COMCAST BUSINESS

2023 Comcast Business Cybersecurity Threat Report

Contents

01.

Executive summary

The global cybersecurity community is at a crossroads.

Technology is accelerating faster than it ever has before, giving IT and security teams more tools to fend off cybersecurity attacks from an increasingly diverse slate of bad actors. However, the tactics attackers are using to access systems are also growing more sophisticated by the day. Access to armies of botnets and sprawling lists of customer data are just a few clicks away on the dark web.

While the attackers' tools have changed, their tactics remain built upon the same foundation of emotional manipulation and social engineering that is the hallmark of most hacks and scams. So for CISOs and CIOs, it's the same old game, but with rapidly changing rules. In an environment where change is the status quo, staying actively informed has become the bare minimum.

The 2023 Comcast Business Cybersecurity Threat Report was developed to help technology and security leaders get a deeper understanding of trends in cybersecurity threats—and the steps they can take to help protect their organizations from an evolving set of threats. Our goal is to provide insights from billions of threat data points and context around common ways that cybersecurity attacks arise and unfold.

As any experienced cybersecurity analyst will tell you, it's impossible to look at individual cybersecurity risks and vulnerabilities in isolation because attacks are never about any single tool, tactic, or procedure (TTP).

This report provides a wide-angle view, based on the analysis of 23.5 billion cybersecurity attacks Comcast Business detected across our vast pool of security customers in 2022. The numbers presented throughout the report represent the collective and anonymized data of customers using Comcast Business security solutions, including DDoS mitigation, endpoint detection and response, vulnerability scanning and exposure management, managed detection and response, and others.

Leveraging this volume of firsthand data from across different vectors helps shed light on the current threat matrix, illustrate the complex and multi-layered strategies bad actors employ, and determine where to direct risk mitigation efforts.

Presented in the context of the MITRE ATT&CK© framework where applicable, the numbers illustrate the interconnectedness between attack vectors, the far-reaching impacts of the attacks, and the relative simplicity with which the attacks are executed.

In this report, we explore:

The anatomy and chronology of a cyber attack

From pre-attack reconnaissance and initial attempts to access, lateral movement, discovery, and extraction, we'll unpack every stage of a cyber attack and the tools and methods adversaries use to gain access to and exploit your network and systems.

Critical links between malware and phishing

With the majority of malware delivered via phishing, it's imperative to understand the doors that phishing opens to network access and how adversaries use backdoor malware—with 14 million attacks observed in 2022—to establish command and control centers and ensure repeatable access.

A growing vulnerability landscape

Over 26,000 new application and infrastructure vulnerabilities were added to the National Vulnerability Database last year. Explore the most prevalent categories, walk through the top 10 vulnerability exploits observed by Comcast Business in 2022, and understand evolving best practices for patch management.

Common evasion tactics

Once inside a network, adversaries use ever-changing techniques to elevate permissions, hijack credentials, modify policies, and gain root access to other systems while appearing invisible to security teams. This report will walk through the nearly 27 million suspected evasion tactics logged by Comcast Business last year, including critical vulnerabilities exploited in common business software applications.

Exfiltration and impact techniques and consequences

Adversaries always have an end goal. Explore the most common manipulation tools enemies use to extract value from data and systems, including data theft, ransomware, resource hijacking, and distributed denial of service.

As a critical network provider, offering connectivity and security services to businesses of all sizes, we're proud to launch the first iteration of this report. We hope it will help technology leaders understand—based on real-life data—where the most pressing threats loom and how they can best invest their cybersecurity efforts and resources.

Context matters

Context helps us understand the causality and effects of what happened. Without context, a phishing attack is just that, a phishing attack. With context, we can see how a phishing attack can domino into devastating impacts like data encryption and organization-wide lockouts. Awareness of the experiences of other organizations can help you determine the right tools to shore up cybersecurity, the best path to align organizational strategy with cybersecurity best practices, and the considerations for selecting the right kind of cybersecurity partner.

A potential breach is closer than you think

Every organization, regardless of size, can be one click away from a potentially devastating cyber attack. Worse, given advances in technology, hackers often don't have to expend serious effort—or even be highly skilled—to find and abuse many weaknesses in your threat surface. All one needs is the desire and ability to break in.

Most attacks used to begin with an exploit of a vulnerability in your public facing network resources that connect to applications and infrastructure within your network perimeter. Today most breaches originate with the users of internal and external resources. Research has shown that approximately 67% of all breaches start with someone clicking on a seemingly safe link[1], which explains why adversaries begin 80-95% of all attacks with a phish.[2]

Whether you know it or not, adversaries are testing your networks, systems, and users for vulnerabilities daily. Attack attempts are inevitable and beyond your control. What you can control is whether you plan and prepare for attacks before they happen or deal with the aftermath later.

