
2024 Cyber
Threat Report
HUNTRESS

Table of Contents

Executive Summary

This past year, threat actors showed their true colors. From exploiting trusted tools to fly under the radar, to crossing lines and targeting vital industries like healthcare, their actions prove that nothing is off the table.

However, since many of today's cybersecurity protections are designed for large enterprises, the businesses that fall below this line get caught in the crosshairs. It's these businesses that serve as a testbed for attackers to try out new tactics and techniques, as well as establish their initial footholds. And it's these businesses that Huntress has unique insight into and aims to protect. With this visibility, Huntress' security and research teams often see trends before they are seen by larger, enterprise-level companies.

This report presents the notable adversarial behaviors, tradecraft, and trends we saw across all of 2023. It offers key insights into the threat landscape, focusing on the heightened risks that non-enterprise businesses and managed service providers (MSPs) face in light of recent cybersecurity developments. By examining these trends, our goal is to equip businesses of all sizes to better prepare and protect themselves from modern cyber threats.

One major shift occurred in August 2023, when the Qakbot infrastructure was dismantled. This event led to a significant change in the behavior of cybercriminals, including the proliferation of ransomware attacks and the innovative misuse of remote monitoring and management (RMM) tools.

In addition to ransomware and RMM tool abuse, we've seen other emerging threats like the misuse of cloud storage services, credential dumping, and business email compromise. These tactics are becoming increasingly sophisticated and challenging to detect, posing ongoing threats to businesses of all sizes and sectors.

Background

Huntress published a report in November 2023 covering the cyber threat landscape for small and medium-sized businesses (SMBs). Our analysis, based on monitoring several thousand organizations across over two million distinct endpoints, identified a number of key trends in the SMB cyber threat space:

Decreasing use of traditional malware in intrusions, with adversaries increasingly moving toward a combination of "living off the land" binaries (LOLBins) and malicious scripting objects.

Increasing use of legitimate software tools, such as remote monitoring and management (RMM) software along with other commercial applications, in lieu of custom remote access tools (RATs).

An increasingly diverse ransomware threat landscape with multiple affiliates and entities operating beyond the organizations that frequently appear in enterprise ransomware incidents.

Adversary targeting of victim identities, especially in cloud and cloud-services environments, to facilitate initial access or for immediate targeting through business email compromise (BEC) and similar attacks.

Based on the above trends, Huntress reviewed data and findings covering the entire year of 2023 to determine if these trends have changed, or if there was any significant fluctuation throughout the year.

Threat Types & Trends

HUNTRESS

Threat Types & Trends

Remote Access Abuse

If there's anything that last year made clear, it's that hackers made it their mission to master the art of disguise. One notable trend that has remained consistent is the weaponization of legitimate tools to hide in plain sight, particularly remote monitoring and management (RMM) tools.

The Huntress team has observed that RMM tools were still heavily abused to achieve remote access and control over systems. Of the known RMM tools, ScreenConnect (15%) and Atera (12%) were the most prolific RMM tools used illegitimately, as seen in Figure 1. RMM tool abuse is also on par with other available attacker tools, such as Cobalt Strike (7%). This indicates that attackers are able to accomplish much of their campaigns with off-the-shelf tools that are widely available instead of having to craft new novel tools, thereby lowering their bar of entry and allowing them to blend in within the target's environment.

The problem with these types of attacks is that end users can spin up a trial RMM version without any real verification of who they are. This makes it easy for attackers to utilize them with impunity. Therefore, there's a potentially missed opportunity on behalf of the software providers to help thwart would-be attackers by locking down random trials by illegitimate entities.

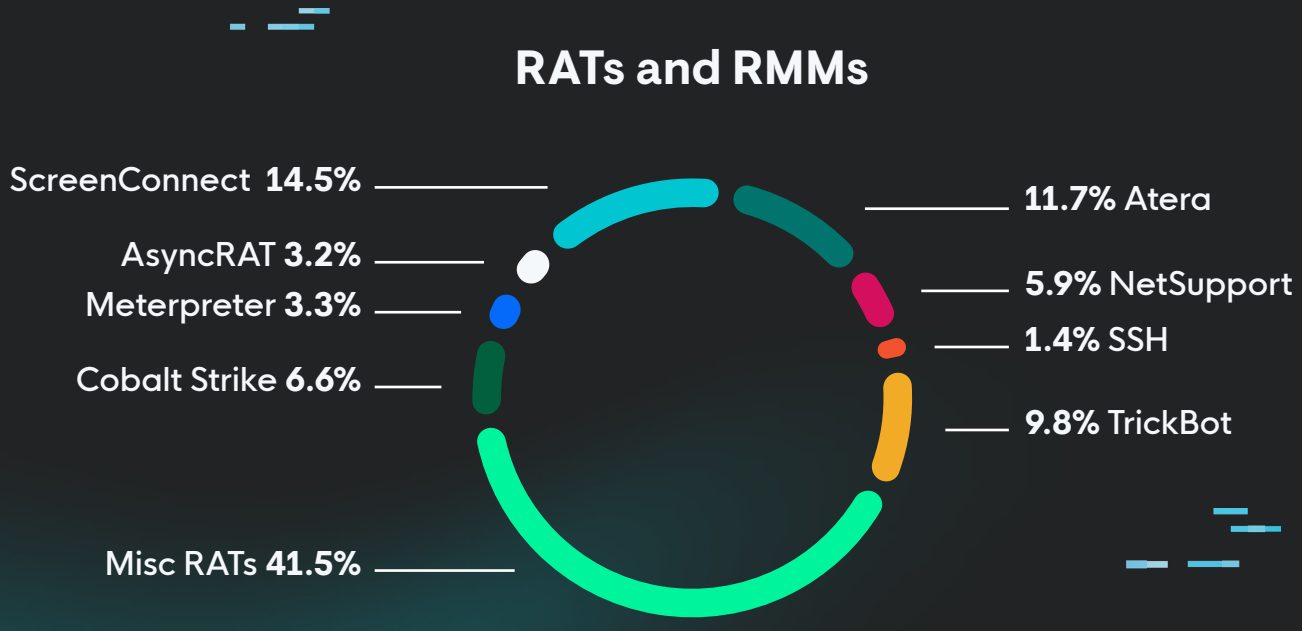


Figure 1: Various remote access tools, both legitimate tools and malicious RATs

HUNTRESS

Threat Types & Trends

Cloud Storage in Attacks

In a similar trend, threat actors are finding ways to evade detection by abusing trusted applications like cloud storage services. Attackers often make use of cloud storage in their attacks, either as a delivery mechanism, or a place to exfiltrate data for offloading.

We were able to identify the most common infrastructures utilized by attackers within our customer demographics, as shown in Figure 2. OneDrive was the most common at almost 79%, while Google came in at 18% and Dropbox took up a little over 3% of the three most common cloud storage technologies.

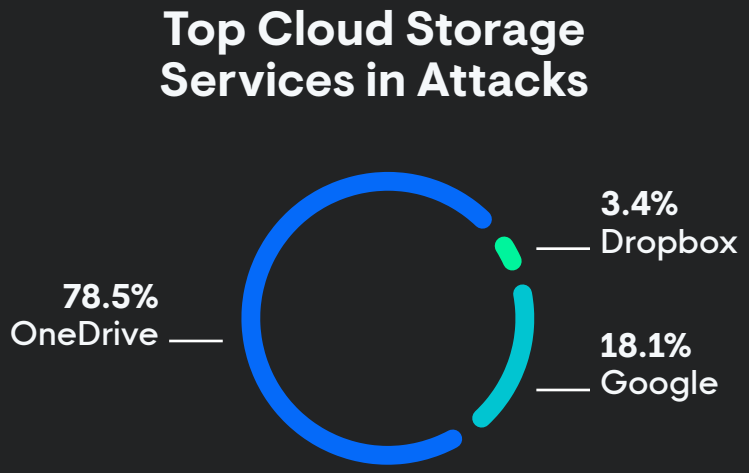


Figure 2: Breakdown of the top cloud storage services misused in incidents

HUNTRESS

Credential Dumping Tools

Attackers will often try to dump credentials in order to move to other endpoints and resources within a targeted network. One of the other trends seen in our data was the range of various tools and techniques used to dump credentials. As seen in Figure 3, most of our reports (54%) of the tools used by attackers were off-the-shelf, known tools, such as Mimikatz, Kerberoasting, Procdump, etc.

