

Attack Superhighway

A Deep Dive on Malicious DNS Traffic



Table of Contents

- 2** Domain Name Servers — a highway for attack traffic
- 4** Akamai DNS traffic analysis terminology
- 6** Danger ahead: the pervasiveness of malicious traffic in organizations
- 25** Home users under attack
- 33** Phishing landscape overview
- 35** Conclusion and recommendations: combat modern attacks with proactive measures
- 36** Methodologies
- 37** Credits

Domain Name Servers — a highway for attack traffic

The Domain Name System (DNS) has been a critical part of internet infrastructure since its earliest days. Much of our internet usage, be it at home or at work, must be facilitated via the DNS in order for us to correctly navigate to our destination on the World Wide Web. Unsurprisingly, attackers often choose to leverage this infrastructure to facilitate their attacks — whether it's a threat that accesses command and control (C2) servers to await commands, or a remote code execution that reaches out to a domain in order to download malicious files onto a machine. Because of its ubiquity, DNS has become an important part of the attack infrastructure.

As a security company, Akamai has a vantage point that allows us to examine and protect [businesses](#), as well as [home users](#), against malicious DNS traffic that could lead to system compromise and stolen information. In this report, we will provide an analysis of the malicious traffic targeting home users and enterprises worldwide. A thorough analysis of malicious DNS traffic, which includes correlation to attacker groups or tools, could arm organizations with important information regarding the most prevalent threats to their organization. As such, this information could aid security practitioners in evaluating their defense posture and conduct gap assessments to meet the techniques and methodologies leveraged against them. Failure to do so could result in breaches leading to confidential data losses, financial losses, or penalties due to compliance violations. With [cybercrime costs](#) expected to surge up to US\$10.5 trillion annually by 2025, organizations must be prepared even before attacks occur.

As we analyzed malicious DNS traffic of both enterprise and home users, we were able to spot several outbreaks and campaigns in the process, such as the spread of FluBot, an Android-based malware moving from country to country around the world, as well as the prevalence of various cybercriminal groups aimed at enterprises. Perhaps the best example is the significant presence of C2 traffic related to initial access brokers (IABs) that breach corporate networks and monetize access by peddling it to others, such as ransomware as a service (RaaS) groups. Those activities are visible to us on the information highway that is DNS, and we are sharing them for the benefit of our readers.



TL;DR



According to our data, between 10% and 16% of organizations have encountered C2 traffic in their network in any given quarter. The presence of C2 traffic indicates the possibility of an attack in progress, or a breach, and threats range from information stealing botnets to IABs.



26% of affected devices have reached out to known IAB C2 domains, including Emotet and Qakbot-related domains. IABs present a large risk to organizations as their primary role is to perform the initial breach and sell access to ransomware groups and other cybercriminal groups.



Network-attached storage (NAS) devices are ripe for exploitation as they are less likely to be patched and they hold troves of valuable data. Our data shows attackers are abusing these devices through QSnatch, with 36% of affected devices in corporate networks accessing C2 domains related to this threat.



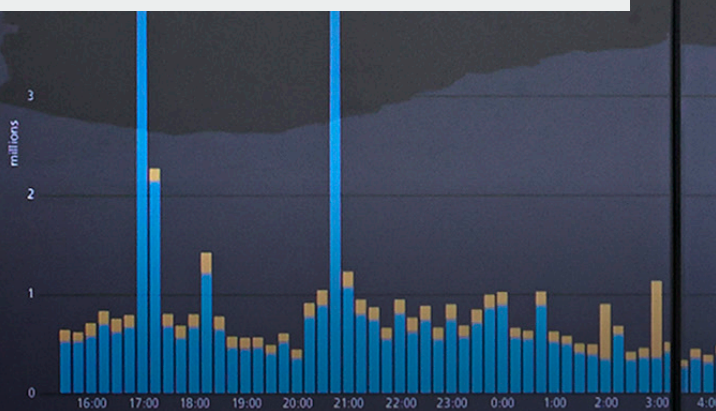
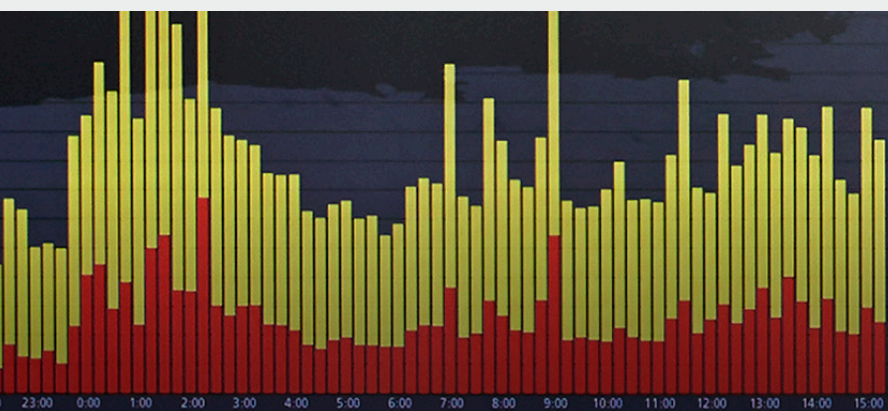
30% of affected organizations are in the manufacturing sector; twice as many as the second largest vertical, underscoring the real-world implications of cyberattacks such as supply chain issues and disruptions to everyday living. Regulations such as [Network and Information Security 2 \(NIS2\)](#) could help curb attacks against essential industries or critical infrastructure like manufacturing.



Attacks on home networks are seeking to abuse not only traditional devices like computers, but also mobile phones and the Internet of Things (IoT). A significant amount of attack traffic can be correlated with mobile malware and IoT botnets.



Through our DNS data analysis, we spotted a burgeoning outbreak of FluBot malware in Europe, Middle East, and Africa (EMEA); Latin America (LATAM); and Asia-Pacific and Japan (APJ). The malware's social engineering tactics and its use of multiple European Union (EU) languages could be some of the contributing factors for the rise of infection.



Akamai DNS traffic analysis terminology

Akamai [Edge DNS](#) and [DNS infrastructure](#) observe up to 7 trillion DNS requests daily. In order to protect Akamai's users and enterprises, Akamai blocks requests leading to domains serving malware or sites that could steal your information. Examining these malicious DNS transactions also allows us to classify these domains into three categories – malware, phishing sites, and C2 – and conduct a deep dive to ascertain today's biggest threats to enterprises and home users.

From a careful data sampling of malicious DNS traffic, we can draw significant conclusions about the most prevalent threats. Our protection covers two demographics: One demographic is that of enterprises wherein Akamai secures corporate networks, and the other demographic is that of home users accessing the internet on their personal networks and are being exposed to threats like botnets that aim to take over their devices for nefarious purposes such as financial gain through cryptomining.



First, let's define the terms *phishing sites*, *malware*, and *C2* and explain how we use them in this report.



Phishing sites are domains tied to phishing kits that mimic and clone the look and feel of retail businesses, banks, high-tech companies, and others in order to dupe users into divulging information like credentials and personally identifiable information (PII). Akamai observes this traffic via DNS to protect both enterprise and home users against identity theft and information loss.



Malware is a malicious domain (or domains) that serves or contains malicious files. This category also contains sites hosting malicious JavaScript and compromised websites serving unwanted ads or redirecting users to a page containing these ads. Many modern attacks require downloading a malicious file to a device from an external source for its initial payload or to download the next stage of an ongoing attack. Observing and blocking this traffic can help protect an organization from an initial infection or ongoing attack.



C2, in the context of our DNS traffic analysis, is a domain used to communicate with the infected devices to send commands and then control the device. After initial compromise, attackers establish C2 communications between the infected system and a server controlled by the attackers to send additional commands – such as the download and spread of other malware, data exfiltration, and shutdown and system reboot, among others – to further compromise the security of the system or network. Detecting C2 traffic is crucial as it signals an ongoing attack that could still be mitigated. Moreover, blocking the domains associated with C2 servers prevents C2 communications from being established, and it prevents the malware from downloading further instructions or commands, reducing the chances of attackers performing malicious activities in your network.



Danger ahead: the pervasiveness of malicious traffic in organizations

Based on Akamai's analysis of DNS traffic, we can see that 13% of devices attempted to reach out at least once to domains associated with malware in Q4 2022 (Figure 1). In addition, 6% communicated with domains pertaining to phishing. In the C2 area, which we will focus on heavily in this report, we observed an increasing trend throughout the year with a very slight decrease in Q4.

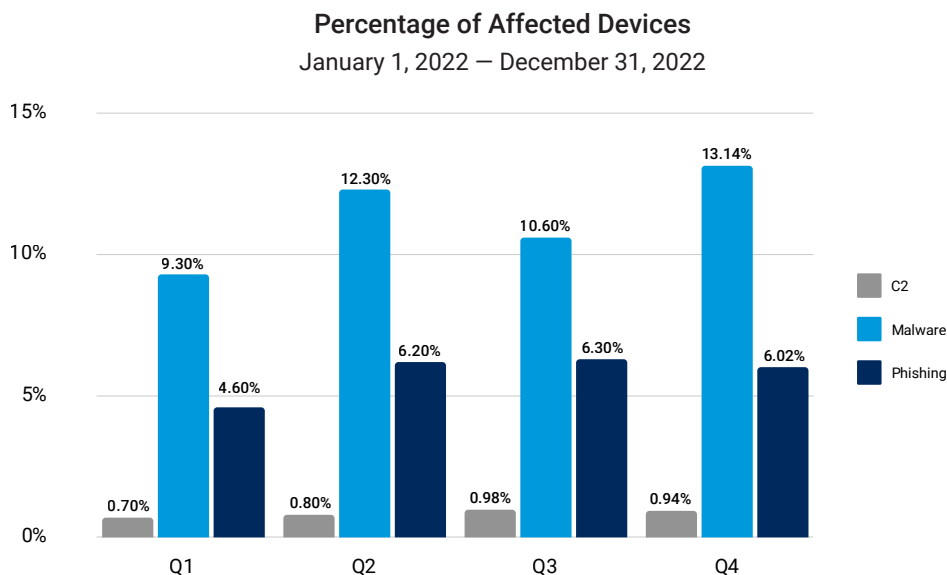


Fig. 1: We see a growing trend in protected devices reaching out to malicious destinations

Note that Figure 1 only refers to individual devices that attempted to communicate with malicious domains. It's important to point out the disparity between devices that reach out to malware destinations (which may be used by attackers to download malware) and devices that reach out to C2 domains (which are typically used during an ongoing attack to facilitate communication between attacker and malware, and can be used for downloading additional malware to further an attack cycle). This disparity may be indicative of the differences between network infiltration attempts, which may be blocked at the first attempt to download malware onto a machine, and successful infiltration (which, in our data, may have not traveled through the DNS) or ongoing attacks, which may reach out to a C2 domain to carry out the attack.