1. IdentityIQ
2. USA FBI, Deloitte, cybertalk.org, csoonline.com

23.5 Billion

Cybersecurity attacks

242.8 MILLION
RECONNAISANCE

24.7 MILLION
RESOURCE DEVELOPMENT

2.03 BILLION
INITIAL ACCESS

3.2 BILLION
EXECUTION

49.3 MILLION
PERSISTENCE

222.8 MILLION
PRIVILEGE ESCALATION

831.7 MILLION
DEFENSE EVASION

176.7 MILLION
CREDENTIAL ACCESS

0.4 MILLION
DISCOVERY

155.3 MILLION
LATERAL MOVEMENT

6.25 BILLION
COMMAND & CONTROL

143.9 MILLION
EXFILTRATION

10.1 BILLION
IMPACT

Keeping adversaries out

Not all exploits happen inside your networks. But with the exception of some types of attacks, like Distributed Denial of Service (DDoS), most adversaries want to breach your networks because that is where your crown jewels reside. Your data, your reputation, your productivity, your services—you name it, adversaries want it. Once inside, the tactics used to spread and destroy escalate quickly and the extent of the damage is often proportional to how well and for how long the adversary can evade detection.

Identifying common breach tactics

Adversaries have access to an impressive toolbox of tactics for breaching your networks, but phishing is still the most popular. This holds true for everyone from the lone wolf attacker to nation states. Why? Because phishing is inexpensive, versatile, extremely simple to execute, and devastatingly effective. Our data shows that phishing, although not the only method for breaking in, was used much more often than other methods. In fact, nine out of 10 attempts to breach our customers' networks started with a phish, which is in line with industry statistics.[3] It's popular because it works.

Other notable methods are abused credentials and exploited public facing resources like remote desktop and email servers.

Once inside, everything is fair game

Once attackers do get inside, the defense posture shifts from detect-and-prevent to hunt-and-respond or mitigate. It's not always easy. Many attacks are hard to detect, especially fileless threats, zero-day vulnerabilities, and unknown threat vectors never seen "in the wild." That's why it's so important to look for risky behavior and to maintain strong threat intelligence.

Defending at scale

During 2022, Comcast Business customers were subjected to 23.5 billion cybersecurity attacks designed to break in, move laterally, escalate privileges, identify and exploit high asset systems, exfiltrate or destroy data, and cut off access to critical resources.

Detecting, blocking, and mitigating this level of activity, spanning 500 threat types and 900 unique infrastructure and software vulnerabilities requires not only expertise, but scale. Many in-house security teams simply aren't equipped with the staff and resources to keep up with a vast array of quickly evolving, sophisticated attacks.

3. Trend Micro

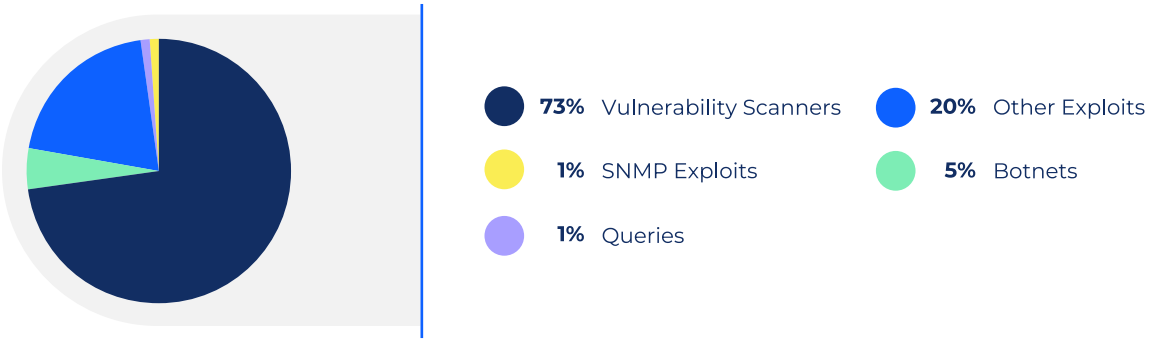
Inside an attack timeline

Reconnaissance & initial access

Adversaries do their homework to uncover vulnerabilities like exposed and open ports or misconfigured systems. Active and continuous malicious scanning of our customers' networks and assets was detected on at least 242 million[4] occasions.

Reconnaissance isn't inherently dangerous and can even be conducted for benign or legitimate purposes. It does, however, reflect overall adversary interest in a potential victim, increasing the importance of accepting network connection requests only from trusted sources.

