might undertake in the cloud involves the use of one API or another.”

they’re using whatever APIs are available to them to access the data and systems that are valuable to them. You can read the [Cloud Accounts](#) section of the Threat Detection Report for a more detailed look at cloud intrusions. However, you don’t necessarily need to know what an adversary’s ultimate objective is in your cloud to reduce the risk associated with its compromise.

What can we do about it?

A cloud defense strategy effectively comes down to three broad categories:

- securing identities
- avoiding misconfigurations
- monitoring API usage

We covered identities extensively earlier in this report, but we’ll briefly reiterate some of the key recommendations security teams can follow to lock down the identities that can provide adversaries access to your cloud accounts:

- Implement and enforce MFA across your corporate identities
- Leverage [conditional access policies](#) to block suspicious logins
- Use passwordless or hardware-based authentication solutions where feasible (especially for highly sensitive accounts)
- Take advantage of short-term access solutions like Entra ID PIM or [AWS STS](#) to prevent adversaries from getting their hands on long-lasting access tokens

Practically speaking, organizations should also assume that accounts can get compromised, and they should strive to implement defense-in-depth strategies for protecting their cloud environments accordingly.

Misconfigurations that leave cloud resources accessible on the open internet have been the source of countless cloud breaches over the years. Unfortunately, documenting all the various ways to avoid misconfiguration across multiple cloud service providers and their innumerable services would require an entire standalone report. So, put briefly, it’s important to educate anyone who’s spinning up cloud services and applications about the configuration options available within the cloud services and providers they’re using and the implications of those configuration options.

Last but not least, APIs are basically the [LOLBINS of the cloud](#). Nearly every malicious or suspicious action that an adversary might undertake in the cloud involves the use of one API or another. It’s critically important that security teams understand the APIs that adversaries frequently abuse and, just as importantly, that security teams have reliable visibility into API usage across their cloud infrastructure. This alone though isn’t enough. Differentiating benign from malicious API use in the cloud is a

tricky problem, so it's necessary that security teams monitor all API usage and become deeply familiar with what's normal and what isn't.

The following is a non-comprehensive list of cloud log sources that security teams should consider collecting from across the big three cloud providers.

Amazon Web Services (AWS):

- AWS CloudTrail
- Amazon GuardDuty
- AWS CloudWatch
- Amazon Detective
- Amazon Security Lake

Azure:

- Audit logs
- Interactive Sign In Logs + Non-interactive Sign in Logs
- Azure Activity ("control plane")
- Resource/Diagnostics Logs per resource ("data plane")
- Graph API Activity Logs

Google Cloud Platform:

- Cloud audit logs

Practically speaking, organizations should also assume that accounts can get compromised, and they should strive to implement defense-in-depth strategies for protecting their cloud environments accordingly.

Email hiding and forwarding rules

What are they?

Email Forwarding Rules and **Email Hiding Rules** are two distinct but closely related ATT&CK techniques that we attempt to track separately across detections as best we can. However, we're grouping them together here because many of the custom detection analytics we leverage to detect suspicious email activity are somewhat ambiguous in the sense that they can unearth both email hiding rules and email forwarding rules. With additional context, you may be able to differentiate the techniques in some circumstances, but there are also times where email forwarding and hiding are happening concurrently. Beyond that, adversaries often leverage these to conduct similar types of attacks, predominantly BEC but also espionage and reconnaissance.

In either case, the general goal is to compromise an email account, typically after compromising an identity, and then to either:

1. exfiltrate email (i.e., when the forwarding address is to an adversary-controlled external email address)
2. send email on behalf of the compromised identity, abusing the established trust of the identity

Adversaries leverage compromised email accounts in an effort to **reroute payments** in one form or another. Two common examples include leveraging a legitimate email account to contact the payroll department and convincing them to update the employee's direct deposit account so that an employee's paycheck is sent to an account controlled by an adversary. Adversaries also compromise the accounts of procurement employees (or any employees that receive payments for that matter) and use them to trick vendors into routing payments to bank accounts controlled by the adversaries rather than to an organization's legitimate business account.

Adversaries create email forwarding rules to send emails from a particular sender or that contain specific keywords to a location—like a newly created folder where the legitimate user is unlikely to look—or to an external email address. Similarly, email hiding rules typically involve an adversary blocking a sender, marking their emails as spam, or otherwise routing email messages to places where the legitimate user won't look, like the archive folder, for example.

What can we do about it?

We've included extensive detection guidance on how to spot these activities in the **Email Forwarding Rules** section of the Threat Detection Report as well as in the **Email threats** section that you can find in the Threat Detection Report archive.

Office 365 users can disable external email forwarding rules for their organization by following this guide by **Microsoft**. Google has a similar guide for **Google Workspace** users.

Beyond that, most email providers have an application log of some kind that will collect the telemetry you need to gain visibility into suspicious email forwarding or hiding rules. For Office 365, this would include the Unified Audit Log (UAL), and you can hunt for email rules using **PowerShell cmdlets** and by monitoring other log sources. For Google Workspace users, the **Security Investigation Tool** will be your starting point and suspicious email rules can be observed by obtaining user Gmail settings through the Gmail API.

“Adversaries leverage compromised email accounts in an effort to reroute payments in one form or another.”

take action



Red Canary helps you find and stop account compromise, BEC, SaaS misuse, and other **identity threats**.

Understanding the important trends in adversary tradecraft, the threats adversaries are leveraging most often, and the techniques they abuse in intrusions is crucial to effective security operations. After reading this report, ask yourself:

- Is there anything my organization can do to improve the security of our identity infrastructure in the short, medium, and long term?
- Am I confident that my security operations team has sufficient security controls to combat the prevalent threats listed and analyzed in this report?
- Does my company have sufficient defense in depth against the prevalent techniques highlighted here and across previous Threat Detection Reports?

If the answers to any of those questions range between “I’m not sure” and “no,” then there are probably security controls you can implement to better prevent breaches at your organization. Some of them—like implementing **conditional access policies** that enforce MFA across your organization—will have a vast, immediate impact at diminishing the risk posed by wide varieties of threats. Some are readily accessible and relatively simple to implement, like **creating a GPO** to open potentially dangerous files in Notepad by default. Others are hard, will take time, and may not pay off in the immediate term, like developing a robust strategy for **monitoring API calls** across your cloud environment. However, nearly every organization on the planet, regardless of their resource or budget constraints, can do something better.

If you want more in-depth information about prominent trends, threats, and techniques, including extensive detection and testing guidance, read the **2024 Threat Detection Report**. And speaking of Threat Detection Reports, stay tuned for the seventh annual Threat Detection Report, which will drop in spring 2025!