



Small and Medium-Sized Business

# Threat Report



# Table of Contents


<b>Executive Summary</b>	<b>3</b>
<b>Quarterly Summary</b>	<b>5</b>
Intrusion Trends	<b>7</b>
Identity-Focused Security	<b>10</b>
Adversary Tooling & Behaviors	<b>12</b>
<b>Adversary Trends</b>	<b>17</b>
Additional DarkGate Observations & Software Impersonation	<b>21</b>
Continued AsyncRAT Infections & Process Chains	<b>22</b>
Espionage in the SMB Environment	<b>23</b>
<b>Response &amp; Defensive Guidance</b>	<b>24</b>
<b>Conclusions</b>	<b>28</b>

# Executive Summary

While the world of cybersecurity often revolves around high-profile breaches and larger enterprises, this report stands apart with a unique mission: to prepare small and medium-sized businesses (SMBs) against the evolving tides of cyberthreats. At Huntress, we believe in empowering SMBs and the managed service providers (MSPs) who defend them with the knowledge, strategies, and tools needed to effectively protect themselves.

**The contents of this report reflect the notable adversarial behaviors, tradecraft, and trends we saw over the third quarter of 2023. Our aim is for this report to serve as your resource to understand, adapt to, and take action against the threats that target SMBs and those who protect them.**

In the past quarter, the Huntress team witnessed a continuing shift in the nature of threats against SMBs. Threat actors have largely moved away from malware-focused tactics. Instead, threat actors focus on non-malware mechanisms and abuse of legitimate tools and system commands in most incidents. Notably, 56% of recorded incidents in this time frame were, in essence, "malware free" across multiple types of intrusions. Of particular note is the increasing use of remote monitoring and management (RMM) software as an avenue of intrusion. In 65% of incidents, threat actors used RMM software as a method for persistence or remote access mechanisms following initial access to victim environments.



**56%** of incidents in Q3 2023 were "malware free"

**65%** of incidents in Q3 2023 involved threat actors exploiting RMM software

These trends are concerning, especially within the managed service provider (MSP) space. IT administrators, who rely on the same techniques and software that are now favored by threat actors, face an increasingly complex conundrum—distinguishing "good" from "bad" becomes a much more difficult task than it has been historically. Consequently, this may introduce an immediate need to move toward more behavior-based threat identification and a heightened focus on monitoring seemingly "legitimate" commands and software.

Furthermore, the migration toward cloud platforms and similar developments have placed an even greater premium on securing identities. Whether leveraged as an initial access mechanism through credential capture and replay, or for inbox access for information gathering, adversaries have migrated to cloud services along with end users to facilitate operations ranging from information theft to business email compromise (BEC) to pre-ransomware operations. Thus, MSPs and system owners need to extend their own visibility and security awareness beyond the traditional network perimeter to encompass external services and providers, as well as to fully capture the scope of identity-based actions and potential intrusions.

The following research reveals that the cybersecurity landscape for SMBs in Q3 2023 calls for a profound reassessment of defense strategies. The dominance of non-malware tactics, coupled with the exploitation of RMM software and identities, necessitates a nuanced approach to threat detection and response and expanding one's security purview beyond conventional perimeters.

# Quarterly Summary

-    -

-    -  
-    -  
-    -  
-    -  
-    -

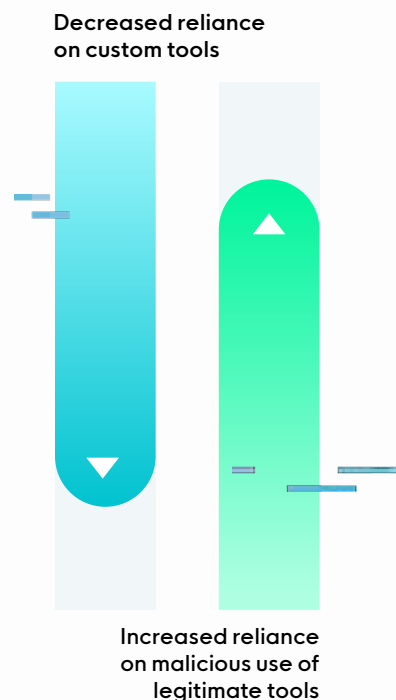
# Quarterly Summary

In Q3 2023, 40% of incidents responded to by Huntress analysts were categorized as “high” or “critical” in severity.

Reported items were distributed across Huntress monitoring mechanisms: [Managed Endpoint Detection and Response](#) and (increasingly) [Managed Detection and Response for Microsoft 365](#). This multi-pronged approach to security monitoring and response enables Huntress to review adversary operations across the attack lifecycle—from initial access and exploitation, through lateral movement and persistence mechanisms, to final adversary actions in victim environments.

Through further analysis and refinement, Huntress researchers were able to discern overall trends in the threat landscape facing SMBs—a sector typically overlooked or ignored in threat reporting. Huntress researchers identified several notable trends in adversary operations facing the SMB space:

- Decreased reliance on custom tools and especially malicious binaries in intrusions until final actions, such as ransomware deployment. As a result, many classic mechanisms for identifying or mitigating threats (such as pure anti-malware solutions) are less effective for countering intrusions.
- Increased reliance on malicious use of legitimate commands and tools, with particular emphasis on RMM software. The shift to RMM (as well as built-in system commands) means greater emphasis must be placed on behavioral analysis of adversary operations for detection and response.
- A highly diversified ransomware ecosystem including many families and strains that do not appear to impact many enterprises or similar entities, but are commonly found in the SMB space. This includes a diverse ecosystem of ransomware entities beyond “headline” entities and many commodity strains that are often dismissed in large enterprise security models.