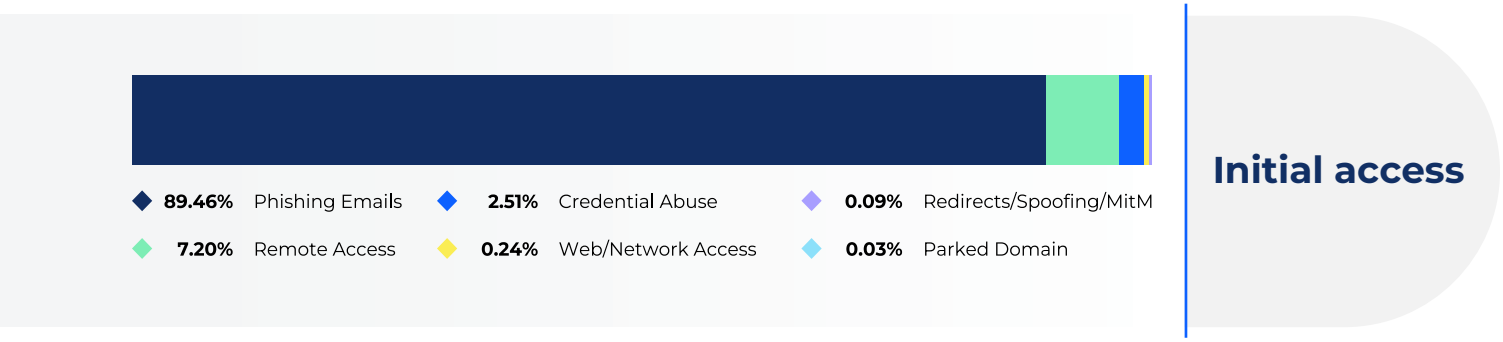
Figure 1: Reconnaissance tools used by adversaries attempting to gain access to Comcast Business customers in 2022



Casting the bait with phishing

Phishing remained the most popular vector used by adversaries to gain initial access to target networks. We detected almost two billion (1,830,533,465) phishing attempts, most of which were directly identifiable as attempts to gain initial access. It's important to acknowledge that phishing isn't necessarily effective in harvesting credentials in bulk. However, it excels at exploiting human nature to gain an initial foothold to breach networks, which can enable adversaries to access domain servers and databases that yield credentials in bulk.

Figure 2: Tactics used to gain initial access to networks and systems



4. Comcast Business tracked 210,768,825 reconnaissance scans during 2022.

Broadening the impact

As discussed earlier, very few attack activities can be considered in isolation. A number that tells you how many phishing attempts were made is interesting, but understanding how the same attack vector is leveraged across multiple stages of an attack cycle is more interesting. Case in point, we identified numerous phishing campaigns that included malicious URLs or attachments for credential-stealing malware, a tactic commonly used by adversaries in later stages of an attack.

Figure 3: Partial list of credential-theft malware detected and disabled in phishing attempts by Comcast Business in 2022

34%

Financial Information & Credentials

- Phishing campaigns containing spoofed URLs for banks, designed to steal information necessary for credit card theft.
- Qadars, Terdot, Tinba, and Fobber were just a few of the malware payloads employed.
- Feodo malware, a Trojan designed to steal online banking credentials, was also used in multiple campaigns.

60%

Other Credential Theft

- Phishing campaigns using actual posts within social media pages. These posts use URL shorteners for linking to phishing sites to evade getting flagged and removed by the social media platform.
- Malware/botnets like Keylogger, Ursnif, Ramnit, and Zeus, widely known for stealing credentials.
- Droidpak malware, specifically designed to steal users' online banking credentials, was detected on multiple occasions.
- Dyre Malware, which was designed to steal user login credentials, yields first-level credentials that can then be used to exfiltrate customer data.
- Carberp and Sinowal trojan, designed to record usernames/passwords and other sensitive data, were detected multiple times.