This report will primarily focus on C2 traffic as a potential indicator of an instance when an attacker has successfully landed on a device. In order for us to understand the prevalence of such attacks, we need to look at the data through a different lens. Rather than look at individual devices, we can aggregate the data by organization to examine how commonly an ongoing attack (indicated by the existence of C2 traffic) appears within the data set.

Percentage of C2-Affected Companies
January 1, 2022 – December 31, 2022

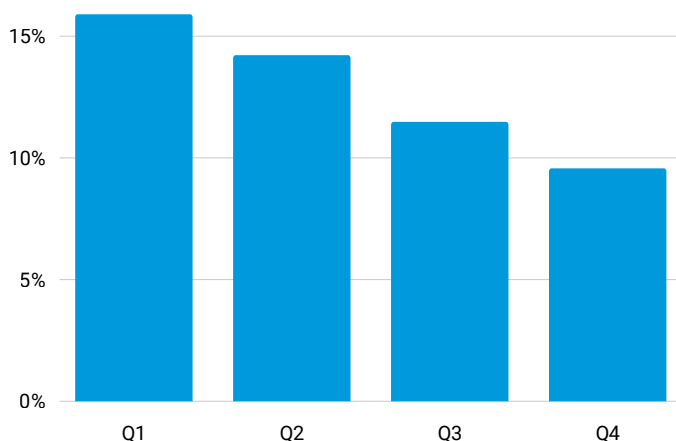


Fig. 2: An analysis of malicious C2 traffic shows the percentage of organizations that have had at least one device reach out to a C2 domain throughout the year

According to our DNS data, between 10% and 16% of organizations have experienced at least one instance when C2 traffic was observed traveling out of their network, in any given quarter.

According to our DNS data, between 10% and 16% of organizations have experienced at least one instance when C2 traffic was observed traveling out of their network, in any given quarter (Figure 2). This may be indicative of malware attempting to communicate with an operator and is a potential sign of a breach. This C2 traffic was blocked by our solution from reaching its destination, but successful attacks might have resulted in data exfiltration, ransomware attacks, and more. As of the first half of 2022, 2.3 billion malware strains were detected, with an average of **1,501 each day**. Our research highlights the effectiveness of leveraging DNS to prevent malware from progressing in a network or causing harm.

Initial access brokers pose a prevalent threat to organizations

Multistage attacks have become a staple of the modern attack landscape (Figure 3). Attackers are finding increased success when they are able to work together (or hire one another), or when they are able to combine various tools in a single attack. C2 is pivotal in the success of these attacks. They can be used not only for communication, but also to facilitate downloading a payload and the next-stage malware to move the attack onward. This is best exemplified by the Emotet/TrickBot/Ryuk ransomware [attack chain](#) observed in the last few years. Emotet first infiltrates the victim’s network, and once initial access is established, it reaches out to a domain to download the TrickBot payload to obtain personal data, credentials, and more. If the victim is considered a high-value target for the attackers, the malware then reaches out to its C2 servers and downloads the final payload: Ryuk ransomware.

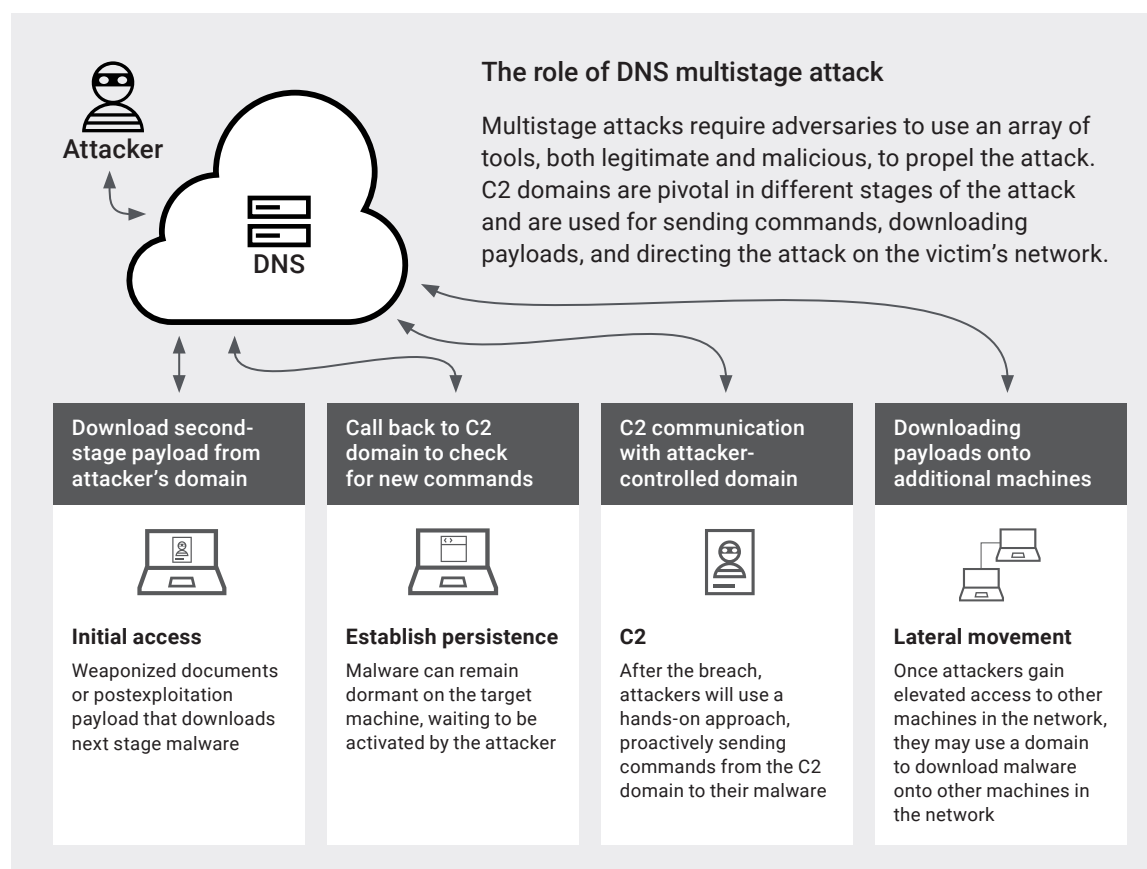


Fig. 3: The role of C2 in each stage of the attack

This chain of events is important to consider when assessing the information in this report. C2 communication can occur at various stages of the attack. Our recent analysis of the methodology of modern ransomware groups, such as the [Conti group](#), showed that sophisticated attackers often assign operators to work “hands on keyboard” in order to quickly and efficiently progress an attack. The ability to view and block C2 traffic can be pivotal to stopping an ongoing attack.

The C2 domains we’ve observed could be categorized into domains with and without attribution to a specific threat family or attacker group. In this section, we will delve into C2 domains with association to a threat type, and help readers assess the level of risk according to the capabilities and methodologies of each group. Please note that some of these malware families may fit multiple use cases, depending on how attackers use them during an attack.

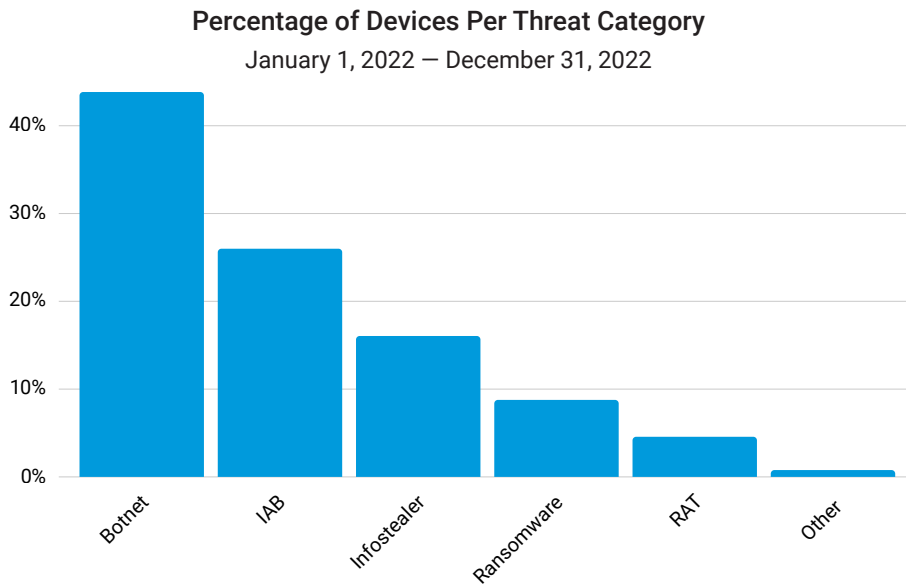


Fig.4: Enterprises are predominantly targeted by botnets, followed by IABs and info stealers

In Figure 4, attacker groups are classified into IABs, botnets, and RaaS groups. Our data findings reveal that IABs pose one of the biggest threats to corporate networks, as do botnets aimed at data exfiltration.



Initial access brokers

IABs focus mainly on providing an initial entry point for other cybercriminals, including ransomware groups, to gain a foothold in organizations’ networks.



Ransomware as a service groups

These are groups that allow other attackers (even those without technical expertise) to become an affiliate and use their ransomware software for a fee.



Botnets

Attackers can use botnets for myriad purposes – from cryptomining and DDoS attacks to data exfiltration, malware deployment, and lateral movement.



Information stealers

Info stealers gather various types of data like usernames, passwords, system information, banking credentials, cookies, and so forth.

We also observe ransomware, remote access tools (RATs), and infostealers in the mix – all have a critical role to play in various attack stages. And with tools readily available in the underground to both novice attackers and experienced cybercriminals that allow them to gain initial entry, remain hidden in the network, and further the attack, organizations are more than ever susceptible to cybercrime. As we course through these groupings, we will also establish the intersections at which they operate and the potential implications and impacts on organizations.

Initial access broker groups

Dubbed “initial access brokers” (IABs), this specific breed of cybercriminals focuses mainly on providing an initial entry point for other cybercriminals and attackers to gain a foothold to organizations’ networks. While multiple cybercriminal groups have similar breach methodologies – such as exploiting RDP and VPN-related vulnerabilities, using brute-force attacks, gathering credential dumps, and launching malware-laced phishing emails – IABs specialize in gaining access to these infected systems and selling that access to other attacker groups, rather than carrying out the entire attack. Ransomware groups behind LockBit, DarkSide, Conti, and BlackByte, among others [reportedly leveraged IABs](#) as part of their operations. A 2023 research study noted that the [average selling price](#) for initial access is approximately US\$2,800.