Of the 40% of miscellaneous tools and methods, most of those consisted of known system tweaks (registry modifications), or lesser-known, but freely available hacker and administrative tools. About 6% of the reports filed were new methods exposed by hunting methodologies. Therefore in total, around 94% of the credential dumping methods employed by attackers in our customer base could have been mitigated by various blocklisting techniques.

Credential Dumping Methods

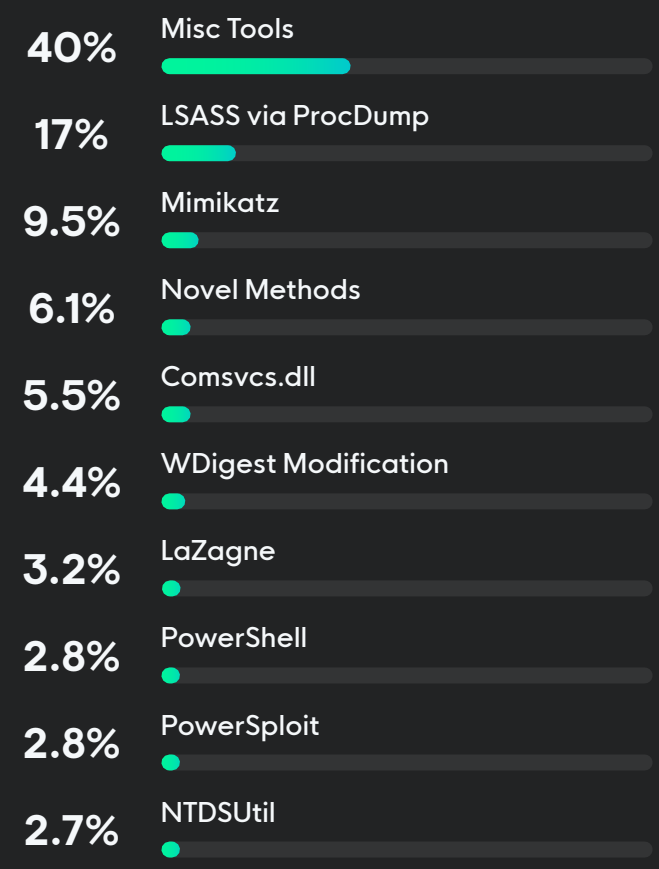


Figure 3: Breakdown of most commonly used credential dumping tools

HUNTRESS

Disruptions in the Ransomware Food Chain

Disruptions in the Ransomware Food Chain

Late 2023 witnessed a number of interesting developments in threat actor activity when looking at specific entities and their operations and tooling. Overall, while many of the specific tools and techniques associated with threat actors remain relatively stagnant (due to their continued success), specific threat actors and their targeting show interesting shifts over time. One of the more fascinating trends was how ransomware activity surged after a top predator in the food chain was taken down—prompting other groups to try and elbow their way to the top.

Disruptions in the Ransomware Food Chain

Qakbot Takedown

One of the most significant developments last year was the US Department of Justice-led takedown of the Qakbot malware distribution and control network in late August. While Huntress customers have been shielded from Qakbot installations for some time, Qakbot represented a widespread, concerning threat for initial access and information gathering for a variety of threat entities. Its abrupt disappearance therefore represented a rare, but significant, "win" for network owners and defenders.

Unfortunately, multiple sources in mid-December 2023 identified what many predicted would likely occur: a resumption of Qakbot activity. Preliminary analysis of available samples indicates that the "new" Qakbot variants are functionally similar, if not indistinguishable, from pre-takedown variants. As a result, existing defenses and controls are still working as of this writing. While emerging Qakbot variants remain relatively unchanged, their emergence is a strong signal that, like the reappearance of Emotet in similar circumstances, threat actors will attempt to capitalize on existing knowledge and investment in the face of defender activity.

While the takedown did appear to have a significant impact on Qakbot infections, Huntress continued to observe residual Qakbot incidents, as well as an increase after a couple of months had passed. While some of these were from new customers who were already infected before monitoring was put in place, it is unknown if the majority of infections during the takedown period were older variants that were installed prior to the Qakbot disruption.