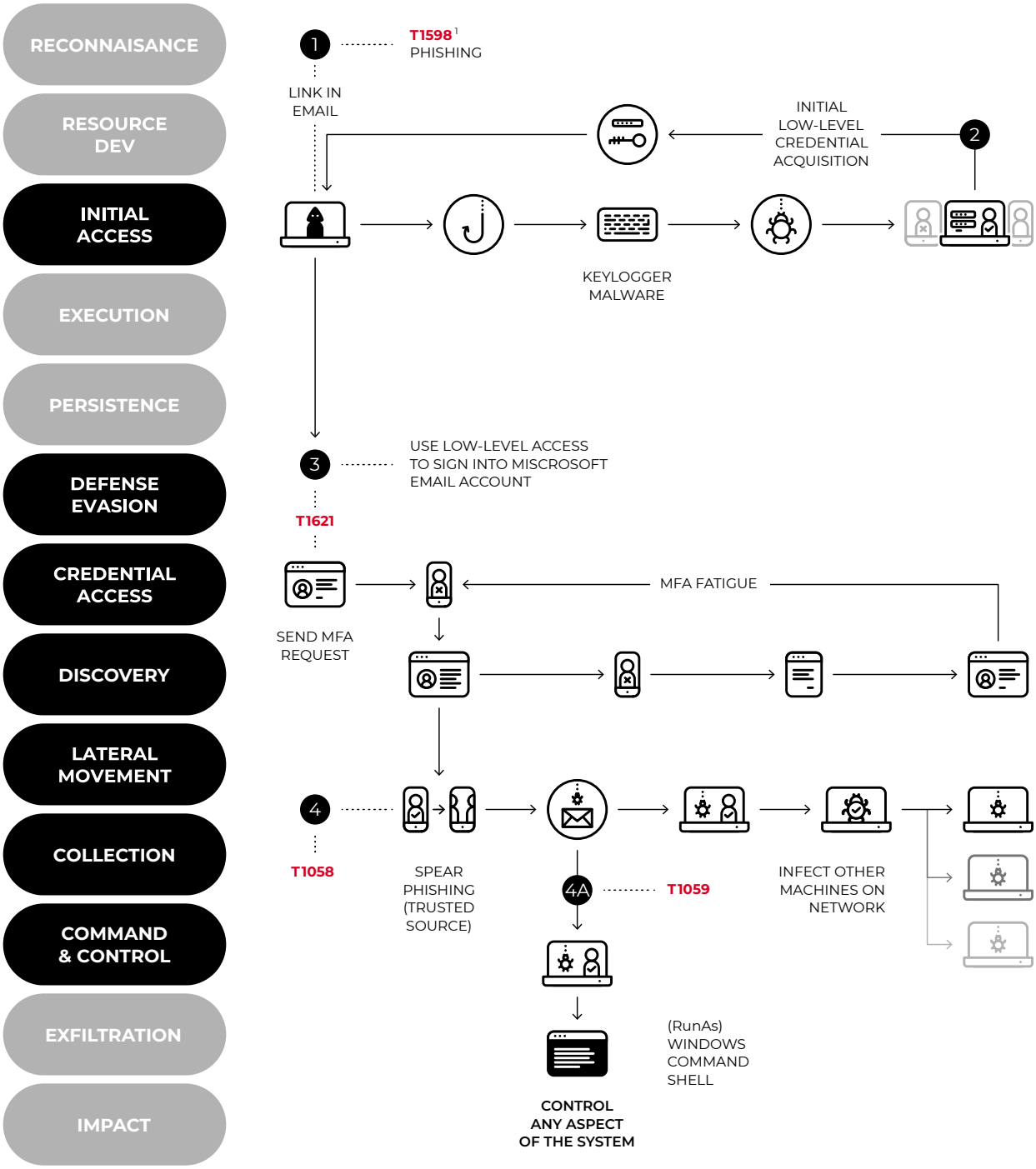
6%

Theft Involving Malicious Documents

- Multiple phishing campaigns using malicious documents that require user interaction.

The MITRE ATT&CK© FRAMEWORK

Figure 4: The MITRE ATT&CK© Framework highlights the importance of implementing a comprehensive set of controls to defend yourself holistically across application, identity, network, and server resources. In this example, identified by our Security Operations Center (SOC), a single user clicking on a phishing email started a chain of events that ended with the adversary gaining access to the Windows PowerShell Command Line Interface (CLI).



[1]Part of the MITRE ATT&CK framework, "T" codes represent techniques adversaries employ to carry out a tactic. https://attack.mitre.org/techniques/enterprise/

Stolen credentials make good business

Any adversary that obtains "legitimate" credentials is a powerful nemesis – one who can authenticate applications, bypass security, elevate privileges, and conduct malicious activities at will. Our logs indicate over 54 million attempts to abuse credentials for initial access, spanning everything from brute-force to failed login attempts.

Dark web marketplaces are brimming with stolen credentials for sale, the most sought after of which are valid credentials for Remote Desktop Protocol (RDP) access[5]. Approximately 68% of dark web posts analyzed by Kaspersky were related to the sale of credentials for RDP access.

Remote desktop: a growing vulnerability

Many organizations rushed to enable remote access for their employees during the COVID-19 pandemic, which sometimes led to leaving unused ports open and exposed. Adversaries exploited vulnerable RDP configurations and made over 185 million attempts to gain remote access to our customers' networks. RDP exploits are also increasingly being used to infect networks with ransomware like Maze, Venus, and Ryuk.[6]

Network exploits did not stop with RDP. Unauthenticated users exploited vulnerabilities in Transmission Control Protocol (TCP) and made 139 million attempts to establish TCP connections to victim servers.

Remote access & TCP connection attempts detected by Comcast Business in 2022

+185M
Remote access attempts

+139M
TCP connection exploits

Other notable initial access culprits: parked domains

Phishing, RDP exploits, and credential abuse vectors accounted for 95% of all initial access attempts. Parked domains, MitM campaigns and malicious URLs made up the remaining 5%.

5. Kaspersky
6. ransomware.org

04.

Your network has been breached – now what?

Understanding the link between phishing and malware

Discussing malware in the same breath as phishing is natural because both are tightly linked. Given phishing's ease and efficacy, it has become the de facto delivery mechanism for most malware attacks.

Our data reveals similar trends with evidence of significant malware activity following successful phishing campaigns and initial perimeter breaches.