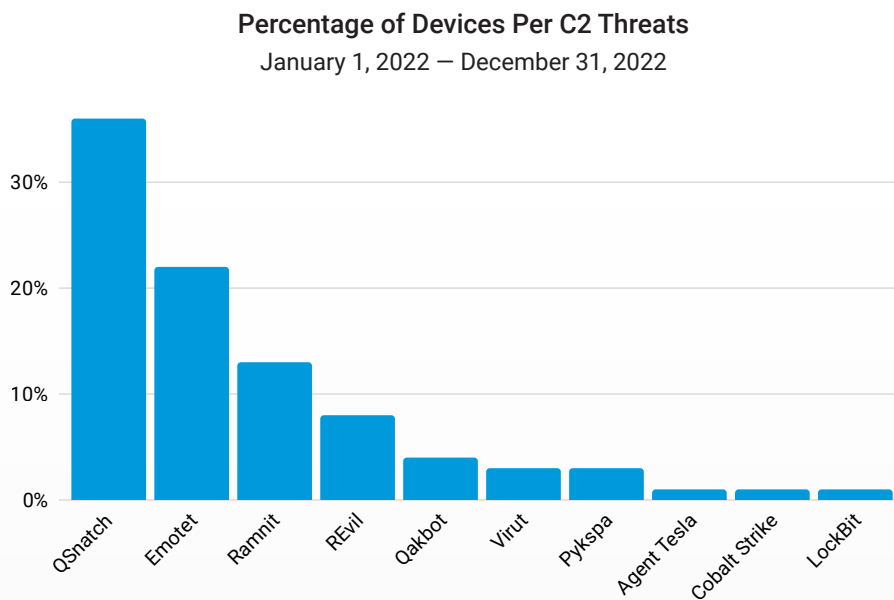



Fig. 5: QSnatch, Emotet, and Ramnit are the top C2 families seen in corporate network traffic

Based on our DNS data (Figure 5), 26% of infected devices reached out to domains related to IABs such as [Qakbot](#) (4% of infected devices) and [Emotet](#) (22% of infected devices). IABs play an important part in the RaaS business model and cybercrime landscape. Ransomware attackers and cybercriminals need remote access and credentials not only to infiltrate their victims' networks but also to move laterally, establish persistence, and gain access privileges, among other activities. Attackers leverage IABs to do the time-consuming tasks of reconnaissance, potential target scanning, and initial infection. Readily available access peddled in the underground eliminates that step and lowers the bar of expertise or time needed by attackers to launch an attack. As such, it introduces a plethora of potential attacks against intended target organizations, resulting in ransomware, stolen confidential and sensitive information, espionage, and data breaches.

Emotet emerges as one of the most prominent IABs in our data. Emotet represents a significant risk to organizations because of the group's connection with ransomware attackers, including the Conti group that impacted various industries across the globe before they [disbanded](#) last year. Over the years, Emotet added more modules, such as Distributed Denial of Service (DDoS) and email theft capabilities, and expanded its intended targets. From a banking Trojan/botnet with a plethora of functionalities, Emotet shifted into a malware as a service (MaaS), distributing threats like IcedID banking trojan, TrickBot, and UmbreCrypt ransomware. The TrickBot group was also observed to use Emotet to distribute several ransomware strains, including Ryuk, ProLock, and Conti, among others. A more detailed view of the techniques used by Emotet can be found in the [MITRE ATT&CK](#) framework on the topic.



Emotet represents a significant risk to organizations, due to the group's connection with ransomware attackers, including the Conti group that impacted various industries across the globe before the gang disbanded last year.



The second most prominent IAB in the data is Qakbot. This group is known to have collaborated with the Black Basta ransomware group that has [reportedly impacted](#) at least 50 organizations from various parts of the world. The Qakbot team is known for its information-stealing capabilities and for delivering second-stage malware to further compromise the system security. According to research, [Qakbot leverages Cobalt Strike](#), a legitimate pentesting tool used by red teams and abused by adversaries, to do an array of malicious activities postintrusion and to facilitate a backdoor into a victim's environment. This is a technique that is increasingly [used by IABs](#) in recent years. The MITRE ATT&CK framework can provide additional intelligence related to the [techniques leveraged by Qakbot](#) during its attack.

Botnet groups

In our analysis, botnets make up the largest grouping of threat types at 44% of the C2 traffic analyzed. A wide array of attackers are represented in this grouping, and it's essential to remember that not all botnets are created equal. The more benign variants might plant cryptominers or leverage the victim's machine to conduct DDoS attacks. Although these represent a cost on their own, the botnets we've found in enterprises can be used for data exfiltration and multistage attacks, which may represent a more significant risk. Botnets can spread laterally into the network and can be used to deploy ransomware, as in the case of TrickBot. or they may specifically focus on information stealing and credential harvesting.

We found that [QSnatch](#), the largest botnet present in enterprise environments, does exactly that – data exfiltration from network-attached devices. According to our data, QSnatch accounted for 36% of infected devices. This malware specifically targets QNAP, a type of NAS device used for backups or file storage by businesses. Although the infection method is still unknown, researchers surmise that QSnatch could infect via exploitation of firmware vulnerabilities or brute force attacks on devices with a default username/password. It is highly recommended that companies using QNAP keep their firmware up-to-date (once infected, QSnatch would [prevent installing patches](#) and disable security products) and to change default passwords immediately. QSnatch is used by attackers to do credential scraping, password logging, remote access, and data exfiltration, to name a few. Attackers may be targeting storage devices as they contain troves of valuable information, and compromising these devices leaves businesses with no backups in case of ransomware attacks. Details on tactics and countermeasures are highlighted in this [CISA alert](#).



Ransomware as a service group

In our analysis of the DNS traffic, 9% of infected devices that reached out to C2 families accessed domains associated with RaaS groups. This type of cybercriminal group allows other attackers (even without the technical expertise) to become one of their affiliates and use their ransomware software for a fee. Organizations hit by ransomware face myriad consequences that are not limited to loss of confidential company data. Enterprises could potentially deal with remediation and recovery costs, legal fees, fines, downtime resulting in loss of productivity, and brand and reputation damages. Cybersecurity Ventures opined that [the cost of ransomware attacks](#) would be approximately US\$265 billion annually by 2031. Akamai's [global ransomware report](#) also highlights the crippling impacts of ransomware that go beyond financial losses, such as supply chain disruption, and, in some cases, ransomware could be [a matter of life and death](#).

One prolific RaaS group is the REvil gang who became notorious for targeting an [IT management vendor](#) in a supply chain attack that impacted more than 1,500 managed service providers. Their operations ceased with [the arrest of several members](#) by the Russian government. However, a few months after the disbandment, security researchers observed that REvil's leak site was again active with information of its latest victims, including some universities in the United States. Researchers have speculated that it may [not be the same REvil gang](#) running this campaign and warned against nation states that claim to be the REvil group in order to hide their tracks. In terms of tactics, [REvil is known for customizing](#) their attack flow depending on its intended victims, which exemplified the level of knowledge the group has of their targets. To learn more about the tactics, techniques, and procedures related to REvil, read [MITRE's post](#).

Attackers may be targeting storage devices as they contain troves of valuable information and compromising these devices leaves businesses with no backups in case of ransomware attacks.

Another RaaS group we spotted in our examination of DNS traffic is LockBit. Following Conti's "disappearance," the LockBit group became one of the most active RaaS providers. Prior to that (from November 2019 to March 2022), it was the RaaS with the most number of victimized organizations after Conti, according to this [report](#).

The LockBit gang prides itself with having a [faster encryption mechanism](#) than other RaaS groups, and [claimed to have impacted](#) more than 12,000 companies with its LockBit 2.0. In June 2022, the group released LockBit 3.0, with additional functionalities, including a bug bounty program. It is also [reportedly leveraging the Log4j vulnerability](#) to get initial access to their targets, underscoring the importance of patching. Organizations who have not addressed such security flaws may be at increased risk of being infected with LockBit. LockBit continues to reinvent itself – one recent addition is the [triple extortion tactic](#) in which they encrypt files, post them in leak sites, and launch DDoS attacks if victims refuse to pay the ransom.

Tools of the trade

The tools identified in this section may play a specific part in an attack, whether it's through breaching the system, obtaining information, or escalating privileges. The arsenal we saw from various attacker groups often requires communication to operate like information stealers and RATs. Understanding these tools, along with the tactics used by attacker groups, can help security practitioners understand how attacks happen and plan accordingly.

Infostealers

Designed to obtain various types of data like usernames, passwords, system information, banking credentials, and cookies, among others, infostealers remain one of the MaaS offerings frequently used in attacks. Attackers who may not have the technical knowledge and/or skills could simply acquire infostealers at a relatively low cost and launch their own attacks.

In the list of C2 malware families, we observed 16% of devices that have accessed known C2 attribution reaching out to infostealers. [Ramnit](#) (13% of infected devices) is not just another run-of-the-mill information stealer. Its strength lies in how highly modular it is, enabling attackers to leverage its various functionalities, such as stealing other sensitive data and downloading/deploying other malware to meet their end goal or further the attack. In 2021, Ramnit was considered the top [banking trojan](#), with recent news citing how another malware [shared similar code](#) with Ramnit.





The presence of infostealers in your network is a telltale sign that your user's credentials may be at risk. Collected stolen information could be peddled in the underground markets and used to gain initial access by other attackers. Ransomware groups could deploy an infostealer via phishing or botnets to obtain valid credentials, [rent an access license to an infostealer](#) in an underground forum offering MaaS, or purchase network access via IABs. In some cases, infostealer operators could become IABs and sell harvested high-value credentials (like VPN or RDP access) to the highest bidders or other threat actors who could launch a far more sophisticated attack.

Remote access tools

Cobalt Strike has been abused by several attacker groups as part of their operations. There are various means in which this powerful RAT is being utilized by attackers, including reconnaissance, privilege escalation, lateral movement through the network, establishing persistence, remote payload execution after intrusion (like ransomware), and data exfiltration. Although the tool is mostly used postbreach for lateral movement and exfiltration, it is also capable of being the initial access vector, as it has a [spear-phishing module](#). Groups that have been known to use this tool are [Conti](#), Qakbot, TrickBot, and Emotet, to name a few. To aid detection of Cobalt Strike in an environment, this set of [YARA rules](#) were created to determine malicious use of the tool.

Our data also shows the presence of [Agent Tesla](#) C2 traffic. This RAT is being [sold in the underground market](#) and its affordable price and ease of use make this tool appealing to cybercriminals. Attackers could use this tool to harvest credentials from various browsers, capture keystrokes and screenshots, and perform keylogging. One of its notable tactics is form grabbing, enabling attackers to gather PII and other sensitive information. Such stolen information could be used for identity theft or fraud. PCrisk has published [more details](#) on Agent Tesla's techniques and how it impacts affected users.

Activity landscape shows sporadic malware campaigns throughout the year

Over the course of one year, we saw fluctuations in the activities of C2 malware (Figure 6). Case in point: Emotet is seen to be particularly active during January and February of 2022, following [its resurgence in November 2021](#). This boost in activity demonstrates a formidable campaign to help it regain its status after months of inactivity. In the months following its comeback, Emotet enhanced its tactics by including ways to circumvent Microsoft’s move to disable Visual Basic for Applications macros. Some [reports](#) indicate that Emotet had become inactive again between July and November of 2022; our data observations demonstrate a decline in C2 traffic in July as seen in the lesser percentage of infected devices reaching out to Emotet domains. This may indicate that the group remained active throughout the year, or this could be a case of installed malware that is still communicating to an outdated infrastructure. Observations in 2023 could help us determine whether the Emotet group has indeed gone dormant.