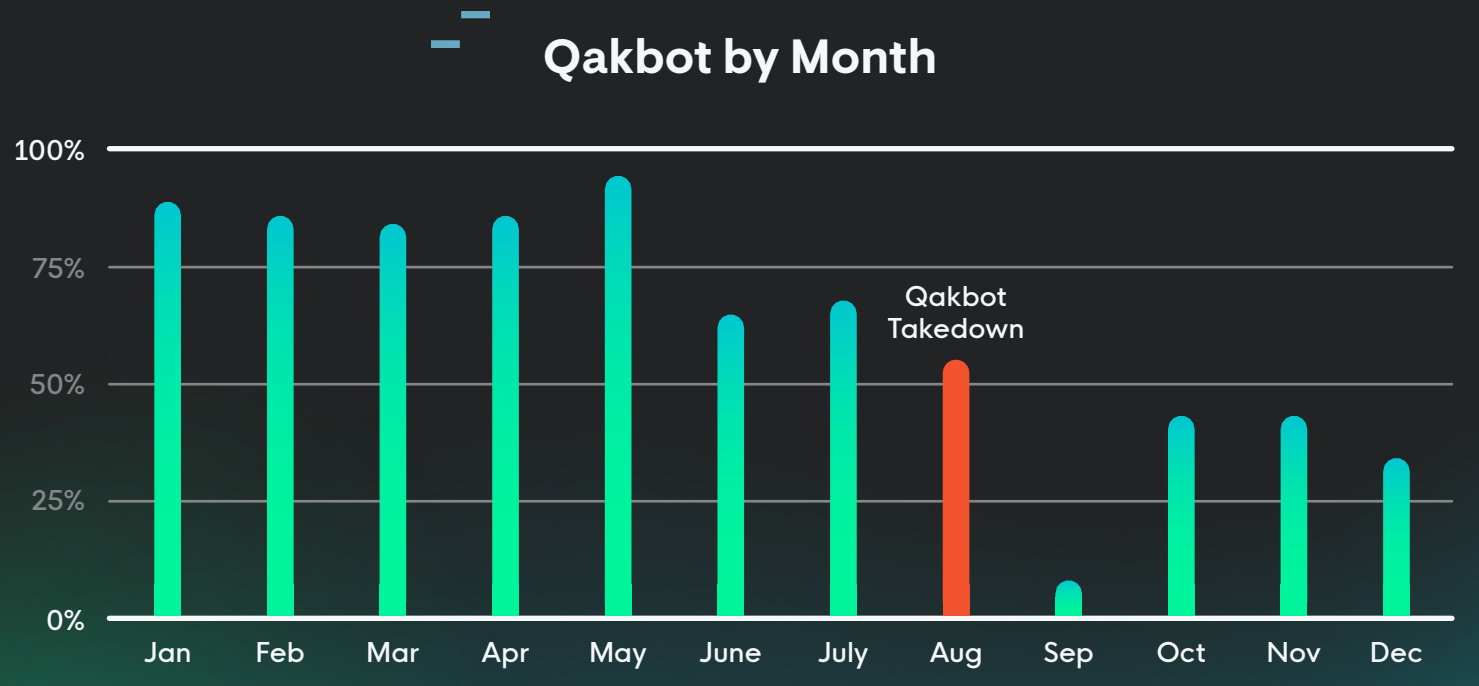


Figure 4: Volume of incidents involving Qakbot in 2023

HUNTRESS

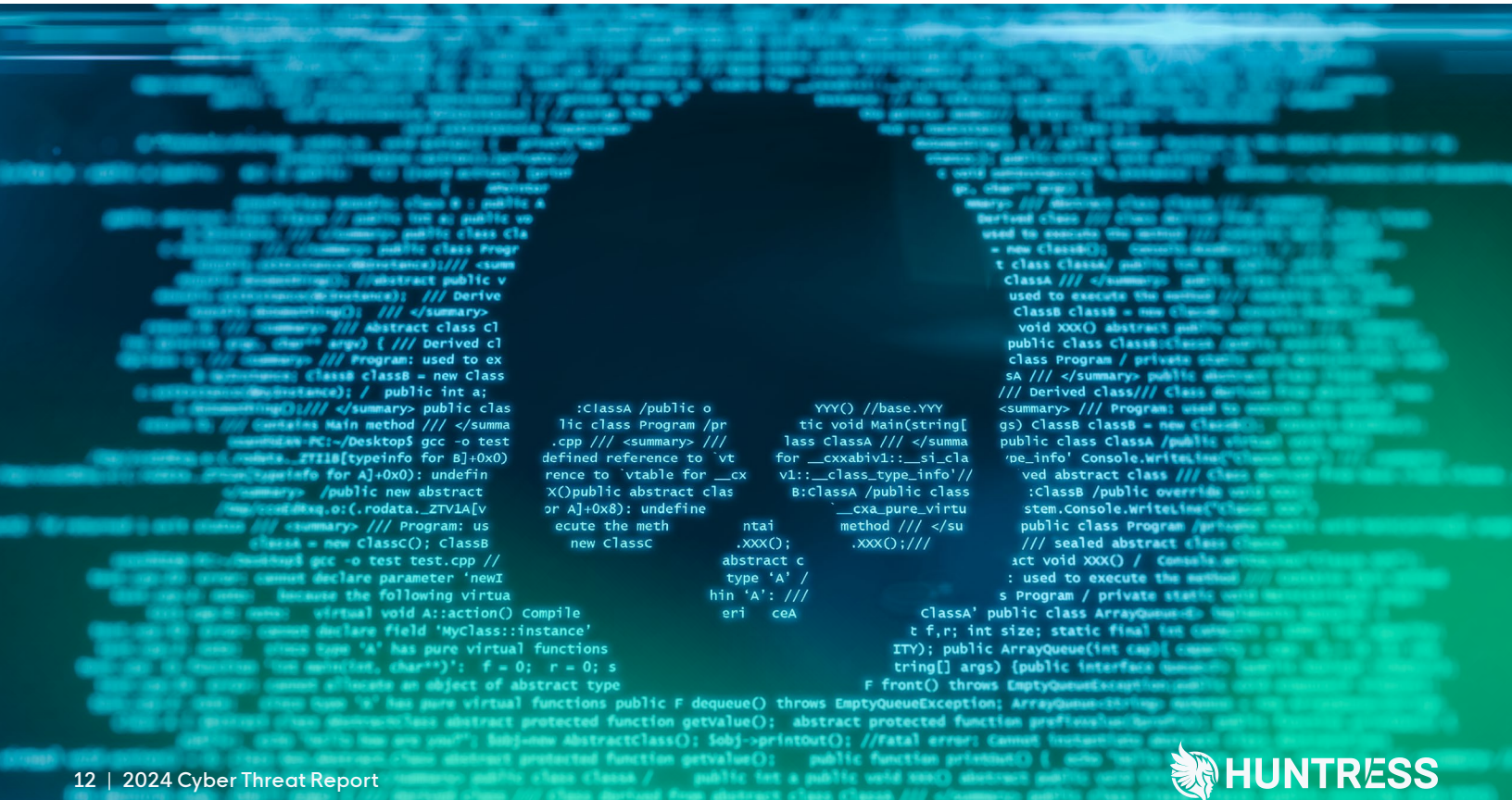
Disruptions in the Ransomware Food Chain

Increased Ransomware Activity

Post-Qakbot takedown, there has been a notable surge in ransomware activities as cybercriminals seek to fill the void left by Qakbot's absence. Small businesses and MSPs are particularly vulnerable due to generally lower levels of preparedness and cybersecurity infrastructure:

Variety of Threat Actors: New and evolving ransomware groups have been quick to capitalize on the gap, adapting existing malware strains and developing new vectors to exploit business networks.

Targeted Ransomware Campaigns: There has been an increase in ransomware attacks specifically aimed at small businesses and MSPs, which are often seen as entry points to larger networks.



HUNTRESS

Disruptions in the Ransomware Food Chain

Year-end Ransomware Activities

One interesting trend that we observed was more diversity in ransomware families in the wake of the Qakbot takedown that took place in August 2023. Qakbot was the reigning strain of malware used by initial access brokers up until its takedown—and after this, we saw a notable spike in activities from August to September from DarkGate (880% increase), Akira (510% increase), LockBit (102% increase), and Play (45% increase). In Figure 5, we can see the relationships between Qakbot and how various ransomware strains picked up in the wake of its takedown.