## Intrusion Trends

Huntress focuses on defending the SMB—the organizations that are below the enterprise level and represent 99% of businesses in the US—and thus maintains distinct visibility from most other security firms. Within this visibility, we have identified continuing trends towards “living off the land” binaries (**LOLBins**) and credential compromise activity in Q3 2023. While custom or outright malicious tools still feature in events, adversaries are largely seeking to “blend in” to legitimate network operations through multiple mechanisms to evade detection and response.

At the SMB level, LOLBin use is especially concerning given the state of monitoring and review for many organizations. Many critical entities—from local school districts to medical offices—may find themselves at best leveraged for cryptomining or botnet purposes, and at worst, the victims of disruptive ransomware.

Figure 1 shows the distribution of tool “types” observed in Huntress-identified incidents, differentiating between compiled malware (e.g., a malicious EXE file), the use of scripting frameworks (such as PowerShell) for malicious activity, and the use of LOLBins and legitimate tools (including RMM software). While malware represents a significant portion of overall activity (44%), the remaining 56% of incidents are effectively “malware free.” Huntress thus observes a majority of incidents featuring LOLBin or similar abuse, or leveraging built-in scripting frameworks for actions.

### Tool Usage in Intrusions



Figure 1: Breakdown of Tool Usage in Intrusions



## **56% of incidents were “malware free,” meaning adversaries opted for exploiting scripting frameworks or legitimate tools in place of malicious software.**

The weaponization of legitimate tools, such as RMM tools in particular, remains an interesting and increasingly popular item in adversary arsenals. [As reported by CISA](#) and [others](#), RMM abuse is increasingly popular in intrusions for several reasons:

- The applications in question are legitimate software, thus evading anti-malware solutions.
- Many organizations already run RMM software, allowing adversaries to “blend in” to the environment.
- RMM tool use is not typically audited, especially in small organizations, allowing for multiple RMM frameworks to be observed in the same environment. This diffusion of tools defeats potential detections, such as identifying a “new” RMM framework different from an existing baseline.



From Huntress observations, RMM and remote access tools are distributed among several frameworks, with [ConnectWise ScreenConnect](#) figured most prominently, as seen in Figure 2 below.<sup>1</sup>

**RMM**, or remote monitoring and management, IT software that helps MSPs proactively locate, update, and monitor client endpoints.

Adversary choice of RMM tool, while interesting for trend analysis, is not necessarily as significant as the fact that adversaries are deploying some form of RMM in intrusions. In some cases, Huntress has observed adversaries diversifying among several RMM tools, such as using a combination of commercial and open-source items, to ensure redundant access to victim environments. Therefore, monitoring RMM tool use and deployment within defended or managed environments is an increasingly important security hygiene measure to ensure owners and operators can identify potential malicious installations.

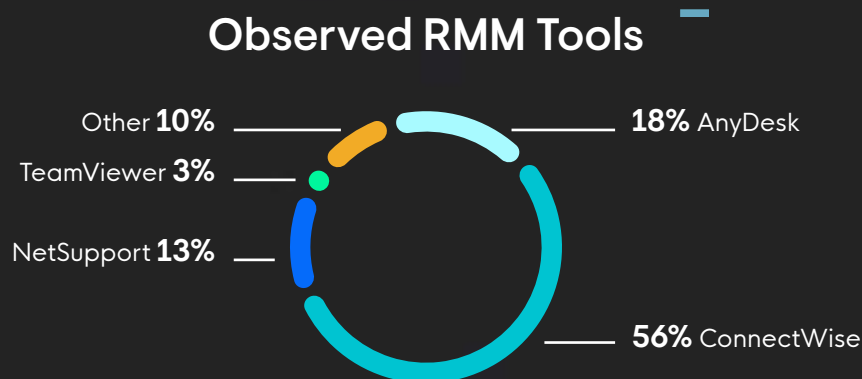


Figure 2: Breakdown of Observed RMM Tools

<sup>1</sup> While ConnectWise ScreenConnect, AnyDesk, TeamViewer, and NetSupport are not technically RMMs, for simplification we are aligning with CISA's categorization of these and similar tools.

# Identity-Focused Security

IT and business operations currently witness a growing importance of securing digital identities. Adversaries have set their sights on cloud services and identity-based attacks for initial access and the perpetration of fraud, such as [business email compromise](#) (BEC). These tactics have emerged as a favored intrusion vector for threat actors, and therefore should become a top priority for SMBs.

In Q3 2023, Huntress began rolling out its MDR for Microsoft 365 service. Even through initial trials and roll-out, Huntress has already observed a number of concerning trends in identity-based intrusions and manipulation, leading to actions such as mailbox manipulation and outcomes such as BEC. Unfortunately, data is not yet complete to enable trend analysis, but Huntress anticipates Microsoft 365 and related cloud targeting to continue growing as a concerning and popular intrusion vector through Q4 and into 2024.