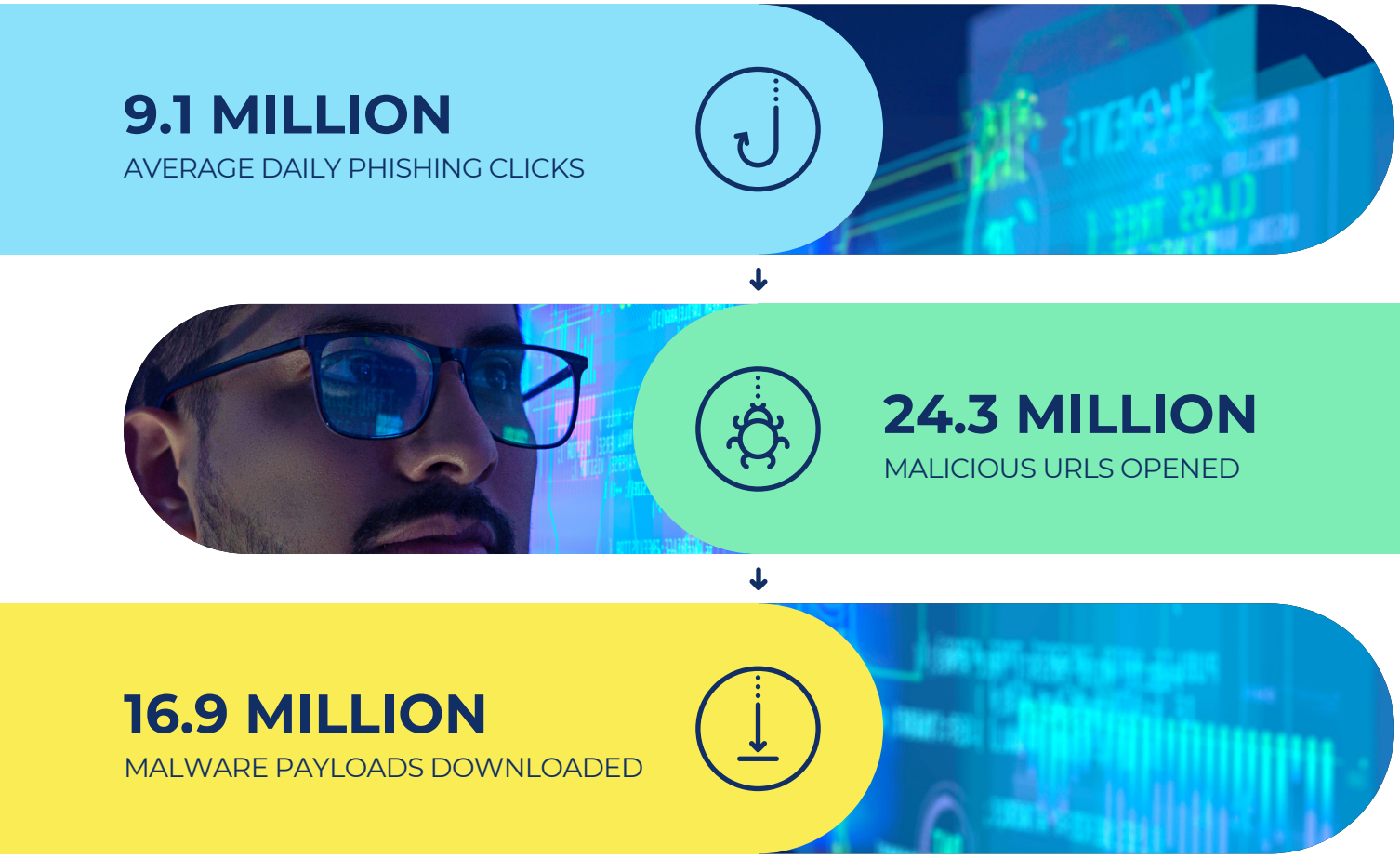
Once inside the network, adversaries move quickly with early-stage malware payloads to scan networks and endpoints for exploitable vulnerabilities, establish external Command and Control centers (C&Cs) for remote access, and implement evasion tactics to avoid detection.

Detecting and blocking malware

14.9B
Malware/Botnet-related activities detected

6.2B
Backdoor Malware connection attempts blocked

Figure 5: Following phishing's impact: Post-phishing activities detected by Comcast Business in 2022



Backdoor malware: the gift that keeps on giving

As mentioned above, one of the first things adversaries want to do after breaching your networks is to make sure they can drop in and out anytime they want. Machines compromised with backdoor malware create encrypted reverse SSH-proxy tunnels to establish communication with the attacker Command and Control. Once in place, the C&C is open for business. Using the tunnel, adversaries can download additional malware and send customized attack vectors to exploit vulnerabilities. Commands can be sent to infect other machines, creating a network of infected machines, or botnet armies, ready to do the C&C's bidding. It's truly a gift that keeps on giving.

Depending on the permissions attackers manage to obtain, they can do serious damage like exfiltrating data, shutting down infected machines or even entire networks, downloading malware to encrypt data, and, to make matters worse, renting out your infected botnet armies to other criminals on the dark web.

Simply put, backdoors are dangerous, which makes the next set of statistics even more relevant. We identified over 14 billion backdoor malware events within our customers' IT environments. We also blocked approximately 6 billion connection attempts made by infected machines to malware drop sites, potentially preventing additional malware or commands from adversary C&Cs from reaching customer networks.