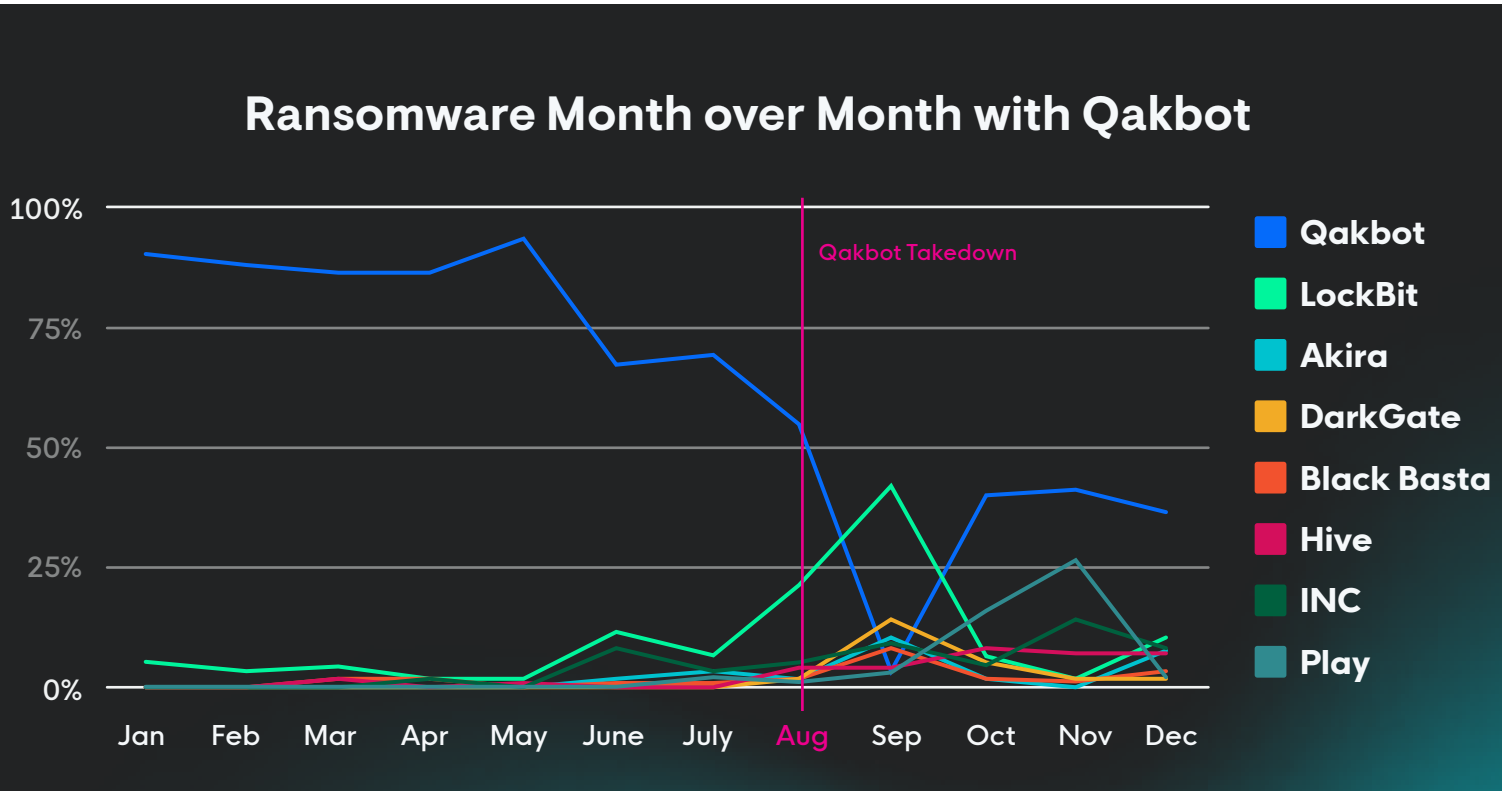


Figure 5: Volume of ransomware variants with Qakbot initial access malware

HUNTRESS

It's clear that there were some other variables at play within the ransomware ecosystem last year.

In Figure 6, we see that there was an increase in activity involving Emotet, which is another initial access malware, right before the takedown of Qakbot occurred. Emotet activity steadily elevated for some time as Qakbot was all but eliminated, but then there's an immediate dip as Qakbot came back online in November. The lines then trend in opposite directions in the month of December, where Qakbot trends down and Emotet rises once again, indicating how closely coupled the relationship between these two families is.

Just as in nature where predators are territorial, and keep other predators at bay from their area, it appears that ransomware operators are not unlike nature's predators in the wild. Unless a threat is eliminated entirely, lethal actions often only result in dips in activities until newer, or adapted threats move in to take their place. While it is shown that predators can live in harmony with prey when certain deterrents are employed to keep them at bay, the argument against takedowns like what was witnessed against Qakbot and LockBit within the last year should be carefully considered before the landscape shifts out of control.

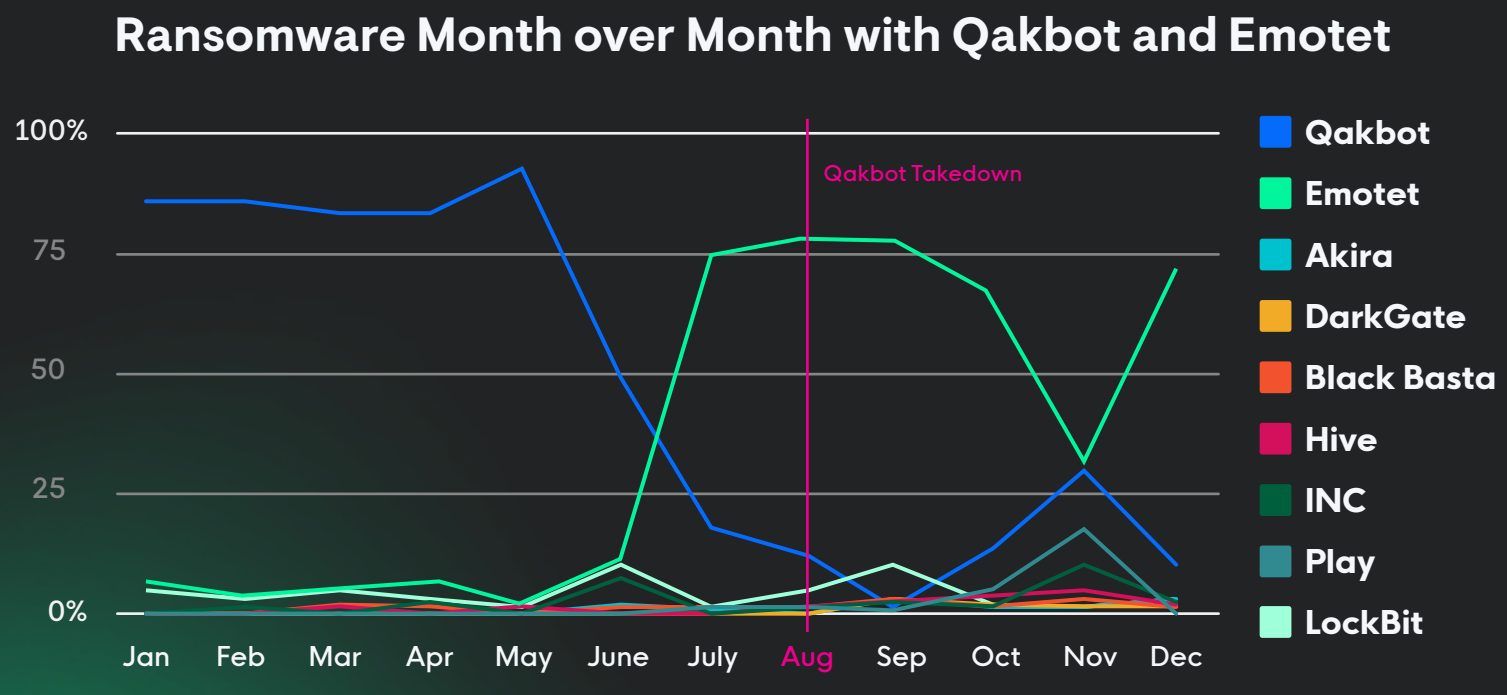


Figure 6: Volume of ransomware variants with Qakbot and Emotet initial access malware

Disruptions in the Ransomware Food Chain

Ransomware Variation & Proliferation

As discussed in our previous threat report, the SMB space faces a variety of ransomware affiliates and variants in identified events. While some ransomware or related affiliates, such as LockBit or ALPHV, remain persistently active across both enterprise and SMB environments, a number of other entities continue to build "market share" in SMB-focused intrusions. While the "long tail" of ransomware threats remains significant, Huntress observes increasing instances of both Play and Akira ransomware variants in SMB environments.

In addition to SMB-related activity, ransomware affiliates increasingly target smaller critical infrastructure entities and their service providers. Examples include healthcare systems and providers, and municipal cooperative utilities. Results of such incidents range from interruption of services, as seen in Ardent Health Services diverting ambulances in November 2023, to the leaking of patient information, as observed in an ALPHV-related incident impacting Lehigh Valley Health Network.