Reviewing identified incidents, as seen in Figure 3, Huntress observes an overwhelming emphasis on [identity-focused malicious activity](#). Identity is something to be stolen, spoofed, or manipulated—and adversaries increasingly focus on precisely these mechanisms. Primarily, we’ve seen a greater concentration on manipulating or compromising communication channels, such as setting up malicious forwarding or other inbox rules, which make up 64% of observed Microsoft 365 incidents. Other activity includes attempting to compromise accounts, as seen in 24% of cases with logons from unusual or suspicious locations.

While the ultimate goal of such activity remains, in most cases, BEC, defensive visibility and adversary kill-chain dependencies mean these actions are largely caught at the account takeover (ATO) phase of operations.

Although ATO and related events present difficult detection and monitoring problems for analysts, Huntress has identified several methods to leverage anomalies in observed logon activity to detect malicious behaviors. In several instances, Huntress was able to identify intrusions in progress through analysis of [User Agent strings associated with Microsoft 365 login activity](#), using anomalous values to surface threat actor activity.

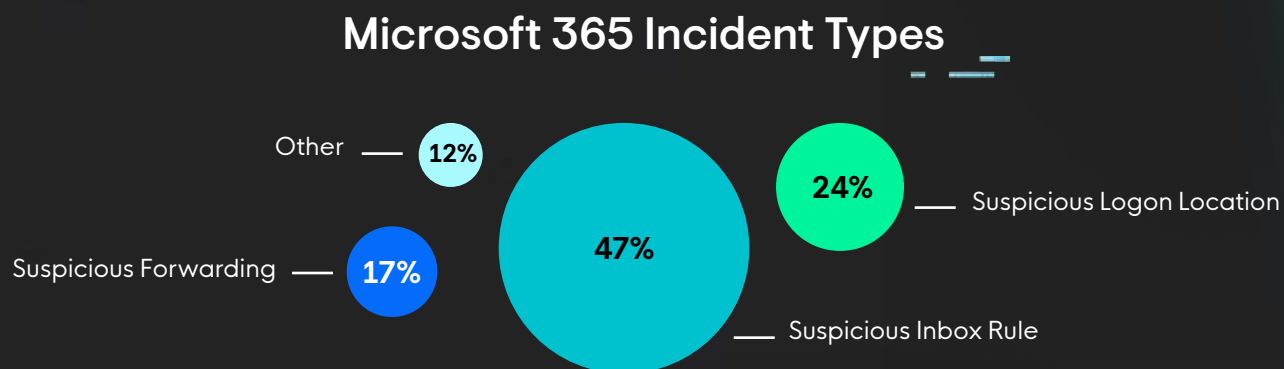
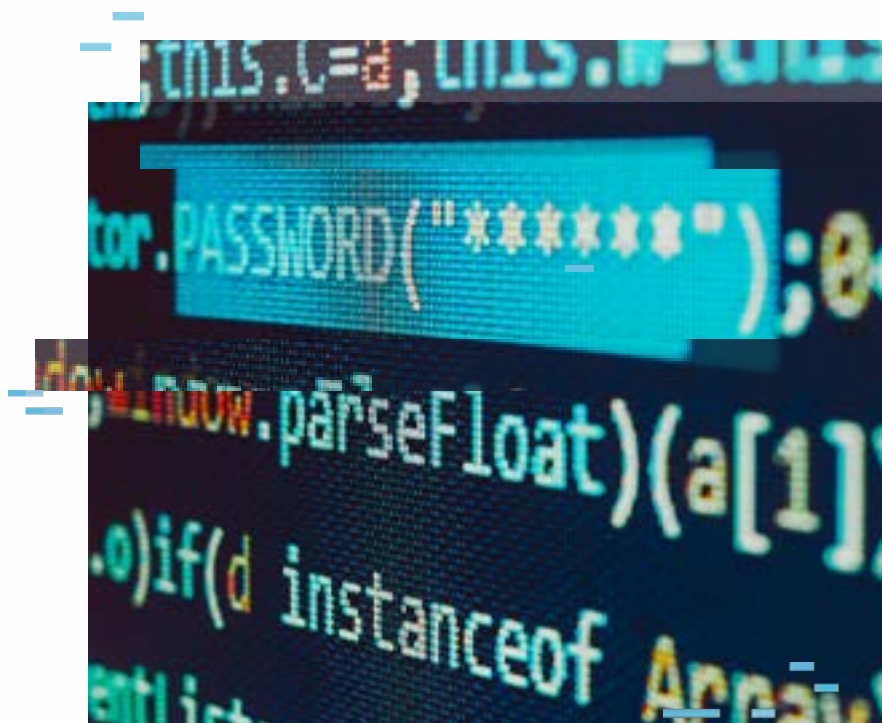


Figure 3: Breakdown of Microsoft 365 Incident Types

## Adversary Tooling & Behaviors

Trends in adversary activity—both the specific tools leveraged in intrusions and the more general behaviors that these items support—are critical in mapping the threat landscape. Identifying commonalities in adversary tradecraft as well as the convergence of operations on increasingly standard techniques can be of great value to defenders in orienting visibility and threat detection.

**Our research has illuminated the diverse spectrum of adversary tactics used today; including a significant reliance on the abuse of scripting frameworks, credential theft, and the exploitation of legitimate remote access software.**



Using the [MITRE ATT&CK framework](#), Figure 4 shows the behaviors most often observed in Huntress-detected incidents for Q3 2023. Notably, in one quarter (25%) of incidents, abuse of scripting frameworks ([T1059](#)) shows continued adversary reliance on built-in tools such as PowerShell, WMI, and related items for intrusion operations, amplifying the earlier observation on increased use of alternatives to compiled malicious binaries.