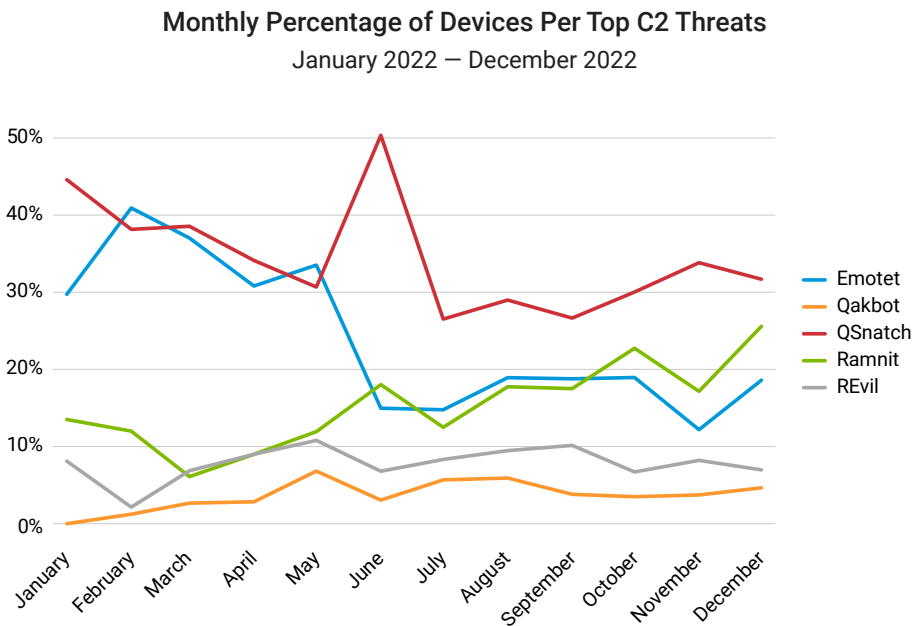


Fig. 6: The monthly trend graph shows that QSnatch was consistently active throughout 2022

Emotet is seen to be particularly active around January and February of 2022, following its resurgence in November 2021. This boost in activity demonstrates a formidable campaign to help it regain its status after months of inactivity.

QSnatch is consistently active throughout the year, peaking around June, showing how prevalent this threat has become. NAS servers are viable targets for attackers for several reasons: First, they contain sensitive data; second, there's less likelihood of NAS servers being patched; and, third, these devices are potentially more accessible in the organizational network and could serve as a hub for lateral movement. Although there are changes in the last few years, like the addition of built-in security solutions, cybercriminals circumvented these by disabling installed security products and/or preventing devices from being updated with new fixes. As such, these devices remain vulnerable against new strains of this malware.

We also see Ramnit's rising numbers in corporate networks from August through December. This is worrisome as this malware could steal a wide array of sensitive information that attackers could later sell to other threat actors for future attacks.

QSnatch and Emotet: common threats among all regions

To determine the prevalent threats per region, we examined the individual region's percentage of devices reaching out to C2 domains (Figure 7). Each percentage is relative to the number of devices affected per region, which also differs depending on the region. Interestingly, we are seeing similar attack trends in all regions, albeit with very few outliers. We therefore recommend that each region follows the recommendations provided in the "Conclusion and recommendations" section or under each malware group in the sections above.

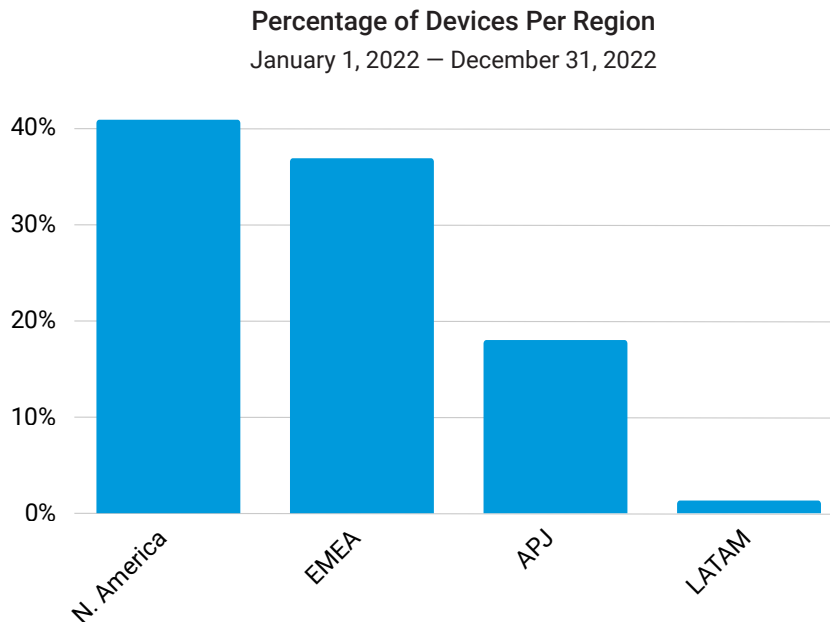


Fig. 7: North America takes the lead at 41%, followed by EMEA (37%) and APJ (18%), when it comes to the number of affected devices per region

North America

The majority of organizations globally suffered from these two biggest threats: QSnatch and Emotet. In North America, approximately 29% of affected devices within the region are impacted by Emotet, while 33% are impacted by QSnatch (Figure 8). According to a Dark Reading [report](#), a Shodan search showed that there are 300,000 QNAP devices connected to the internet, which makes it an attractive target. In addition, NAS devices like QNAP could be used as backup and serve as media or file servers.

Other notable threats in North America include Ramnit, Qakbot, and REvil. This is interesting given how IABs like Emotet paved the way for other infections, including (but not limited to) ransomware.

Percentage of Devices Per Top C2 Threat in North America

January 1, 2022 – December 31, 2022

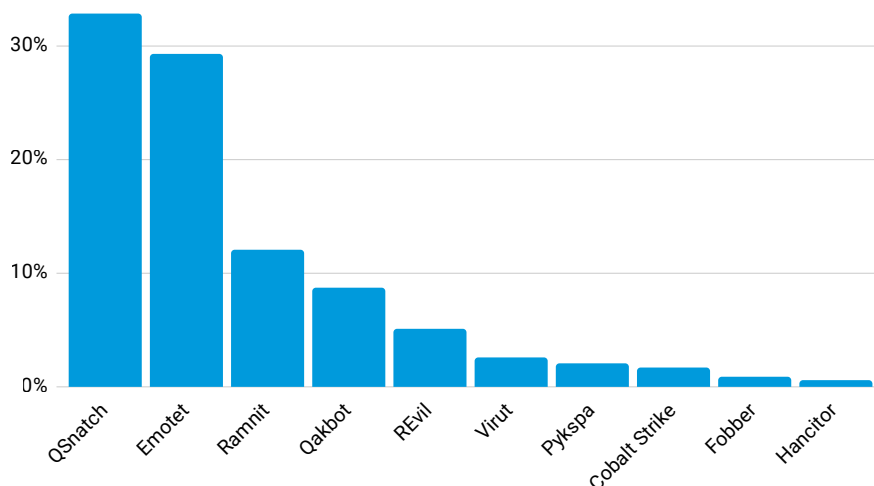
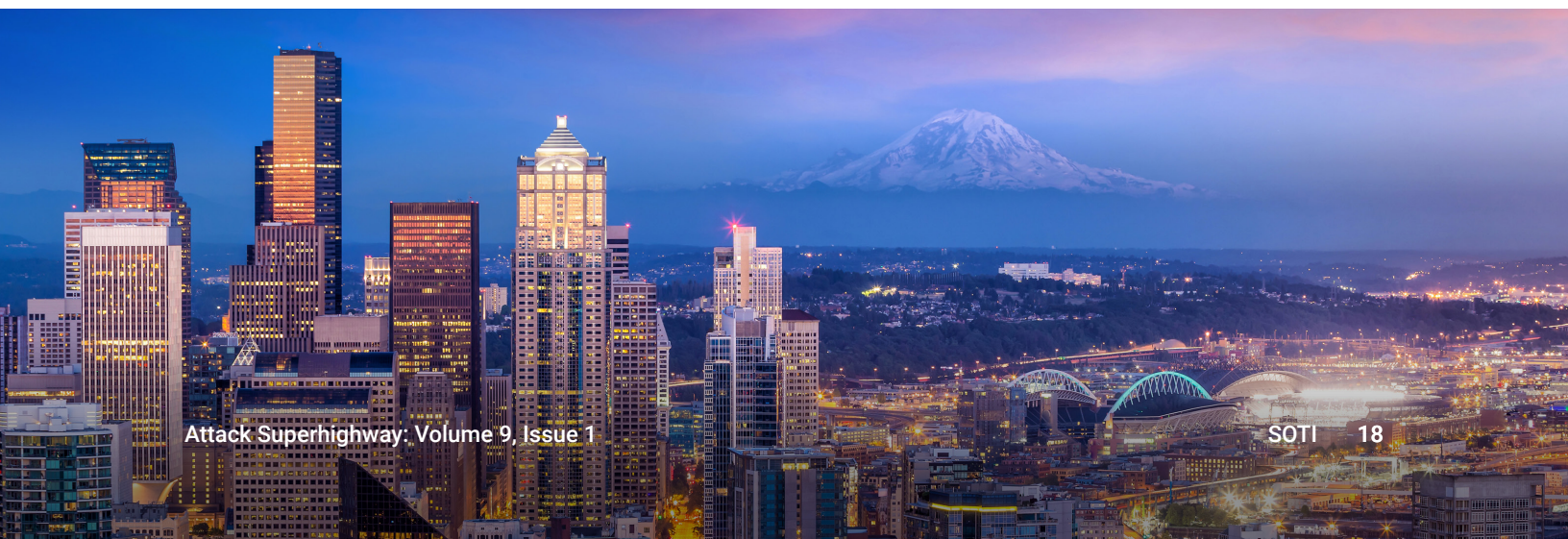


Fig. 8: The majority of affected devices in North American organizations accessed domains related to QSnatch, Emotet, and Ramnit at least once



Europe, the Middle East, and Africa

EMEA has the highest percentage of affected devices next to North America. The top threats we saw in the region (Figure 9) included QSnatch (28%) and Ramnit (21%). It is not surprising to see Ramnit's ascent in the region since its operators targeted [banking/financial institutions in Italy, the United Kingdom, and France](#) in the past. In one of its iterations, Ramnit's configuration included EU countries as main targets. In fact, if one compares the numbers of devices affected with Ramnit globally, EMEA still accounts for the biggest number of Ramnit infections. In addition to that, devices with Emotet infection were also high in the region at 19%.