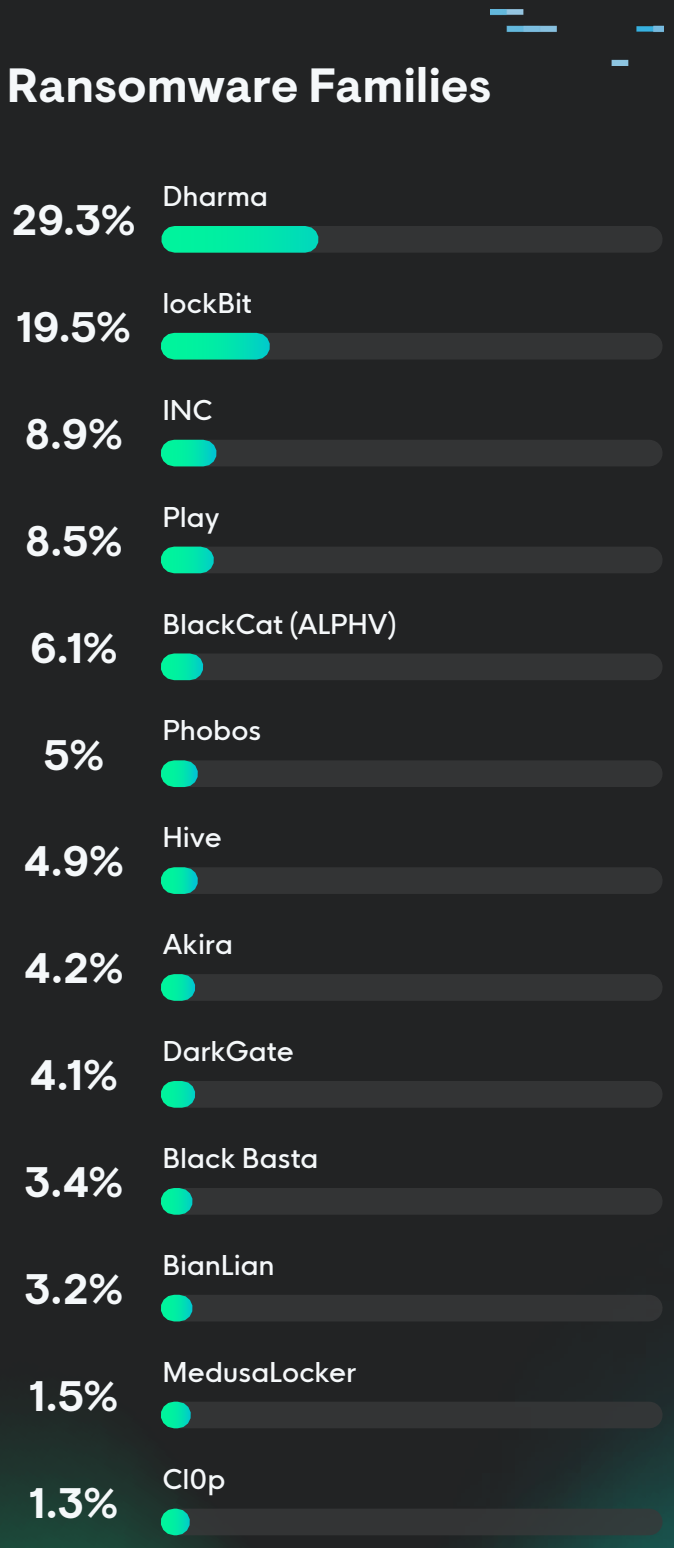


Figure 7: Breakdown of ransomware families seen in incidents from 2023

HUNTRESS

Inside the Threat

DarkGate

DarkGate is commodity loader malware with an extensive feature set that can include keystroke logging, info stealing, and more. Huntress analysts began reporting a number of incidents involving the download and installation of DarkGate in August 2023—most of which were the result of malicious ads, or "malvertising." In these incidents, a user searches for a popular network scanning tool, such as the Advanced IP Scanner, or the ColaSoft MAC Scanner, and is then offered a download site for the tool via a malicious ad. The resulting download is a Microsoft Installer (.msi) file (rather than the legitimate .exe installer executable), which includes the scanner along with the DarkGate loader installation. The resulting DarkGate installation is easily detected, allowing Huntress SOC analysts to identify and report the alert to the customer in a timely manner, often isolating the endpoint and preventing further ensuing issues. Our SOC analysts continued to report DarkGate infections to customers through August and into October 2023.

Inside the Threat

INC Ransomware

In August 2023, Huntress analysts detected an endpoint that had files encrypted using the INC ransomware. Further investigation of several involved systems revealed that the threat actor performed several actions while accessing endpoints, including data collection via 7Zip, and likely data exfiltration via MegaSync.

Then in November 2023, Huntress analysts investigated another endpoint with files encrypted via the INC ransomware variant with markedly different TTPs from the August incident. This time, the threat actor accessed a domain controller and then launched the Group Policy Management Editor via the Group Policy Management Console. This was a key part of the attack because the threat actor used PSExec and WMI to push a batch file to remote endpoints, and the first line in that batch file was a command to force a Group Policy update. Subsequent commands in the batch file included disabling Windows Defender, and enabling Terminal Services on the impacted endpoint.

Both incidents shared some common TTPs, like the use of 7Zip for data collection and staging, and the use of MegaSync, likely for data exfiltration. Another commonality was the threat actor seemingly struggling to run the file encryption executable on some systems and likely troubleshooting by repeatedly using the executable's "- debug" command line switch.

Business Email Compromise

Business Email Compromise

The overwhelming majority of seen threats in our customers' Microsoft 365 environments were related to various types of inbox rules and manipulations. As shown in Figure 8, the most common tactics employed by attackers consisted of creating inbox rules (43% of incidents) such that messages were moved to an RSS folder. This type of attack is useful for preventing the user from discovering that their account has been compromised.

The next most prevalent attack consisted of using either a VPN or proxy (19% of incidents) in order to appear to get around location limitations. Since a lot of companies are able to lock down their environments such that logins are only valid from certain locations, attackers are able to utilize VPNs in order to log in from locations that have been allow-listed. Utilization of VPNs and proxies also helps hide the attacker's real location from investigators.

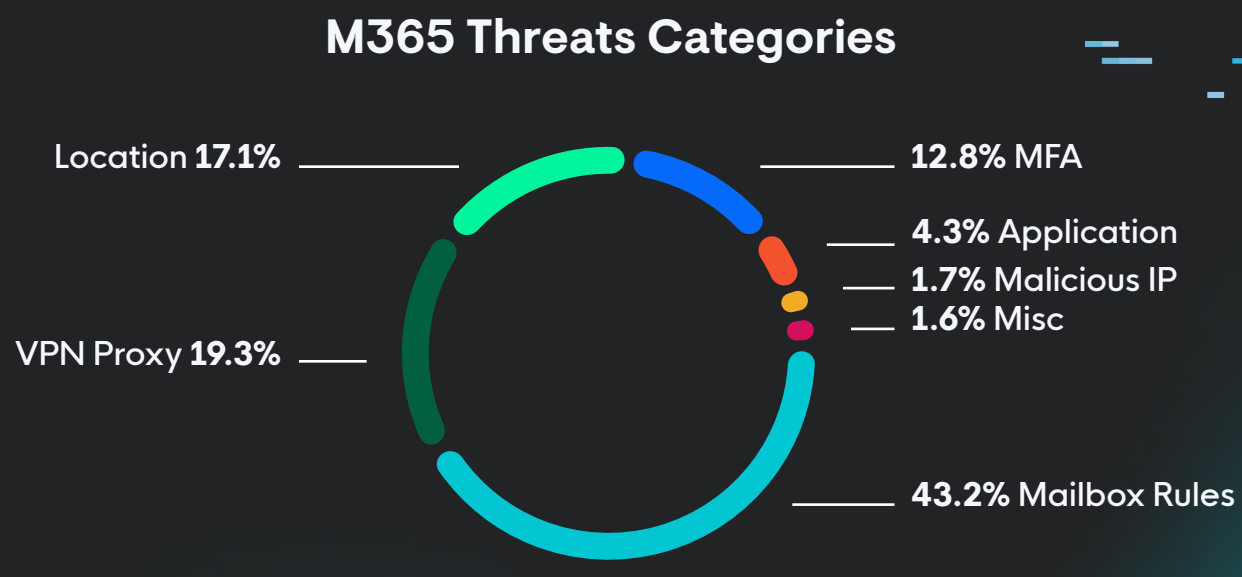


Figure 8: Breakdown of threats seen involving Microsoft 365 entities

Threats Across Various Industries

Threats Across Various Industries

Threat Landscape in Healthcare

Huntress also has customers that are within the healthcare industry. Such customers are ripe targets for threat actors to extract information, as well as extort directly through the threat of releasing patient information, or company information on the Internet; as well as creating real life-or-death situations by taking critical machinery offline.