While representing a smaller fraction of overall incidents, Huntress response identifies nearly all intrusions (i.e., multiple incidents or compromised hosts can exist within a single organization's intrusion) feature credential capture in some fashion or at some phase of adversary operations. Operating system credential dumping ([T1003](#)) remains a critical component of the adversary intrusion lifecycle, with entities typically leveraging multiple possible techniques to access user credentials to enable lateral movement and remote process execution in victim environments. As described later in this report, migrating from single-factor authentication mechanisms to more robust multi-factor authentication (MFA) applications, especially for sensitive accounts such as domain administrators, is a critical security control to reduce attack surfaces and stymie adversary "break out."

## Adversary Intrusion Behaviors

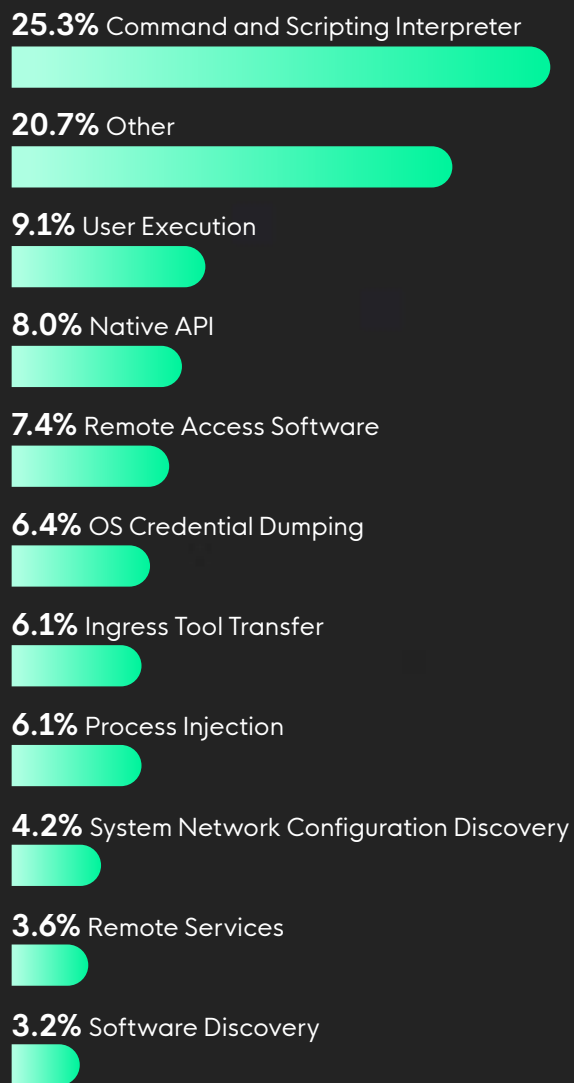


Figure 4: Breakdown of Adversary Intrusion Behaviors

As part of investigations as well as an integral feature of Huntress' Managed EDR product, Huntress gathers antivirus (AV) detections in addition to analyst identification of malicious software or related tooling. While AV detections for the identification of specific malware types can sometimes lead to incomplete or misleading results, analyzing overall trends based on functionality and malware type or classification can be enlightening to identify patterns in adversary use and activity.

The [coordinated takedown of Qakbot in Q3 2023](#) represents one of the more significant events in the identified time period and is partially reflected in Huntress data. Of note, [Huntress clients have been protected against Qakbot infections since late 2022 through the use of a "vaccine" approach to interrupt malware execution](#). While Qakbot has essentially been neutered from full execution, Huntress still observes its delivery and attempted execution, indicating its prevalence in the wild.

As shown in Figure 5, we have observed a declining number of Qakbot-related incidents over 2023, with approximately half as many events in Q3 as in Q1. While "zombie" distribution is likely to continue for some time, Huntress anticipates this to drop even further in Q4 to the point of near eradication.