Percentage of Devices Per Top C2 Threats in EMEA

January 1, 2022 – December 31, 2022

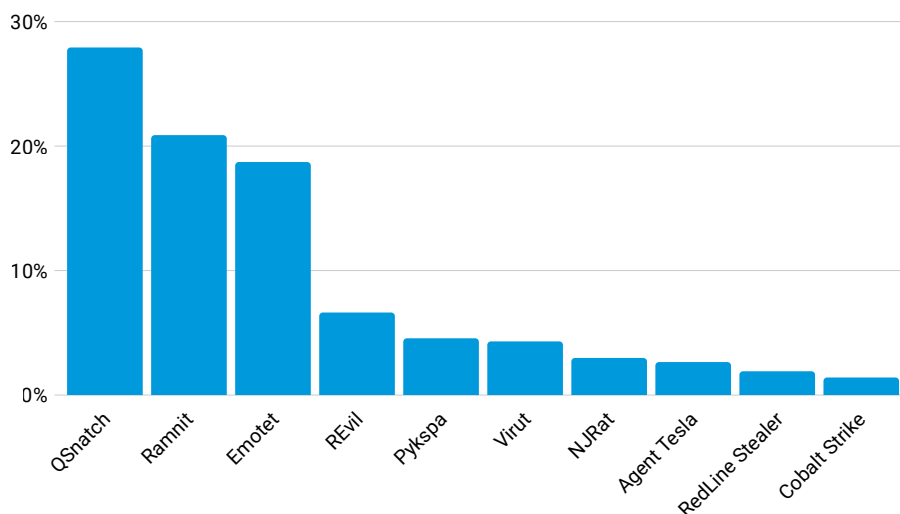


Fig. 9: We saw more devices reaching out to Ramnit C2 in EMEA than in other regions, significantly increasing the risk of their organizations



Asia-Pacific and Japan

In APJ, we saw QSnatch infections significantly impact the region (Figure 10). When we compare the numbers behind each region, APJ ranks second next to North America in terms of devices with QSnatch infections. On the other hand, APJ should also watch out for the ransomware strains REvil and LockBit as they were in the top five threats seen in affected devices in the region. Although members of the [REvil gang were arrested last year](#), this malware was seen again in the wild several months later. It's possible that old members who have access to the code attempted to revive REvil. It is not surprising to see ransomware threats (which are largely financially motivated) like LockBit and REvil. And as RaaS operators continue to leverage IABs like Emotet, ransomware would remain a critical security challenge to businesses across industries and regions.

Percentage of Devices Per Top C2 Threat in APJ

January 1, 2022 – December 31, 2022

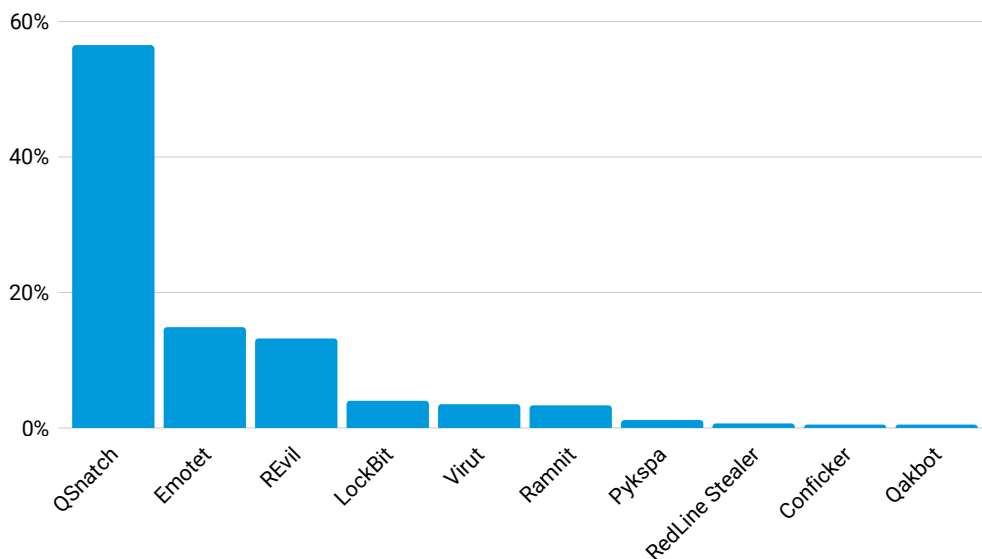


Fig. 10: Akamai observed a significant number of QSnatch infections in the region



Latin America

Let's now examine the trends in LATAM. Although this region has the least number of affected devices, that does not necessarily mean that it is less targeted or impacted. Similar to the global trends, this region has been impacted by QSnatch and Emotet (Figure 11). Just examining this individual region alone would reveal that Agent Tesla, Virut, and Ramnit are prominent.

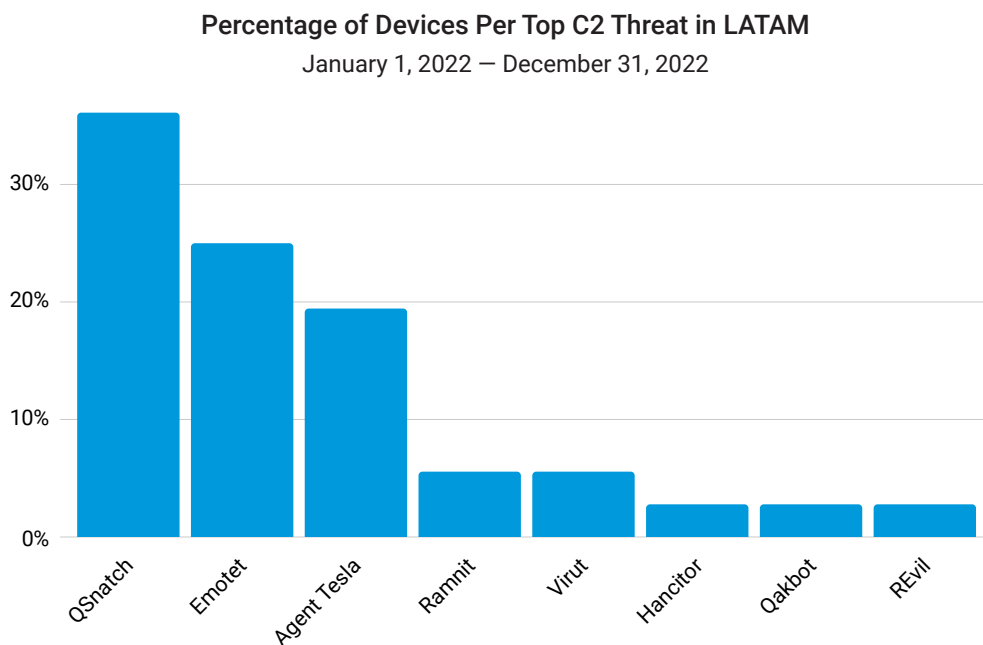


Fig. 11: Global trends also resonate in the threat landscape of LATAM

Regional breakdowns are important to see not only the similarities but also to identify what specific threats are unique for each region. Although QSnatch is always the leading threat family, the next four top threats change across regions with a mix of Emotet, REvil, Ramnit, and Agent Tesla. Regional threats make a difference as you decide what your vulnerability management and pentest teams should focus on.



Industry and vertical trends: manufacturing heavily hit by initial access brokers, botnets

An analysis of industry trends allows us to see the risk level of each individual vertical and how they fare in comparison with other industries. Instead of examining the number of affected devices, we aggregated the devices by customers to come up with how many companies are impacted per vertical (Figure 12). Based on our DNS data, we saw that more than 30% of analyzed organizations with malicious C2 traffic are in the manufacturing sector. In addition, companies in the business services (15%), high technology (14%), and commerce (12%) verticals have been impacted. The top two verticals in our DNS data (manufacturing and business services) also resonate with the top industries hit by Conti ransomware, which we tackled in our [global ransomware report](#). In that report, we dove deeply into the victims of Conti ransomware and profiled them according to vertical, revenue, and region, illustrating attack trends of this prolific threat.

Based on our DNS data, we saw more than 30% of analyzed organizations with malicious C2 traffic are in the manufacturing sector. In addition, companies in the business services (15%), high technology (14%), and commerce (12%) verticals have been similarly impacted.

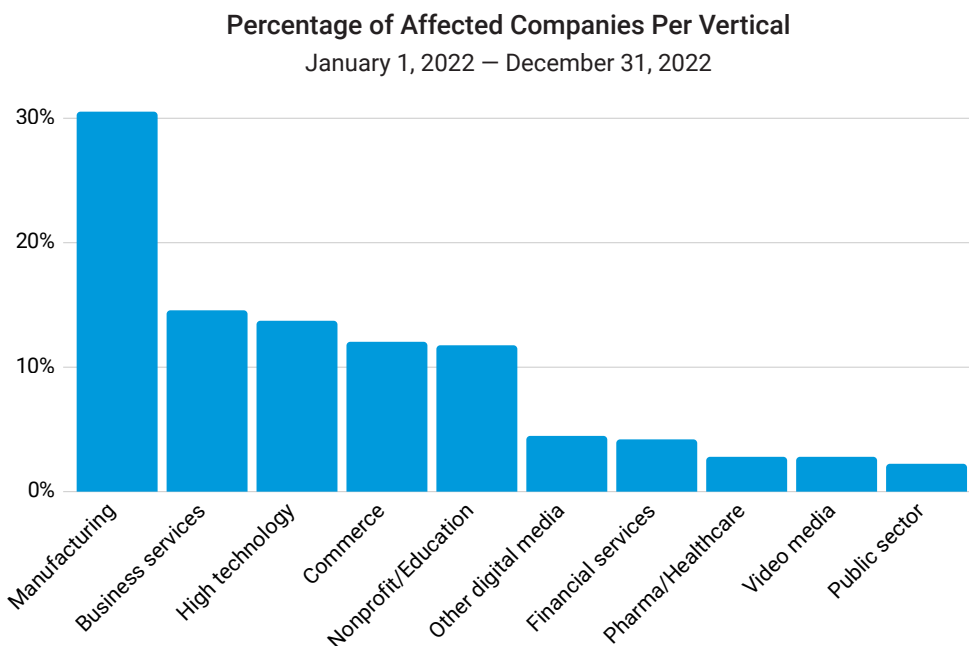


Fig. 12: Manufacturing, business services, and high technology are the industries most affected by C2 infections



The fact that we're seeing that manufacturing is heavily hit by various C2 attacks is concerning since it's considered a critical infrastructure, and successful attacks on this industry could potentially cause real-world effects, such as supply chain disruptions. The data doesn't demonstrate specific reasons as to why manufacturing is the most impacted vertical, but a deeper investigation into threat types in this industry may shed some light.