One of the key strengths of backdoor malware is obfuscation. Once installed, it's hard to detect and disable. Comcast Business's DNS security solution, SecurityEdge™, played a key role in detecting and blocking millions of threats during 2022, helping to stop the spread by disconnecting malware from adversary Command & Control servers.

Figure 6: Noteworthy malware downloads prevented by Comcast Business SecurityEdge™ in 2022

Malware	Description
MSIL/Bladabindi	Bladabindi is a backdoor Windows malware package that steals passwords, logs keystrokes, takes screenshots, executes arbitrary commands, and can download and install additional malware. Adversaries usually bundle and deliver Bladabindi along with Windows VPN updates.
W32/Simda	Like Bladabindi, Simda belongs to a family of backdoor, password-stealing trojans.
Bedep	Downloaded from websites using Adobe Flash, Bedep is a trojan that opens a backdoor on a compromised system, provides a malicious actor with complete control over the system, and downloads additional malware.
Qsnatch	Tailored to attack QNAP storage hardware.
Agent Tesla	Used heavily during the pandemic in COVID-19 PPE-themed phishing campaigns.

A wide vulnerability landscape

Last year, the National Vulnerability Database (NVD) added 26,448 new application and infrastructure-related vulnerabilities, 59% of which were classified as "critical". This brought the total vulnerabilities count to 198,305[7], according to the Common Vulnerabilities and Exposures (CVE) system.

Our customers were no strangers to vulnerability exploit attempts. We stopped more than 450 million vulnerability exploit attempts in 2022, covering about 900 unique categories that spanned web and software applications, as well as hardware infrastructure[8]. Clearly, exploited vulnerabilities remain a critical ongoing challenge for businesses, both within their networks and at the perimeter.

Pre-packaged exploit kits and services sold on the dark web allow even unskilled adversaries to exploit targeted software vulnerabilities in client applications and browsers to execute code remotely. Our data show the problem is rampant.

In 2022 alone, National Vulnerability Database added:

26.4K
New application & infrastructure-related vulnerablities

59%
of vulnerabilities classified as critical

7. cvedetails.com
8. Comcast Business blocked 451,655,953 vulnerability exploit attempts during 2022.

Figure 7: The top 10 attempted vulnerability exploits stopped by Comcast Business in 2022

CVE CLASSIFICATION	CVSS 3 SCORE	ACCESS COMPLEXITY	DESCRIPTION
CVE-2020-8620 ASSERTION FAILURE	7.5	LOW	An unauthenticated attacker can establish a TCP connection with the server and send data on that connection to trigger assertion failure, causing denial of services (DoS). There is partial risk to service availability.
CVE-2021-44228 Log4jShell	10	LOW	Allows adversaries to use a single malicious code injection into the open-source logging framework. Complete information disclosure, availability impact, and complete integrity impact.
CVE-2022-21893 RDP CODE EXECUTION	8.8	MEDIUM	Allows unprivileged user connection to malicious RDP servers via remote desktop. Complete information disclosure, availability impact, and complete integrity impact.
CVE-2014-0994 EMBARCADERO BUFFER OVERFLOW	6.8*	LOW	Allows users to generate a buffer overflow in the VCL library of Embarcadero Delphi, to trigger a DoS, and potentially execute code. Considerable information disclosure.
CVE-2021-42278 MICROSOFT BRUTE FORCE LOGON	8.8	LOW	Allows adversaries to attempt authentication with many different passwords for different accounts. Considerable information disclosure.
CVE-2022-26809 MICROSOFT RPC RUNTIME CODE EXECUTIONS	9.8	LOW	A remote adversary can pass specially crafted inputs to the application and execute arbitrary code on the target system. Risk of complete information disclosure.
CVE-2017-9841 Util/PHP/ eval-stdin.php	9.8	LOW	Allows remote attackers to execute arbitrary PHP code via HTTP POST. Considerable information disclosure risk.
CVE-2020-14882 ORACLE WEBLOGIC RECE	9.8	LOW	Easily exploitable vulnerability which allows unauthenticated adversaries with network access via HTTP to compromise Oracle WebLogic Server. Complete information disclosure, availability impact, and complete integrity impact.
CVE-2020-25078 D-Link DCS-2530	7.5	LOW	The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure. Considerable information disclosure.
CVE-2018-6892 CLOUDME SYNC BUFFER OVERFLOW	9.8	LOW	Allows an unauthenticated remote attacker to connect to the “CloudMe Sync” client application listening on port 8888 and send a malicious payload causing a buffer overflow condition. There is significant information disclosure risk and partial risk to performance.