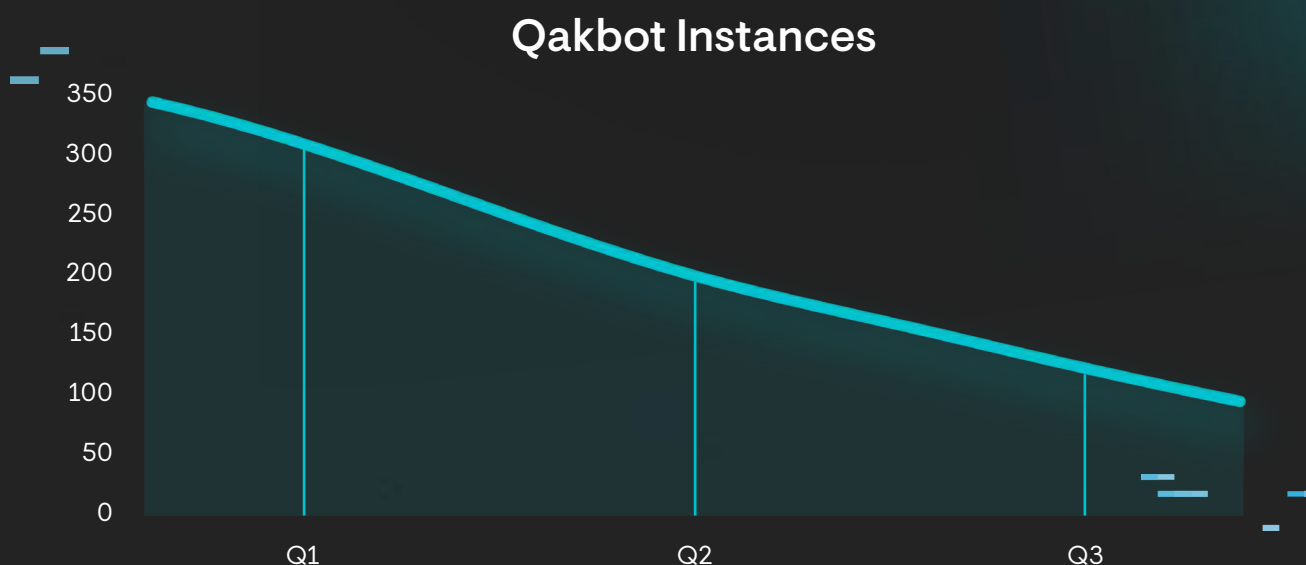


Figure 5: Trends of Incidents Involving Qakbot by Quarter

Aside from specific tool deployment, Huntress focuses significant research efforts on post-intrusion access tools. This perspective provides excellent insight into the tools and behaviors favored by adversaries once they gain access to a victim's environment. While items like Qakbot may recede, it is hardly alone in the information security landscape, and will rapidly be supplanted by other frameworks. Interestingly though, as seen in Figure 6 showing the identified applications in incident reporting, Huntress observations of post-intrusion tooling are heavily skewed toward legitimate applications.

The abuse of legitimate remote access software ([T1219](#)) for persistent access to victim environments is heavily observed in available data. Huntress identified RMM applications in the majority of incidents (65%) either installed by threat actors or abused by them after capturing credentials. RMM abuse is supplementing or replacing the use of other frameworks, such as [Cobalt Strike Beacon](#) or [Metasploit Meterpreter](#), in adversary operations. Additionally, RMM abuse offers adversaries the benefit of blending into legitimate remote administration activity and evading anti-malware security tools. Note that this view only covers those instances where applications were used to further an intrusion, while a number of incidents—nearly one third of the total as previously discussed—involve mechanisms such as LOLBins and credential capture to achieve adversary objectives.

## Post-Intrusion Access Tools Observed

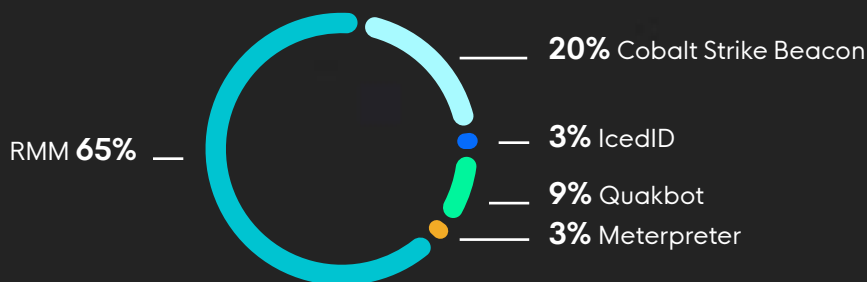


Figure 6: Breakdown of Post-Intrusion Access Tools Observed

Aside from intermediate tooling, ransomware continues to be a scourge across all organizations, from small businesses to large enterprises. Yet the small business perspective is interesting in providing a unique insight into ransomware affiliate or family deployment, which at times diverges from what is observed in enterprise networks. As seen in Figure 7, [LockBit](#) accounts for the majority of known-variant ransomware deployments observed by Huntress (25%). However, a long tail of uncategorized, unknown, or “defunct” (i.e., strains assessed to no longer be actively deployed) make up the majority of all identified ransomware events (60%).

While some new families continued to emerge in Q3 2023, such as [INC Ransomware](#) and [Akira](#), the overall outlook from the SMB perspective is on existing strains and, except LockBit, less well-known affiliates.

**60% of observed ransomware incidents were from uncategorized, unknown, or “defunct” ransomware strains.**

## Count of Ransomware Families

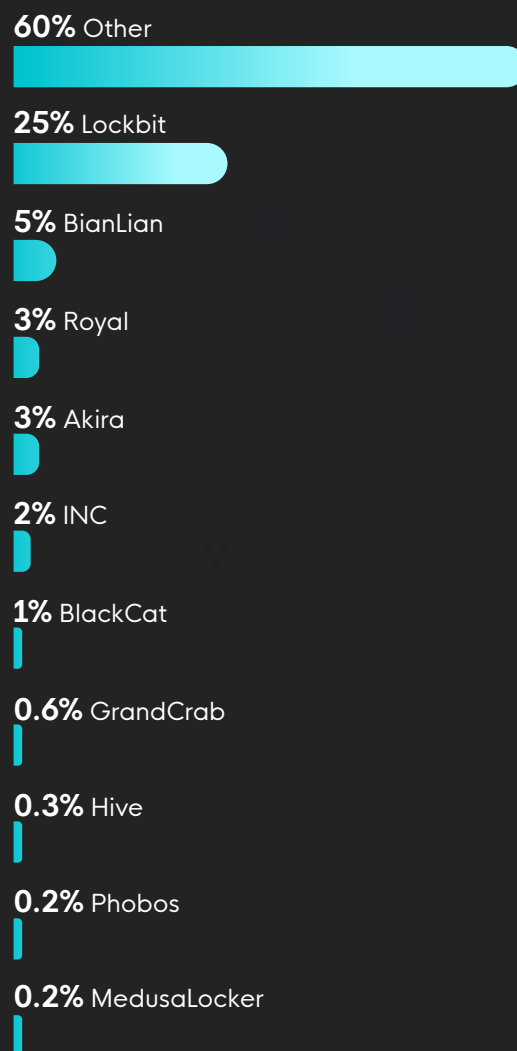


Figure 7: Breakdown of Ransomware Families Observed

# Adversary Trends



# Adversary Trends

**Phishing and end-user targeting remain common and widespread tactics for threat actors ranging from ransomware affiliates to BEC operators.**