We are seeing some countries use regulations to bolster security in critical sectors like manufacturing. The EU-wide legislation called NIS2 has strengthened cybersecurity standards and security requirements, such as risk analysis and information systems security policies, supply chain security, and incident handling for essential entities (e.g., energy, transport, banking, health, etc). It has also expanded the scope of impacted verticals.

Percentage of Devices Per Top C2 Threat in Manufacturing

January 1, 2022 – December 31, 2022

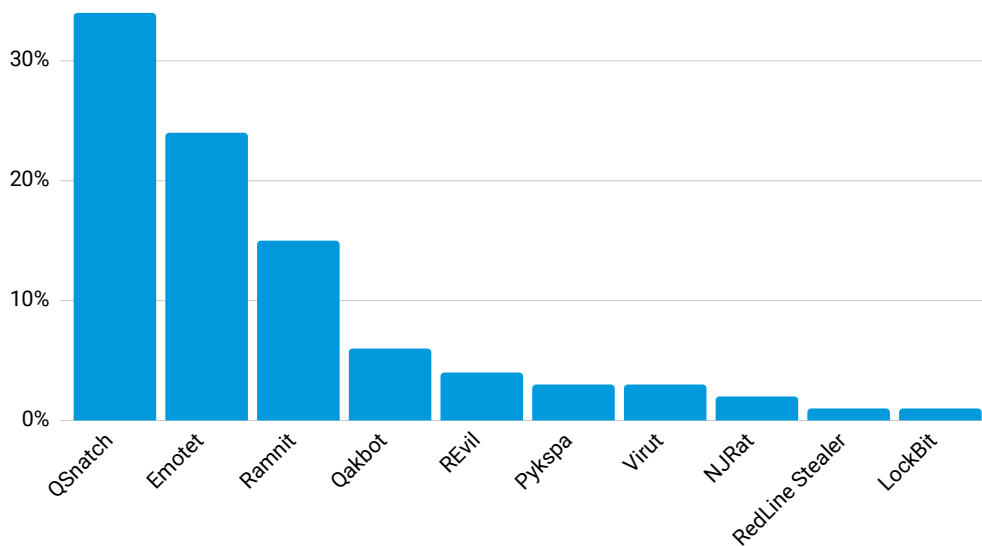


Fig. 13: The top C2 threat families found in the manufacturing industry are QSnatch, Emotet, and Ramnit

An in-depth look at the manufacturing industry reveals that QSnatch, IABs, and Ramnit are some of the top C2-related domains that were accessed by organizations in this vertical (Figure 13). The presence of IABs in their network could be indicative that attackers are gathering intelligence about their potential targets, and once they have access to compromised machines, attackers can sell that data to other cybercriminals like RaaS groups. Moreover, we can also see infostealers in the list of C2 malware that is threatening this industry. One threat to watch out for is [RedLine Stealer](#), which has a capability of harvesting browser information, like credentials and credit card details, and is currently being sold as a MaaS for a US\$100–\$150 monthly subscription. According to [research by Group-IB](#), this infostealer harvested an estimated 35,585,412 logs, which may contain single sign-on accounts, between 2H 2021 and 1H 2022. Moreover, the C2 domains related to this infostealer [surged by 409%](#) in Q3 2022 alone.

Industry trends are always interesting to track. What is happening in one vertical is often just a stepping stone as the cybercriminals work their way across the landscape to all the industry verticals. Sometimes, we see attackers focus on a technology that is prominent in an industry. Other times, they will go after those most likely to pay or to those who would pay the most. We also have seen them go after industries that don't traditionally invest as much in cybersecurity. The takeaway is that when you see smoke next door, it is a good idea to check your own fire prevention system.



Home users under attack

Attackers set their sights on enterprises because it presents a bigger payoff when they successfully breach their networks. They use a wide range of tools and tactics to infiltrate an enterprise perimeter, maintain persistence, and, in some instances, exfiltrate confidential information. As such, we see threats like infostealers and IABs in corporate networks as discussed in the previous section. However, it's a different scenario in home networks, regarding what threats are being employed, and to what end.

Home users represent a demographic that is often not as secure as a corporate environment, but this demographic does not present the same monetary return. Attackers know this and so look for ways to monetize their ability to more easily infect home devices. For example, they launch large-scale campaigns hoping to compromise as many devices as possible in spray and pray tactics, whereas attacks against enterprises are highly targeted. Once these home devices become part of a massive botnet, attackers could mobilize these zombie devices to perform myriad cybercriminal activities without the user's knowledge, like spamming and launching DDoS attacks against organizations. And for botnets to be successful or for cybercriminals to rent their botnets, they need to infect as many devices as possible. Another way for attackers to gain financially from impacting home users is using the computing resources of infected devices for cryptomining purposes.

Once these devices become part of a massive botnet, attackers could mobilize these zombie devices to perform myriad cybercriminal activities without the user's knowledge, like spamming and launching DDoS attacks against organizations.

Home networks show heavy traffic from botnets

As we shift our focus to home users, we will examine the malicious DNS traffic of home networks by analyzing an anonymized sample of the millions of malicious flagged queries from the past six months to demonstrate what threats users should be concerned about. At a glance, the top threats pertain to botnets, which could explain how attackers are leveraging IoT devices for different purposes, which we will discuss in the succeeding sections.

Query Count Per Top C2 Threat

July 2022 – January 2023

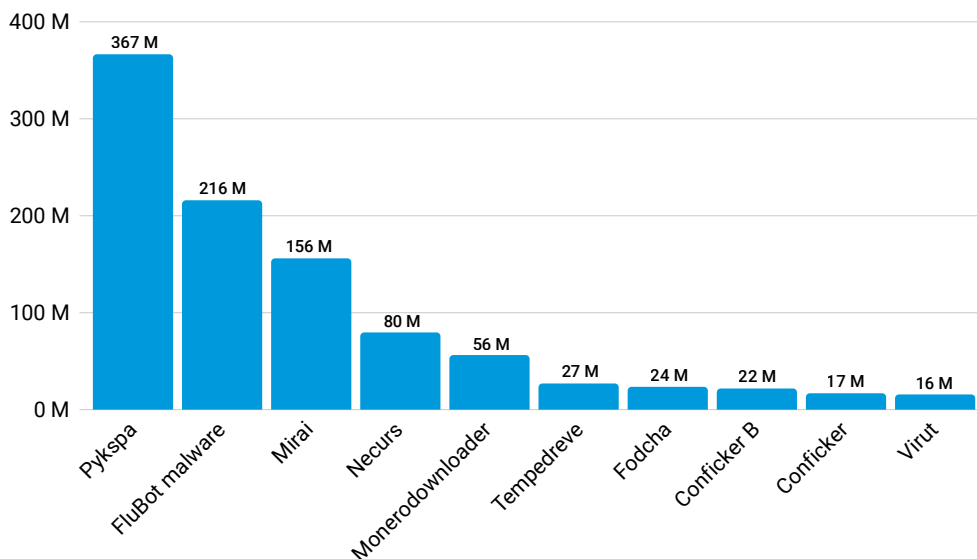


Fig. 14: Pykspa, FluBot malware, and Mirai are the top three botnets observed in the DNS traffic of home networks

Pykspa: propagation via social media

Based on our data findings, Pykspa accounted for 367 million DNS queries flagged globally (Figure 14). This threat spreads through Skype by sending malicious links to the affected users' contacts. In certain cases, when Twitter is opened in the browser's tab, it will also create a tweet with a download link to the malware. In addition, it uses a domain generation algorithm (DGA) in order to establish C2 communication. In the past, its v2 used a [subset of its DGA](#) to prevent being detected, and stay within the network for a longer period.

Its [backdoor capabilities allow an attacker](#) to connect to a remote system and execute arbitrary commands such as download files, terminate processes, and propagate through various means (e.g., mapped drives, network shares), among others. Pykspa also queries the Skype configuration to gather personal information about the affected users. It also prevents the users from accessing certain websites, particularly if they contain certain strings related to anti-malware solutions. Interestingly, it checks the language interface of the affected user's Skype and if it's one of the many languages they are monitoring – including English, German, French, Spanish, and Italian – the malware tweaks the spammed Skype message accordingly.

FluBot: Android malware botnet

FluBot malware is the top C2 malware family after Pykspa. It primarily infects Android phones via text messages, enticing users to click on a malicious link, which subsequently leads to the download of the malware. As part of its [propagation tactic](#), FluBot malware uploads the affected users' contact lists on the C2 server and also sends the victims' contacts with the same social engineering lure. For users, having FluBot on their device puts their banking and financial information at risk since this malware has the capability of overlaying a bogus page when users access legitimate banking apps. As such, these credentials could be used for identity theft or to make fraudulent transactions.

This malware uses various social engineering lures. For example, it may suggest that users click on a link to check the status of their parcel delivery; in other situations, it may trick users into downloading a bogus voicemail app by telling them there's a voicemail message. It may also [pretend to be a security update](#) and urge users to click the link. Once users click the link, it instructs them to download an app. This app, in turn, asks for permission to access contact lists and make phone calls, etc. What makes this threat so dangerous is that it also [requests permission for Accessibility Services](#) allowing attackers to control screen taps, potentially leading to installing more apps. Users are advised to [factory reset their devices](#) to remove this malware.

Mirai: harnessing the power of the Internet of Things to cause wide-scale disruption

In our research, Mirai follows closely on the heels of FluBot malware, with 156 million flagged DNS queries. Known for targeting IoT devices with open telnet ports, Mirai became infamous for the [DDoS attack](#) against one of the largest DNS providers. This self-propagating worm looks for vulnerable devices that use the default username and password combinations. At one point, it amassed a flock of more than [100,000 zombie devices](#) that the attackers used in DDoS attacks against high-profile targets. In one of its earlier attacks, [Mirai leveraged 145,000 devices](#) for an assault on a technology company. This is one example of how unsecure devices could be weaponized to commit cyberattacks and cause wide-scale disruption against enterprises.

In 2016, the group behind [Mirai released the source code](#), possibly to prevent law enforcement from tracing it back to the original authors (and to, therefore, avoid arrest). With this, other groups began to use Mirai's code, [modifying and enhancing it with more functionalities](#), such as being able to infect systems. One of the effects of releasing the code in the wild is that we've seen new variants, like Okiru, Satori, Masuta, and PureMasuta, with the purpose of launching DDoS attacks as well. Although rebooting the infected device helps, since the malware is constantly scanning for devices, there's a high likelihood of being reinfected unless the user changes their passwords.

Necurs: malware distributor and access seller

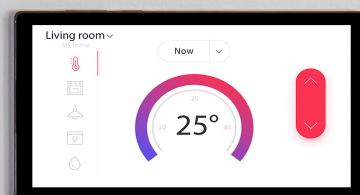
The Necurs botnet, which was first spotted in 2012, accounted for 80 million flagged queries over the past six months. It poses serious risk to home users and organizations alike with its capability of [delivering other malware payloads](#) like Dridex, TrickBot, and Locky, among others. One notable factor worth highlighting is that this botnet also [sells access](#) to infected computers to other groups as part of its botnet-for-hire offerings. Like most botnets, it uses a DGA to churn multiple domains for its C2 servers and to continue its operations despite domains being blocked.