* CVSS2.0

Source: cve.org

Ongoing Apache Log4j™ Exploits

Emerging as a zero-day vulnerability in 2021, Log4j exploits have become endemic. We stopped almost 105 million Log4j exploit attempts during 2022[9]. Even a year after Log4j first appeared in the wild and upended the cybersecurity world, it remains a significant risk. Research shows that three out of five organizations so far have experienced Log4j exploit attempts.[10]

Following Log4j exploits, we saw attempts at backdoor malware installation, system credential and data theft, and dropped crypto miners, among other malicious results. Our data suggests that many of the 14 billion backdoor malware attempts we blocked were the result of post-Log4j exploits.

Why is Log4j exploitable?

It's prevalent because it's widely deployed across millions of java applications, making a staggering 72% of organizations vulnerable to exploits. It remains successful because as of Oct 2022, only 28% of vulnerable organizations have remediated or patched susceptible applications. And it's persistent because despite doing the right thing, many organizations that remediated their systems reintroduced Log4j again as new systems[11] were introduced to their environment.

Which brings us to an age-old question asked by exhausted and sleep deprived IT teams worldwide: "Why is patching so important?"

Why is patching so important?

Eighty-five percent of all vulnerability exploits involve unpatched software[12], and 71% of vulnerabilities identified before 2017 are still being exploited[13]. Wouldn't patching vulnerable systems solve the problem? The answer is yes, but it's not that simple.

Patch management—including people, processes, and technology—is the elephant in the cybersecurity room. It's not uncommon for large enterprises to have over 100,000 unpatched systems at any point in time. In our experience, it's even more common for small businesses to be at significant risk due to lack of maturity around organized vulnerability and patch management programs.

9. Comcast blocked 104,588,781 Log4j exploit attempts during 2022.
10. Neustar International Security Council
11. Tenable® Telemetry Study of Log4j
12. Cisa.gov
13. Checkpoint

So why is patch management so challenging when Windows and Mac OS updates occur automatically, and SaaS applications don't require users to implement version control?

Well, it's complicated.

First, scanning programs or technologies are essential to identify and remediate newly discovered vulnerabilities, but very few SMBs have this capability in-house. Worse, most small businesses don't have High Availability (H/A) configurations and can't risk taking down the only 'service' they have.

Second, patches can break existing functionality or introduce more bugs in applications, like in the Log4j example above.

Third, IT departments are overwhelmed with patches from multiple vendors and often need months to validate a patch before deploying it to all endpoints.

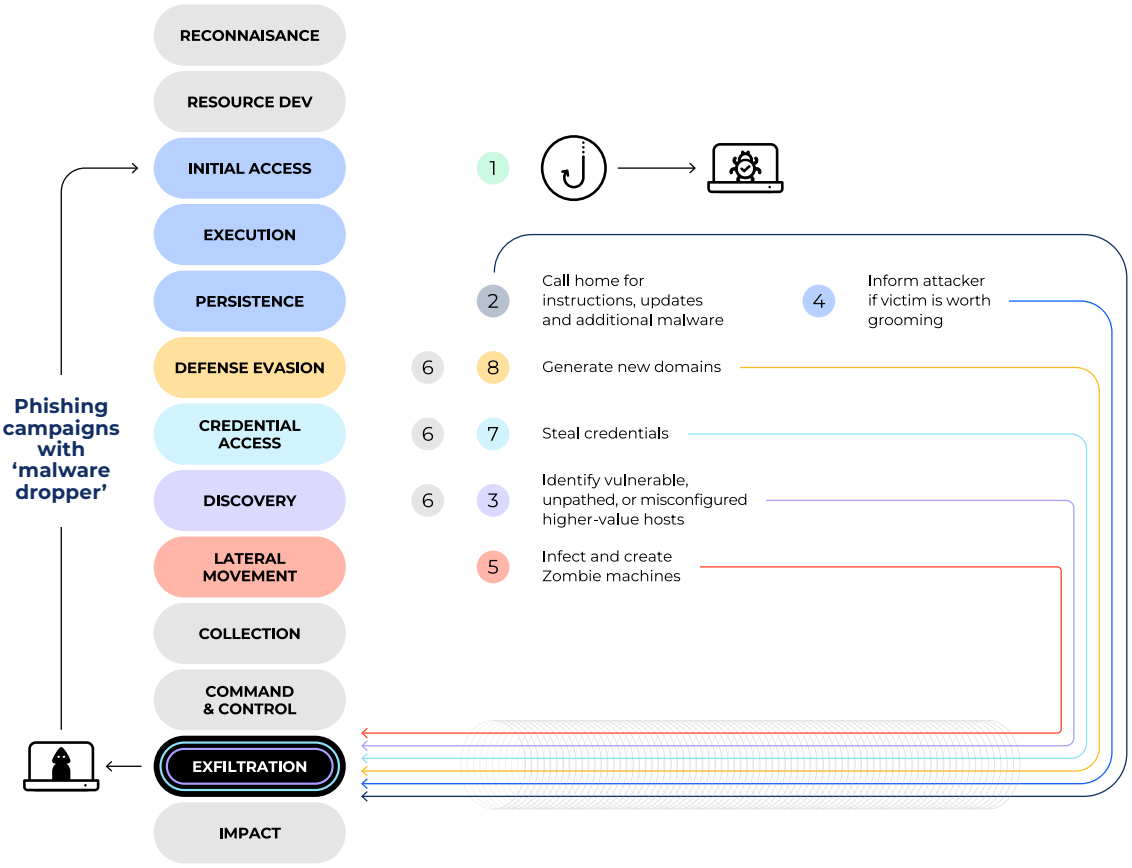
And fourth, tech stack complexities turn everything upside down. End users don't know enough about the applications, like code libraries and extensions, let alone how to patch them. For businesses to know what to patch and when to patch it, vendors must do better to publicize all the connections and dependencies on the supply chain.