Within the last year, we have seen major disruptions, including the recent incident against Change Healthcare at the end of 2023. If large conglomerates are unable to withstand such threats, what chance do the smaller, private healthcare businesses stand?

Breakdown of Threats Seen in Healthcare

Looking at various customers that are within the healthcare industry—customers including dental offices, doctor's offices, pharmacies, healthcare technology, and medical labs to name a few—we can see that some of the threats are similar to those and other small businesses that make up our customers. It's worth noting, though, that while some of these threats may not seem advanced, like potentially unwanted programs (PUPs), adware, or cryptominers, in some cases, these seemingly benign programs paved the way for bigger problems and opened the endpoints to initial access brokers later down the line. The more common tactics we see utilized against the healthcare industry, as seen in Figure 9, are mainly precursors to ransomware attacks, with RATs, RMM abuse, and Trojans ultimately leading to ransomware delivery.

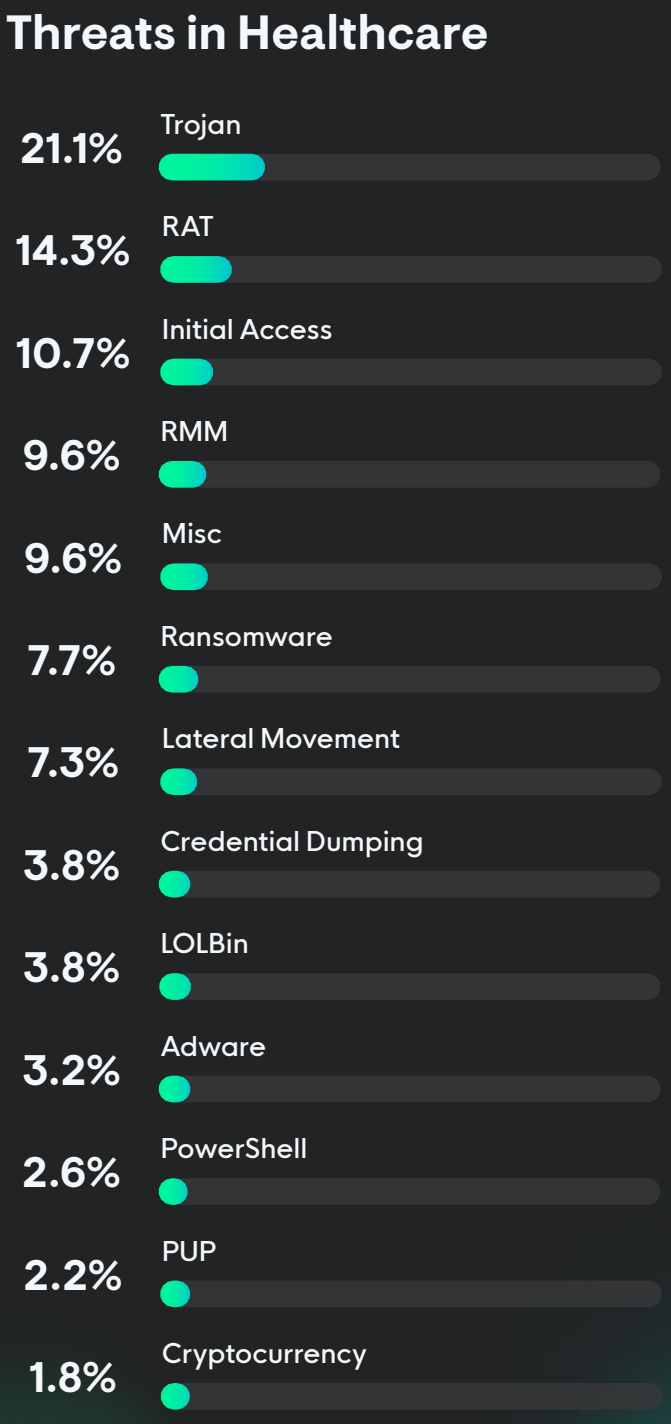


Figure 9: Most commonly seen threats in our healthcare customers

HUNTRESS

Ransomware Variants Seen in Healthcare

Another difference we see in the data from our customers in the healthcare industry is a difference in ransomware variants. Figure 10 shows the three main ransomware families seen amongst our healthcare customers: Dharma (29%), DarkGate (17%), and LockBit (15%). There were several other miscellaneous ransomware variants, but none that were worth highlighting. Again, the upticks in these particular attacks occurred towards the end of the year, in the wake of the Qakbot takedown.