Apart from distributing ransomware and banking Trojans, Necurs is also used to distribute various spam attacks, like Russian dating scams, pharmaceutical scams, and so forth. During an investigation, Microsoft monitored the activities of this botnet and found out that in just 58 days, it sent out approximately 3.8 million spammed email messages. In 2020, the [operations of the Necurs botnet were disrupted](#) through the collaboration of law enforcement and the security community.

Monerodownloader: mining botnet

One of the many ways in which attackers gain profit is to use compromised machines for cryptomining. The increasing popularity of the cryptocurrency Monero among cybercriminals is one reason why we're seeing botnets made specifically to mine it. Attackers prefer this cryptocurrency since the chain is not as exposed and it offers anonymity; therefore, it doesn't get traced back to them. Although very little is known about Monerodownloader, some of the tactics it performs include gathering information and connecting to C2 servers for the actual payload.

Leaving systems unpatched paves the way for threats like Monero cryptominers. Other similar Monero coinminers leverage vulnerabilities, pose as free software to lure users into downloading the miner, and have capability of moving laterally through the network and infecting other devices to gain as much revenue as they can. Although the description of lateral movement is more applicable to companies than home users, this gives us an insight on how cryptominers work to maximize infection.



Top threats per region: botnets continue to reign in home networks

Let's take a closer look at our regional data to elucidate which specific botnets are prevalent per region based on the DNS traffic of home networks, and to examine some possible factors that contribute to such a trend.

North America

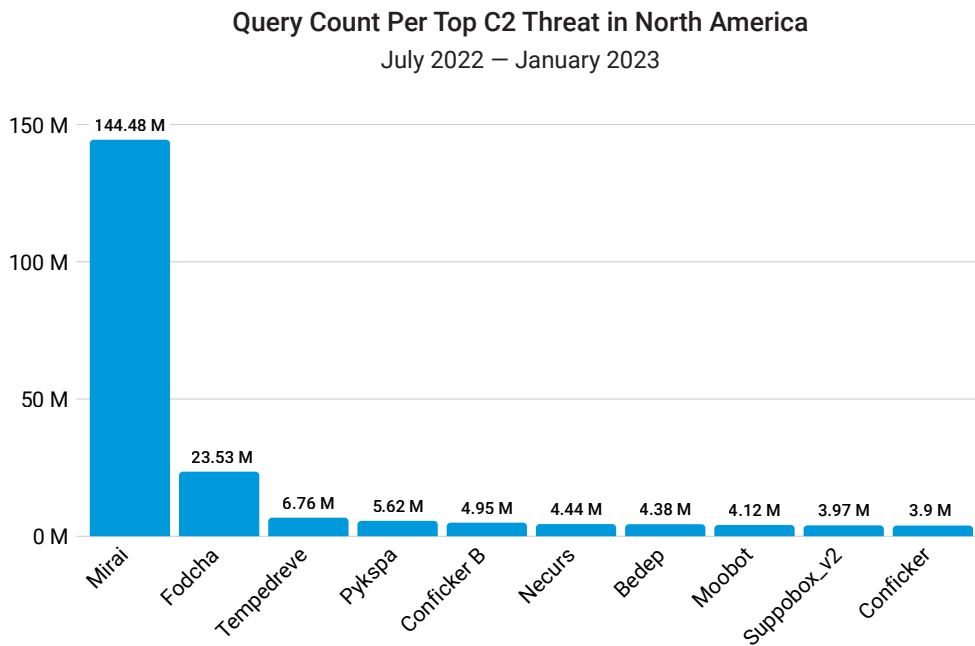


Fig. 15: Mirai continues to make waves in North America potentially because of unsecure IoT devices

In North America, more than 144 million queries associated with the Mirai botnet were seen in home networks (Figure 15). This botnet targets vulnerable IoT devices that are still using default usernames and passwords. The high volume of queries coming from this region could be due to the popularity or high usage of IoT devices in households. In 2022 alone, U.S. households [reportedly](#) have an average of 22 connected devices, which slightly decreased from 25 the previous year. And with IoT connections [predicted to increase](#) in North America (5.4 billion by 2025), there is a high probability of more threats like Mirai, or similar variants, that abuse unsecure IoT devices.

For home users, the impact of such a threat is that cybercriminals can exploit their devices without their knowledge to commit crimes. But organizations also suffer from the effects of DDoS attacks, or even from malicious spam campaigns, launched by botnets like Mirai. As best practice, it is always a good idea to change the default username and password of your devices to protect them from Mirai and other similar attacks.

Europe, the Middle East, and Africa

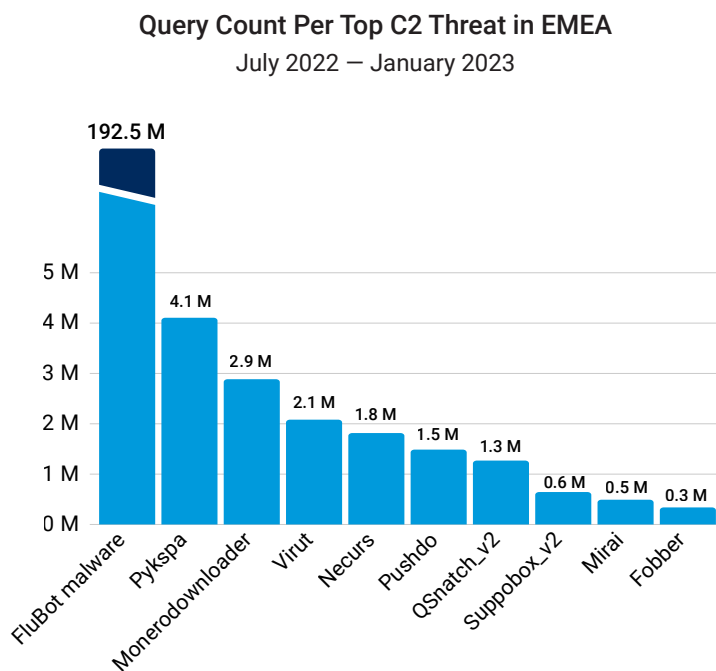


Fig. 16: We saw an outbreak of FluBot malware in the EMEA region possibly due to its propagation tactic and its use of several European languages as part of its social engineering bait

To say that FluBot malware is spreading like wildfire in EMEA would be an understatement. The whopping volume of the DNS queries observed in this region (approximately 193 million) is notable. And through our examination of the DNS traffic, Akamai was able to see these infections happening in EMEA (Figure 16). One contributing factor is its propagation tactic of smishing – a form of phishing in which the attacker sends out SMS to the victim’s contact list. In addition, it tricks users into downloading an app related to a package delivery or voicemail app that is actually the malware. Apart from this, FluBot asks for additional permissions and secretly logs users’ banking/financial credentials without their knowledge. It reportedly [targeted users](#) in Spain, Germany, Finland, and the United Kingdom, among others. The SMS is also written in multiple other EU languages, like German and Hungarian, which could be one of the many factors this malware surged in Europe.



Latin America

Query Count Per Top C2 Threat in LATAM

July 2022 – January 2023

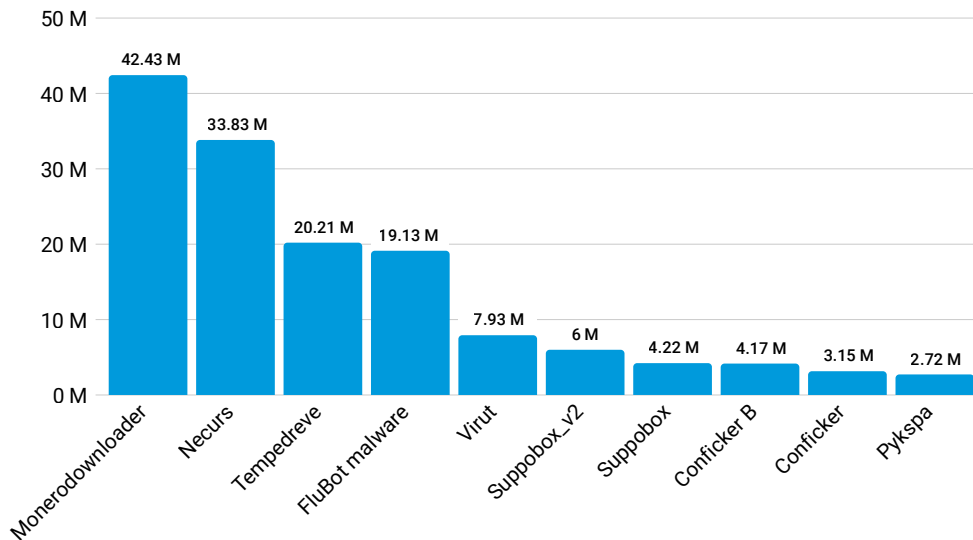


Fig. 17: The Monerodownloader cryptomining botnet became the top threat in Latin America possibly due to the high usage of crypto in the region

Unlike North America and EMEA, the LATAM region showed a more diverse distribution of botnets (Figure 17). Monerodownloader, a cryptomining botnet, leads the list of active botnet groups at 42 million flagged queries, followed by Necurs (34 million) and Tempedreve (20 million). The high [adoption rate of cryptocurrency](#) in the region, fueled by high inflation and remittances, could explain why botnets like Monerodownloader topped the list. Without the user’s knowledge, cybercriminals could be using the resources of user devices for mining purposes, and for their own financial gain. It is also worth noting that FluBot is one of the top threats observed in the DNS traffic, which shows the botnet’s prevalence even outside the EMEA region, where we saw a high volume of traffic.