Adversaries continue to leverage a consistent triad of initial access techniques: user-targeted phishing activity, credential theft and replay, and external-facing system or application exploitation. Some of these can be combined together (e.g., credential phishing activity to acquire login information, followed by replay against systems not enforcing multifactor logins), or deployed independently at scale (e.g., [MoveIT exploitation activity earlier in 2023](#)).

One of the key themes of Q3 2023 is an emphasis on “[hot zero day summer](#)”—a series of vulnerabilities disclosed in external-facing applications (such as MoveIT) or systems (such as [VPN concentrators](#), [firewalls](#), or [email security gateways](#)) enabling adversaries to rapidly establish presence in victim environments. Huntress, as a managed security vendor emphasizing system endpoint visibility, is seldom directly involved in the first phases of such intrusions, as they take place against dedicated appliances with custom operating systems and similar limitations. However, Huntress frequently observes the follow-on impacts of such activity, where an exploited externally-facing system becomes “patient zero” for subsequent lateral movement in the victim environment.

While garnering significant attention, adversaries do not rely on vulnerabilities alone for initial access. Phishing and end-user targeting remain common and widespread tactics for threat actors ranging from ransomware affiliates to BEC operators. Yet the nature of such phishing has shifted significantly since [Microsoft disabled macro execution](#) by default in Microsoft Office as well as earlier “[Mark of the Web](#)” [security controls implemented for Visual Basic for Applications \(VBA\) scripts](#).

As a result, adversaries continue to look for [new payload mechanisms to deliver malicious content to end users](#). Interestingly, many of these methods require significant user interaction for successful execution. Huntress observes this trend with payloads landing on victim machines such as ZIP or ISO archives containing malicious LNK or scripting objects, requiring multiple interactions from victims from initial delivery to execution.

In other instances, adversaries leverage new access vectors to interact with end users. For example, [TrueSec published on activity leveraging Microsoft Teams for distributing phishing links](#) in early September 2023. Huntress identified similar activity between September 6–8, 2023, leveraging LNK objects masquerading as PDFs to encourage user interaction, resulting in the installation of [DarkGate malware](#). Examples of payloads include the following objects:

File Name	SHA256
Fresh_Mission_and_Core_Values.pdf.lnk	3f1ffd99e31fb9c3568369565ed0a3bf2 f81553044cb28b3adafb1b61f423f33
Company_Transformations.pdf.lnk	a4ee4fff22ccafa9a92fbd74d70f005e3 03297682b88421769798c28da0c8397
Position_Guidelines.pdf.lnk	784974fd06397cab27761cbef5a2e3dd b58bedfb13580292b70dc24907f63fd
Revamped_Organizational_Structure.pdf.lnk	14d26d8e50fa0b14c4bd63754e87dc53e 93fdc0699b12e7ac7adc35a6726eede
Employees_Affected_by_Transition.pdf.lnk	9789e08b4768fe414644b2c1f5cdc8af9 e2ee63f279a0628564e53340057d684

Demonstrating that indicator analysis and research can be valuable for defenders, all of the above payloads, along with those identified by TrueSec researchers, leveraged the same hard-coded command and control server: **5.188.87[.]58**. Additionally, object metadata within the LNK files themselves show identical records for the creating system, tying all samples back to a single entity. Focusing on the C2 node, references to that IP address in various repositories reveal a variety of LNK objects communicating with it from September 1–20, 2023.

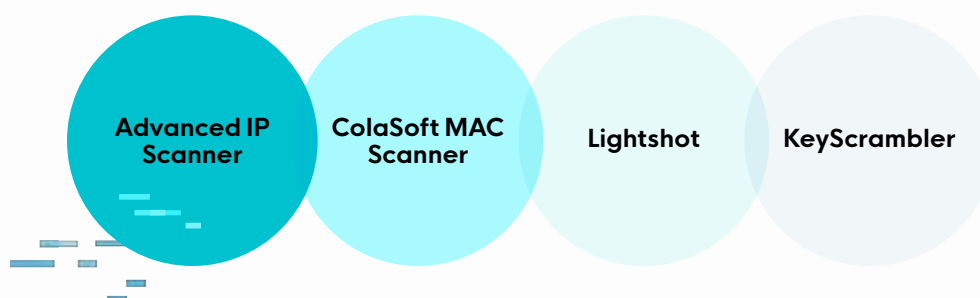
Overall, such activity demonstrates continued adaptability by adversaries to avoid known detection and alerting mechanisms, such as email monitoring for phishing activity, while migrating toward areas with little or no monitoring, such as chat applications. Along with the above, adversaries will utilize these mechanisms—such as LNK files masquerading as documents—to launch what are ultimately sequences of legitimate system commands to retrieve and install malicious payloads.