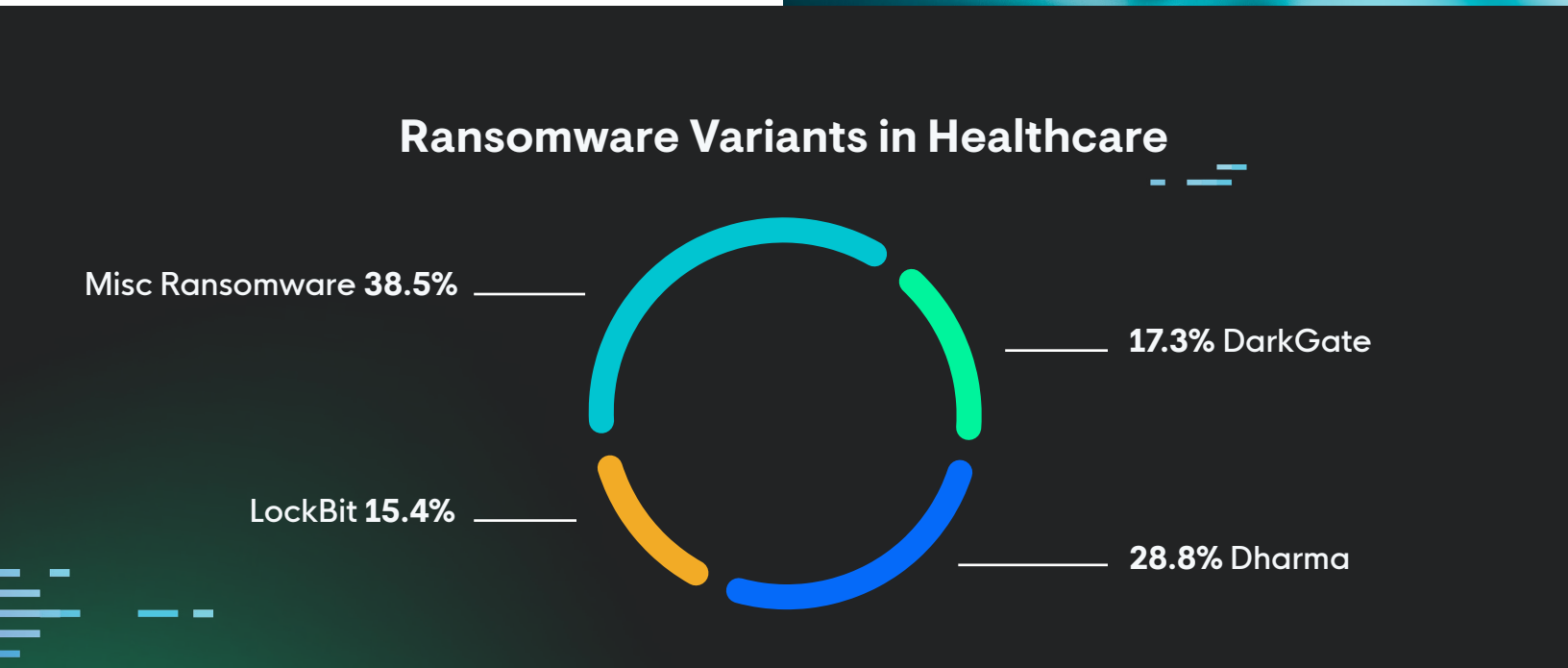


Figure 10: Most commonly seen ransomware variants in healthcare customers

Healthcare Business Email Compromise

Potential business email compromise (BEC) attacks occur in the healthcare industry, just like any other industry. Whenever there's something to gain, attackers will take advantage. The end goal may be to defraud an organization out of funds, or possibly even appear as a legitimate person in a healthcare organization and defraud patients. Regardless, Huntress saw plenty of incidents that involved healthcare customers.

The potential BEC threats in healthcare are actually not much unlike those seen in other industries. The main threats entail various Mailbox rules (RSS feeds, mail manipulation, etc), logging in using a VPN or Proxy in order to get around location settings, malicious applications, attacks against MFA, and logins from various unauthorized locations, or malicious known IP ranges.

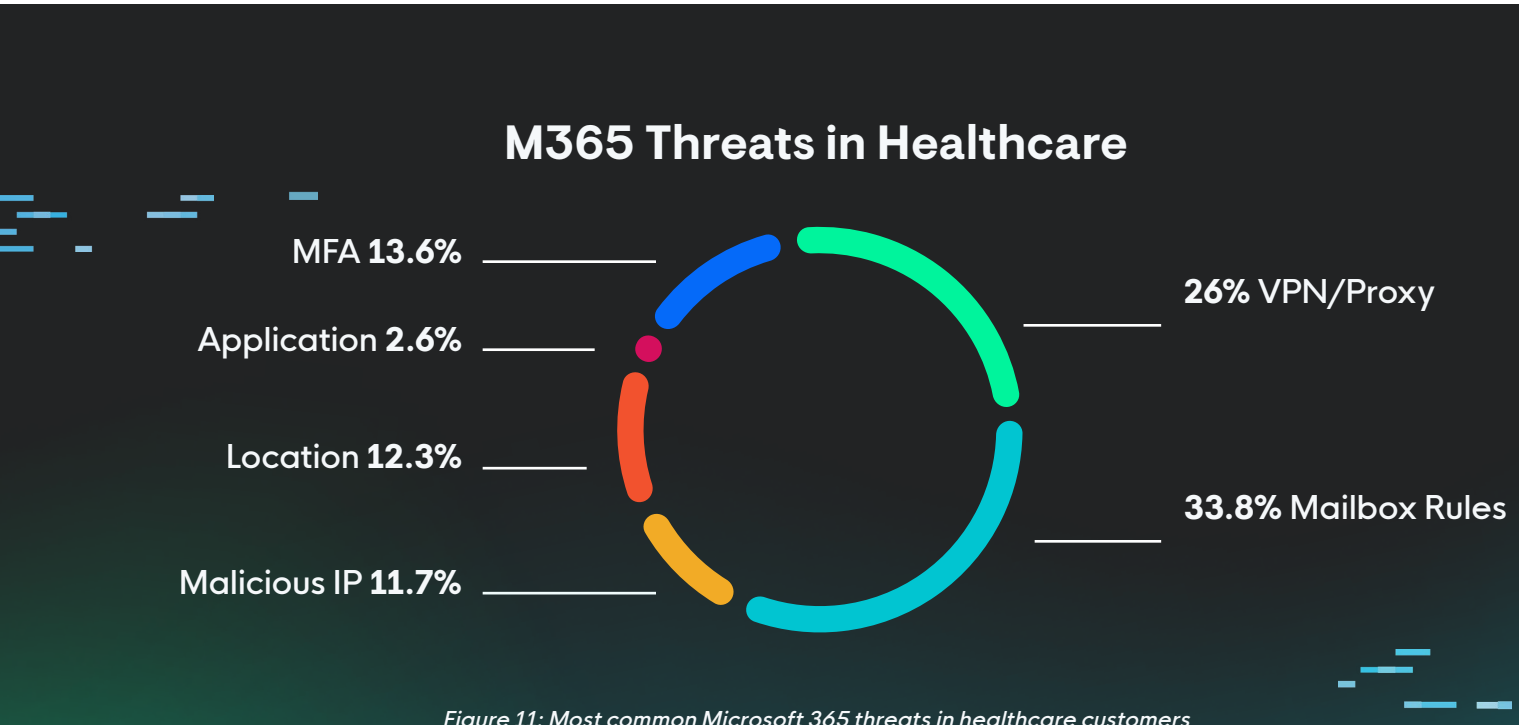


Figure 11: Most common Microsoft 365 threats in healthcare customers

Threats Across Various Industries

Threat Landscape in the Industrial Industry

Customers that fall under the industrial category are also ripe targets for attackers, especially from the aspect of industrial espionage. Such company makeups can include (but are not limited to) construction, aerospace, defense, tools, and machinery, and can include government contracting entities that specialize in any of these items. As such, these companies have a plethora of attacks that showed the attackers playing the long game, by setting up initial access methods.

Breakdown of Threats Seen in Industrial Companies

The industrial sector is far more plagued by cryptominers and access brokers. This is likely an easier payout for attacking the industrial sector, as they do not have the same incentives to pay quickly that is present in healthcare.

Since some of these companies may have higher-end equipment, it makes sense that they would make ripe targets for cryptominers, since they could make the calculations more effectively. However, as we have seen in the past, cryptominers may also lead to more malicious attacks later down the line and shouldn't be ignored.