Asia-Pacific and Japan

Query Count Per Top C2 Threat in APJ

July 2022 – January 2023

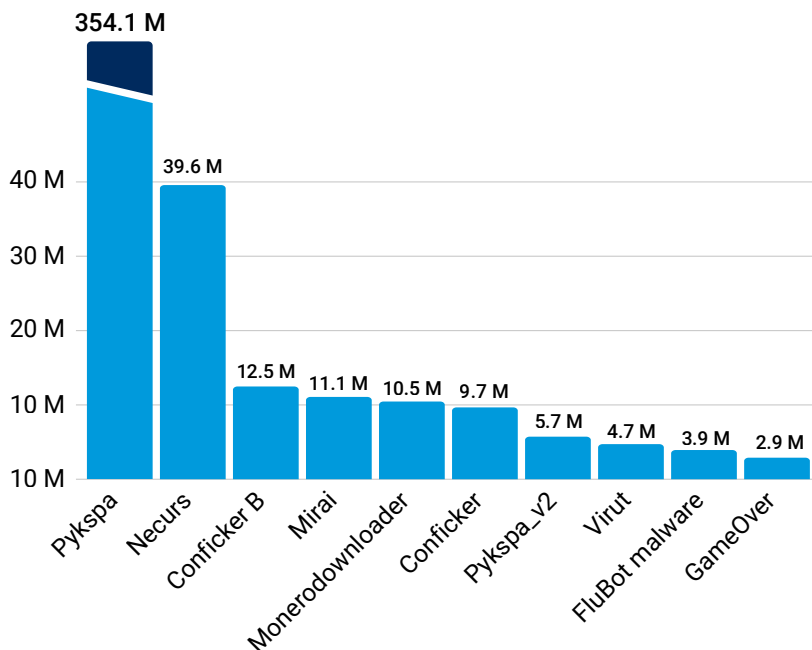


Fig. 18: The dominant threats in APJ include Pykspa and Necurs

More than 350 million queries related to Pykspa were observed in APJ (Figure 18). In a 2019 [blog post](#), we noted that Pykspa used a selective DGA mechanism to remain under the radar for a long period. The domains highlighted in that report were mostly found in East Asia. We also observed queries associated with botnets like Necurs, which is a strong indicator that systems are infected with other malware.



Phishing landscape overview

In the last part of our DNS traffic analysis, we examined phishing kits and their crucial role in the success of the phishing campaigns. Phishing is still relevant – more than ever – due to the constantly evolving tactics used by adversaries and the increasing amount of personal information available online. Adversaries are using social engineering to make their phishing attempts appear legitimate, and evidence indicates that the success rate of these attacks remains high. Akamai’s research on [holiday phishing scams](#) revealed new techniques and tactics being used by adversaries to continue to stay under the radar. These novel tactics include using fake users’ testimonies as part of the scam and the newly discovered technique of using HTML anchoring to make sure only valid users land on scam websites.

The increase in remote work due to the COVID-19 pandemic has also made it harder to detect and prevent phishing attacks, making it more important for individuals and organizations to stay vigilant and take steps to protect themselves. Additionally, the rise of social media and the increasing number of devices connected to the internet have created more opportunities for adversaries.

Phishing campaigns hit financial services

When investigating which brands are being abused and mimicked by phishing scams, there are a number of ways one can collect the data. We collated the total number of campaigns versus the number of victims. This allows us to assess the success rate of a given campaign, as well as to see what percentage of each industry is being targeted.

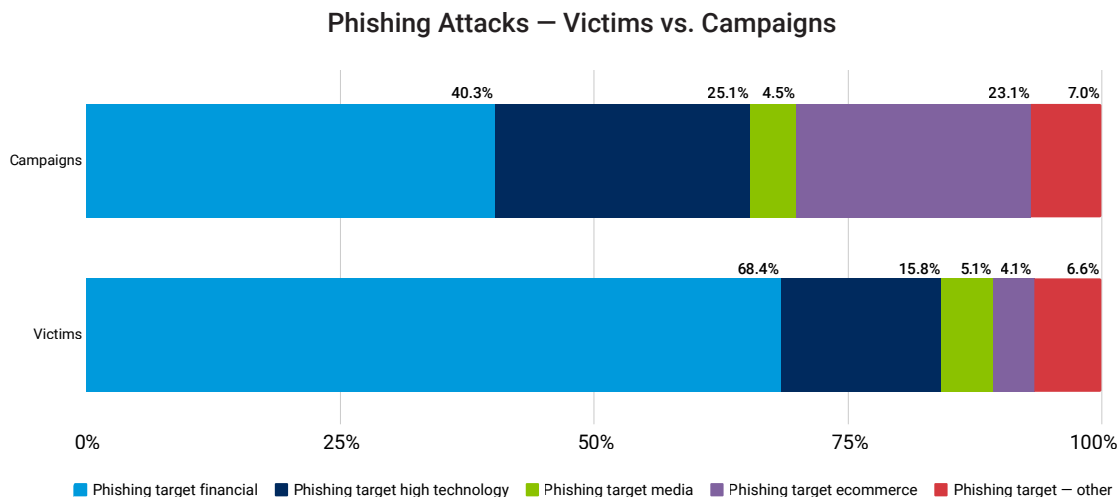


Fig. 19: The majority of the phishing campaigns targeted the financial services industry (Q4 2022)

Our research found that financial and high technology brands led in both the number of campaigns and victims (Figure 19). We saw that 40.3% of campaigns on financial services customers were activated, resulting in 68.4% of victims, indicating that attacks against financial services were highly effective in Q4 2022. In our financial services report, [Enemy at the Gates: Analyzing Attacks on Financial Services](#), we underscored how phishing attacks are financially motivated and mostly target financial services and its customers. The potential impacts of such attacks include damage to brand and reputation and loss of customer trust. Phishing could also cost the organization resources to fix the issue.

Ecommerce saw 23% of phishing campaigns activated Q4 2022. Although we saw more campaigns than actual victims, it is also worth noting that attackers are targeting this industry and users must remain vigilant as cybercriminals may be after their personal or banking information.

Phishing toolkits: enablers of phishing scams

The overwhelming phishing landscape scale and magnitude is being driven by the existence of phishing toolkits. Phishing toolkits support the deployment and maintenance of phishing websites and enable even nontechnical scammers to join the phishing adversary landscape and execute phishing scams.

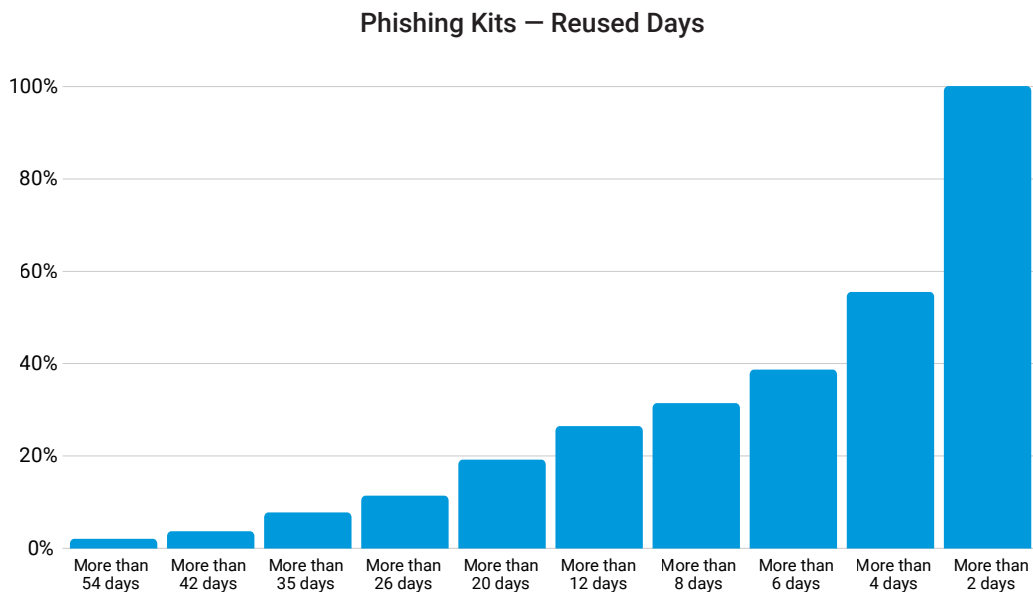


Fig. 20: Phishing toolkits by number of reused days (Q4 2022)



According to our research, which tracked more than 300 different phishing toolkits being used in the wild to launch new attack campaigns, 2.04% of the tracked kits were reused on at least 54 distinct days in Q4 2022 (Figure 20). Further, 55.5% of the kits were reused to launch a new attack campaign on at least four days, and 100% of the tracked kits were reused on no fewer than two distinct days over Q4 2022.

Conclusion and recommendations: combat modern attacks with proactive measures

Now that we have covered threat groups and attacker methodologies, let's talk about how to leverage all that information. We'll start with how to manage DNS – internally or outsourced to a third party. For larger or more complex organizations, it makes sense to have a provider who specializes in managing DNS take care of it for you. Either way, ensure you monitor performance and protections for your DNS. Next, consider the different controls that you will need. DDoS protection, malware attacks and scraping, lateral movement, and exfiltration are the key areas to mitigate. Following this data journey and looking for all the critical vulnerabilities you can stop at every step is a cybersecurity model often referred to as the cyber kill chain.

Consider creating playbooks for the attack techniques covered in this report. Check with your pentest team or red team to determine if they use the same tools and techniques as IABs such as Qakbot and Emotet, bots such as QSnatch, ransomware such as LockBit (in lab environment), and tools like Cobalt Strike. It is important to make sure your security controls are alerting and stopping these types of attacks effectively, and that your teams are trained to address them.

If Cobalt Strike is detected in your network, it is prudent to immediately create an incident report and investigate it. Although the tool could be employed by your red team (in which case, it should be investigated and reported nonetheless), the presence of such traffic should sound the alarm as this could indicate intrusion by other RaaS attacker groups or threat actors, and signal an ongoing attack that could still be mitigated.

Consider how your security operations center operates and determine how you are tracking processes (like bits, Wget, or cURL) that could possibly indicate the likelihood that an IAB-related threat is in the network doing reconnaissance. The critical parts are figuring out what was downloaded and stopping it if it's still running. Then, investigate what triggered the IAB – Was it an LNK file, macro, or VScript? – and discover from there how the breach started.

Stay plugged in to our latest research by checking out our [Security Research Hub](#).

Methodologies

Command and Control Attack Traffic

The data in this report is generated by our Secure Internet Access (SIA) product and describes command and control (C2) attack traffic. SIA is a cloud-based secure web gateway that is designed to help users easily connect their devices to the internet in a secure manner. The two different sets of data utilized throughout this report separately reflect security alert data from either enterprise organizations with large amounts of users or internet providers with individual home users. This data was measured by the number of affected devices and the number of queries, respectively. An affected device was defined as a device that reached out to a known and identified C2 domain at least once. Similarly, a C2 query was defined as a query that reached out to a known and identified C2 domain. Our security teams use this data in-house to research attacks, flag malicious behavior to notify customers, and feed additional intelligence into Akamai's security solutions.

Credits

Editorial and Writing

Or Katz

Eliad Kimhy

Badette Tribbey

Review and Subject Matter Contribution

Tanya Belousov

Stiv Kupchik

Shiran Guez

Grace Wang

Ophir Harpaz

Steve Winterfeld

Data Analysis

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

Marketing and Publishing

Georgina Morales Hampe

Shivangi Sahu

More State of the Internet / Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet / Security reports. akamai.com/soti

More Akamai Threat Research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research.

akamai.com/security-research

Access Data from This Report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

More on Akamai Solutions

To learn more about Akamai solutions for threats targeting enterprises, visit our [Secure Internet Access Enterprise](#) page. Service providers targeting consumer and SMB markets can visit [Secure Internet Access services for ISPs](#).



Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on [Twitter](#) and [LinkedIn](#).
Published 03/23