# Additional DarkGate Observations & Software Impersonation

Roughly simultaneously with the Teams-focused campaign described previously, DarkGate continued to evolve beyond direct phishing to likely search engine poisoning and social engineering victims to download legitimate software from malicious resources.

**In observed intrusions, Huntress identified a variety of legitimate applications “spoofed” for delivering DarkGate payloads, such as:**



Notably, the malicious variants of the above software are provided as MSI files, whereas the legitimate versions available on company websites are all EXEs. After coercing or convincing a victim to download a malicious software package masquerading as a legitimate download, execution would result in an LNK created in the user's StartUp folder as a persistence mechanism to load on start a DarkGate variant. The DarkGate variants themselves are run as AutoIT3 payloads.

After early September 2023, Huntress identified additional infection or distribution vectors for DarkGate. Examples include archives with malicious VBS scripts that retrieve and execute a remotely-hosted payload. Based on file locations and other data, Huntress assesses with high confidence that the archives were delivered via phishing. Notably, in this activity, Windows Defender was able to identify and quarantine the malicious VBS object, but only **after** it had succeeded in running, resulting in an infected victim. This observation emphasizes the need for organizations of all sizes to practice defense in depth, combining anti-malware solutions with endpoint visibility.

# Continued AsyncRAT Infections & Process Chains

**AsyncRAT** is a remote access tool (RAT) designed as an [open-source RMM tool](#). First emerging in 2019, the tool has rapidly expanded as a simple, freely available post-exploitation tool observed in multiple incidents investigated by Huntress.

In Q3 2023, Huntress observed convoluted infection chains starting with downloaded HTML files (likely delivered via phishing) leading to the download of password-protected archives. When opened, the archives would extract and launch a WSF file leading to a PowerShell command to download and run `1.txt` from `185.81.187[.]219`. The TXT file, in reality, is a script that creates a BITS job on the victim host to download an additional archive, in which resides a further VBScript object. This final object spawned a PowerShell command that created a Scheduled Task to run every two minutes on the host, each time compiling AsyncRAT from the source and executing it.

While AsyncRAT is neither rare nor especially advanced, sequences such as the below chained operations are frequently observed to install commodity tools such as this to enable persistent access to victim devices. In the case of legitimate tool abuse or leveraging LOLBins for this activity, visibility into processes and process relationships is critical to identify nested execution and various phases of de-obfuscation required for adversary success. Through endpoint visibility and monitoring, such relationships can be identified to allow for follow-on investigation and response.

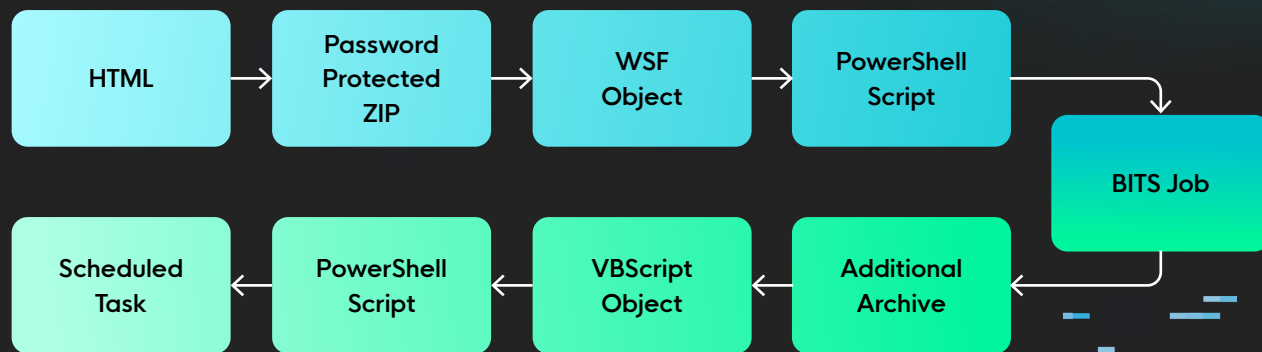


Figure 8: Infection and Process Chain of AsyncRAT

# Espionage in the SMB Environment

Huntress identified and responded to intrusions at a small enterprise in the defense industrial base (DIB) in Q3 2023. The intrusion, despite penetrating deep into the victim's environment and having a dwell time of several weeks, did not result in ransomware or similar monetization behaviors. Instead, Huntress analysts observed systematic identification and collection of sensitive files related to defense projects. While exfiltration was not directly observed, overall, the intrusion in question has all the hallmarks of an espionage-focused, intellectual property theft-related campaign.

Instead of leveraging exotic malware or similar, custom tools, all actions observed by Huntress aligned with credential harvesting, credential reuse, and living-off-the-land behaviors, combined with some script execution. Irrespective of the "common" nature of the adversary's tactics, techniques, and procedures (TTPs), they were very effective in achieving (or nearly achieving) perceived goals in information collection.

## Several lessons emerge from this activity:

- First and foremost, sensitive areas of national economies, including the DIB, extend well into the SMB space, with many enticing targets for state-directed or -supporting entities to pursue.
- Intrusions into such organizations need not rely on exploits or exotic tradecraft to succeed, but may operate through mechanisms familiar to junior pen-testers to achieve success.
- Increasing visibility and monitoring of such environments is necessary to identify such intrusions when they take place and to counteract such events where possible.
- Implementing increasingly standard security controls, such as MFA, are not mere luxury items but necessary steps in defeating intrusions of multiple types and provenance.