Threats in Industrial Customers

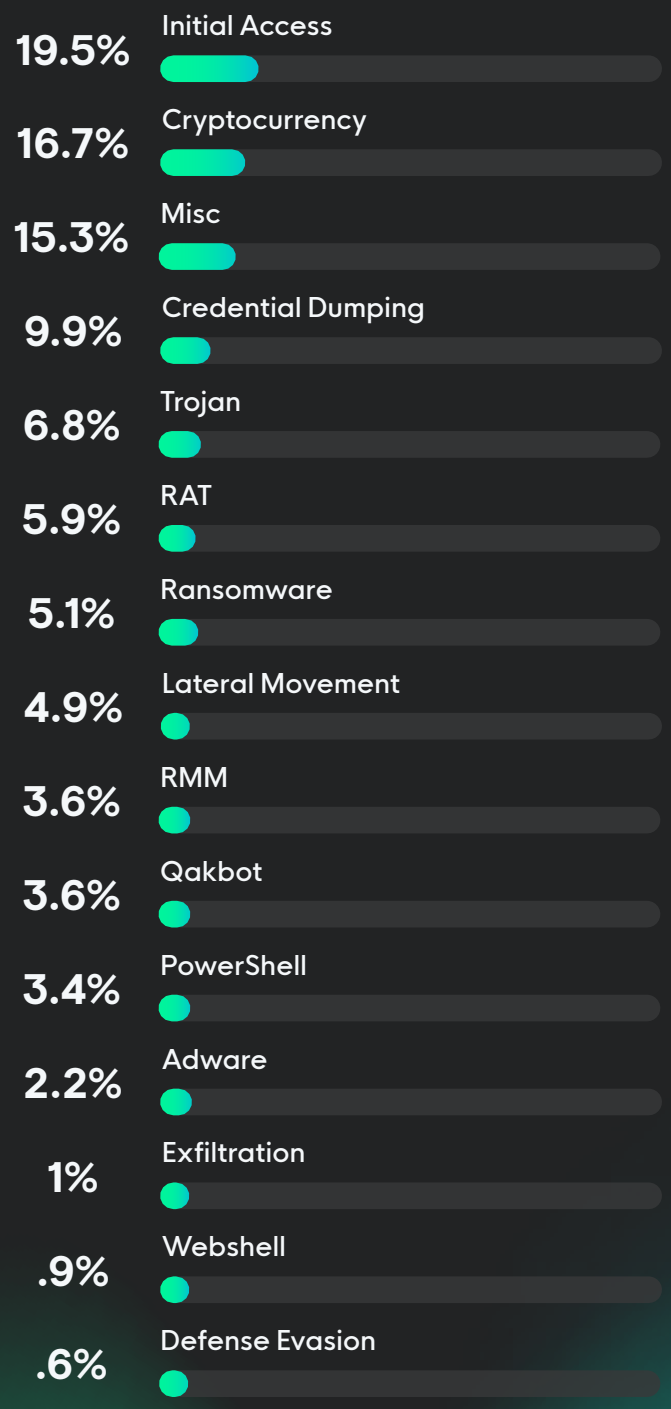


Figure 12 : Breakdown of threats seen in indusstrial customers

HUNTRESS

Ransomware Variants Seen in Industrial Companies

Unlike what was seen in our healthcare customers, the top ransomware variants were more diverse within our industrial customer base. They also seemed to be more targeted and precise. There were often clearer delineations that pointed to known threat actor groups, such as cl0p, instead of more of the miscellaneous small-time or unknown ransomware groups.

Also unlike the healthcare industry, where a payout is more likely due to the urgency, or potentially life-threatening implications of the encrypted medical equipment, or even implications of potentially losing patient data, threat groups are often more calculating when targeting those in industrial companies, which can include anything from steel companies to government contractors. Therefore, we have seen activity that is directly attributable to known threat actors, such as cl0p, when investigating incidents in this customer base. Oftentimes, these threat actors are willing to play the long game and may be more strategic in the information that they steal before pulling the trigger, if at all.

Figure 13: Breakdown of most common ransomware families seen across the industrial sector

Industrial Business Email Compromise

Much like the threats that we saw in the healthcare industry, and all our customers, the industrial customers are not immune to BEC attacks. In fact, it's quite the opposite.

Since most of these customers may deal with larger business contracts that include wire transfers, they are ripe for attackers to overtake their emails and change payment details. Warning signs of such activity include attackers setting up mailbox rules to hide responses to malicious emails sent to the victim, which helps avoid detection. As seen in Figure 14, the majority (60%) of the threats against industrial businesses include various mailbox rule manipulations.

Another interesting callout from the data is that there were fewer instances where the attacker came from a known malicious domain. In contrast, attackers targeting the healthcare industry were much more egregious in utilizing known bad infrastructure. The juxtaposition of these two industries' data shows how much more targeted industrial businesses are, and how much more vulnerable smaller healthcare businesses are, at least according to the attackers' perspective.

Figure 14: Breakdown of threats seen in Microsoft 365 incidents in industrial customers

Other Potential Emerging Concerns

Other Potential Emerging Concerns

While many elements of threat actor behaviors have remained consistent from Huntress' last in-depth reporting, a number of emerging concerns (some of which overlap with items previously reported) remain. Particularly, the mechanisms used for initial access to victim environments continue to proliferate among a variety of options, many of which elude existing defenses and monitoring.

For example, threat actors continue to leverage vulnerabilities in high-availability, external-facing applications such as security appliances and VPN concentrators to establish initial points of presence in victim networks. A specific, and concerning, example of this is the persistent use of CVE-2023-4966, referred to as "CitrixBleed," by various entities. Most notably, LockBit affiliates have extensively used this vulnerability in late 2023 to compromise a variety of SMB, government, and related victims to facilitate follow-on ransomware deployment.

Another, increasingly popular access route for either network access or information gathering is credential gathering and user spoofing in cloud-based applications and services. In these events, threat actors will acquire user credentials through various mechanisms—through "infostealer" malware, underground forums, or leak sites—and then access external resources masquerading as that user. In the case of third-party cloud applications, logs may be difficult to review or non-existent to the victim entity. Even when available, tracking items such as logon location or source network is prone to "noise" if employees travel, leverage various commercial VPNs (a significant security hygiene issue in its own right), or similar activity. Once achieved, access can be either used directly for information gathering or follow-on identity spoofing, or used as an intrusion "beach head" if the adversary can elevate privileges.

Inside the Threat

Midnight Blizzard & the SMB Space

In October 2023, JetBrains disclosed CVE-2023-42793 in on-premises TeamCity software. At the time of disclosure, Huntress identified some targeted exploitation of this vulnerability, but no widespread activity impacting Huntress customers. Two months later, in mid-December 2023, multiple government agencies identified state-directed exploitation of this vulnerability linked to Russian intelligence services. Notably, this reporting identified exploitation starting as early as September 2023, prior to public disclosure of the vulnerability and patch release.

Linked to a threat actor referred to as Midnight Blizzard by Microsoft (and also labeled APT29 or Cozy Bear by other entities), the campaign appears to focus on widespread, indiscriminate exploitation of vulnerable TeamCity instances. Notably, this opportunistic exploitation activity includes the exploitation of entities such as IT services providers like MSPs, medium-sized manufacturing entities, and various technology firms.

At this time, Huntress has not identified evidence of this activity successfully compromising Huntress-monitored entities. However, the scope, scale, and nature of this event emphasize that, like earlier state-directed exploitation activity, SMBs and the MSPs and other entities providing services to them cannot simply dismiss their environments as "irrelevant" or "unimportant" for such threat actors. Whether for direct action (such as intellectual property theft) or the development of proxy networks of compromised machines for follow-on activities, state-sponsored and -directed threats will remain a significant concern even for the SMB space for the foreseeable future.

Conclusions

Conclusions

We are just starting to scratch the surface of the unique threat landscape within the businesses that fall below the large enterprise level and those who seek to protect them. This demographic is both vulnerable and valuable, attracting the wandering eye of threat actors of varying skills and motives. This is apparent in the trend that ransomware continues to thrive, even after takedowns of various infrastructure has occurred. It's just too lucrative and profitable for cybercriminals to resist.

Regardless of industry, there are some common issues that are worth highlighting. Remote monitoring and management (RMM) and living-off-the-land binaries (LOLBins) remain a challenge for businesses and MSPs alike. These types of threats are designed to blend in with normal activities and fly under the radar, taking advantage of gaps in our visibility or security tools. Therefore, it's becoming more important for businesses to adopt more advanced security measures, such as monitoring tools that can detect unusual activities and behaviors that might otherwise go unnoticed.

We've also seen attackers exploit widely known vulnerabilities early on, such as MOVEIt, 3CX, and ScreenConnect, which suggests that businesses on the smaller or medium size are being used as an attacker's testbed as they try out TTPs before taking them to the enterprise arena. With these trends in mind, it may be time to consider some alternative, more proactive strategies to keep the predators at bay.

About Huntress

Huntress is the leading cybersecurity partner for small and mid-sized enterprises 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 today's businesses defend against cyberattacks.

Schedule a Demo

HUNTRESS