Given the nature of the intrusion, no firm indicators of compromise exist as the adversary relied exclusively on built-in system commands and ephemeral scripting activity. The lesson learned from this activity is the necessity of performing behavior-focused monitoring and alerting for the abuse of legitimate applications for malicious purposes.

# Response & Defensive Guidance




## Response & Defensive Guidance

**Visibility remains key to defense. Particularly given trends in adversary operations, relying more on abusing legitimate applications than distributing custom code and tools, the ability of organizations to identify and differentiate “malicious” from “normal” and “benign” is vital to enable meaningful, useful defense.**

Overall trends toward increasing RMM software abuse, credential theft, and identity spoofing demand defenders work harder to classify and understand actions taking place within monitored environments.

Note that visibility now extends well beyond just the systems and networks managed by MSPs or owned by given organizations. Visibility now must incorporate third-party and cloud-based services as these become tightly integrated with business operations and critical organizational functions. Understanding this new, “perimeterless” paradigm in operations and developing mechanisms to monitor and defend these environments is thus critical to maintaining a secure posture in the cloud era.


In line with the above trends, implementing MFA across all available systems (and especially ALL externally facing or publicly available systems) is now a minimally acceptable security measure given threat actor behaviors. Defenders must assume that any single-factor authentication system exposed to the internet will be compromised eventually, either through brute force or credential theft. However, adversaries increasingly identify mechanisms to [circumvent MFA through strategies such as token theft](#).



**As a result, relying purely on preventive measures for identity theft is insufficient. Defenders must implement visibility, monitoring, and profiling of identity activities as well to identify almost inevitable abuse or compromise.**


Beyond external access, legitimate credentials remain key to adversary operations following initial access. Whether dumping credentials from system memory or opportunistically identifying passwords recorded in clear text on disk, adversaries consistently and meticulously look for ways to subvert trust within victim environments. At minimum, organizations must look to enforce MFA for critical accounts such as local and (especially) domain administrator accounts, work to limit the use and access to these privileged accounts, and then audit their use to better identify their abuse by threat actors.

Adversaries continue to identify and exploit vulnerable systems exposed to the internet. While phishing remains an initial access concern, server- and application-side exploitation makes up an increasing percentage of intrusions. Unfortunately, many of these systems, such as VPN concentrators or email security gateways, are often highly customized systems with non-trivial difficulties in logging activity from them. Defenders must instead combine preventive measures such as rapid patching, attack surface reduction, and enhancing visibility within the network to identify potential post-exploitation activity and lateral movement.




Overall, the above recommendations must not take place in isolation, but rather need to be combined into an effective defense-in-depth posture for merely adequate security. As seen in examples in this report, adversaries leverage multiple techniques and strategies to obfuscate or evade detections, meaning simple reliance on anti-malware as a safeguard is no longer sufficient, especially when combined with LOLBin abuse. Thus layering defensive visibility across artifacts, such as potentially malicious files, host commands and actions, and even network visibility and communication, remains necessary to catch even supposedly “commodity” adversaries in the current ecosystem.

Finally, a common theme across multiple examples, whether socially engineering users to run a file or spoofing identities to generate a BEC attempt, is the subversion of user trust. Adversaries know that users face significant hurdles in their day-to-day jobs and often rely on implicit trust in systems or other persons to effectively carry out tasks. [Security awareness training](#) and user education can work to inform end users of the risks inherent in current processes and tasks, while managers and other leaders should look to build more resilient processes to combat adversary attempts to abuse existing functional pathways.



**Layering defensive visibility across artifacts, such as potentially malicious files, host commands and actions, and even network visibility and communication, remains necessary to catch even supposedly “commodity” adversaries in the current ecosystem.**



# Conclusions\_

— — —

— — —




## Conclusions

Q3 2023 demonstrated that there is no slowdown in the information security space. More importantly, from a Huntress perspective, the landscape remains a difficult one for the majority of organizations that lack the resources and expertise residing in enterprise network environments. Whether for monetization purposes through ransomware or BEC, or potentially even state-directed espionage activity, SMBs remain at risk from a variety of entities.

More worryingly, these adversaries are taking advantage of “holes” in our visibility and awareness to subvert or avoid many legacy security controls. Whereas once upon a time, a small organization could likely “get by” with a combination of a good anti-malware solution and spam filtering, the current threat landscape renders these simplistic (if historically reasonably effective) efforts no longer satisfactory.

In addition to learning about adversary tendencies and operations, business owners and network administrators must also understand how adversaries increasingly take advantage of the very nature of modern networks and distributed environments.



**The path forward entails a dual-pronged approach—enhancing visibility into events while simultaneously reducing the available attack surface. This adaptive approach is indispensable in coevolving with threat actors in today’s ever-changing cybersecurity landscape.**

# About Huntress

Huntress is the leading cybersecurity partner for small and mid-sized businesses (SMBs) and the managed service providers that support them. Combining the power of the Huntress Managed Security Platform with a fully staffed 24/7 Security Operations Center (SOC), Huntress provides the technology, services, education, and expertise needed to help SMBs overcome their cybersecurity challenges and protect critical business assets. By delivering a suite of purpose-built solutions that meet budget, security, and peace-of-mind requirements, Huntress is how SMBs defend against cyberattacks.

[Learn More](#)

Start a free trial **today.**