Not discounting the complexities of patch management, it is still the only way to really protect your organization from falling victim to known vulnerability exploits.

Figure 8: Access isn't the end goal. Adversaries may have a series of objectives once initial access to target systems or networks is achieved.

Adversary Goals

1. Infect low-level host with malware droppers
2. Open pipe for getting instructions and sending stolen files, discoveries, etc.
3. Identify higher-value targets like a file server or domain controller to the attacker.
4. Inform attacker if further attacks are worthwhile.
5. Create infected Zombie bots for hijacking later.
6. Download additional malware based on Attacker instructions.
7. Send back stolen information – credentials, files, customer data.
8. Generate new Domains to avoid detection while within victim perimeter.



How adversaries evade detection

Privilege, persistence, and blending in

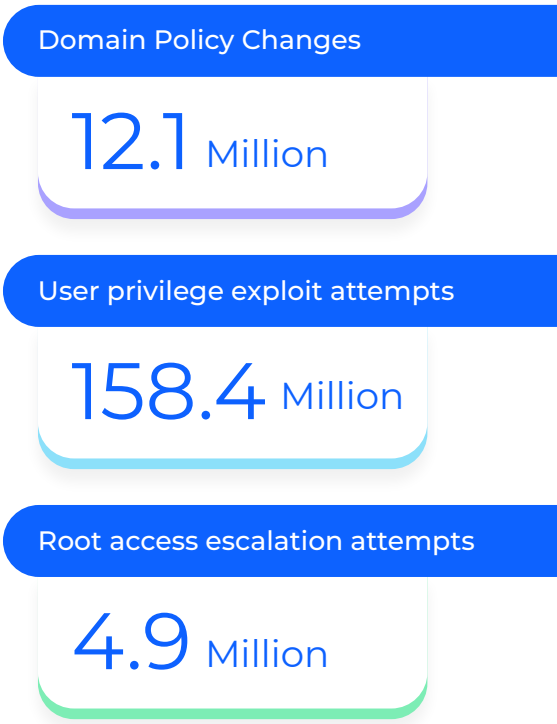
Adversaries don't go to all the trouble of breaching your networks without a plan to remain inside. At a minimum, they install malware to scan for exploitable vulnerabilities and then decide whether you are worth further effort. The ability to remain hidden increases a target's value.

We detected 26,663,491 attempts to 'blend in' via a variety of evasion tactics across our customers' networks. Our logs show these failed evasion tactics by adversaries as attempts to modify, create, and delete accounts, directory objects, and security groups. Many of these attempts followed the exploits listed in the vulnerability section above.

The privilege and persistence activities did not stop there. Adversaries tried to leverage escalated network administrator permissions 2,648,328 times to modify or create new firewall rules to establish external communications for C&C and data exfiltration.

In total, we identified 222,768,273 attempts to elevate permissions within our customer networks by exploiting vulnerabilities, modifying domain policies, local group enumeration, and through the use of admin-level privileges. Nearly 5 million attempts were made to gain root access on other systems via newly acquired superuser-level resources.

Figure 9: Privilege and persistent activities observed in 2022



Diving deeper into credential access

For an adversary, legitimate credentials offer access to a landscape littered with exploitable vulnerabilities inside the perimeter. The credential-stealing malware we discussed earlier contributed to 159 million attempts to steal and then use stolen credentials to access and expand within our customers' networks.

Two billion credentials and PII records were stolen worldwide last year, which reinforces the importance of protecting credentials.[14] Businesses should focus on locking down their identity management systems and processes, integrating them with human resource systems, and especially, implementing multi-factor authentication and zero-trust solutions to better thwart attackers who try to leverage stolen credentials.

Attempts to steal and use credentials detected by Comcast Business in 2022

159.8 M
credential theft attempts

3.5 M
brute force attempts

14. Cyber Security Hub

Discovery & lateral movement

Once an adversary has gained access to a network, their focus shifts to expanding their presence, identifying vulnerabilities in internal servers and workstations, and capitalizing on them.

The more information an adversary can gather, the better their chances are of increasing attack impact. Discovery, much like the reconnaissance stage, allows adversaries to gain a detailed understanding of the network, uncover where the crown jewels are located, and develop an attack strategy to get there. Compromised networks within our customer base experienced 404,775 directory and path traversal activities, some of which were followed by lateral movement activities to spread out and execute plans that access and exploit corporate assets.

The bigger the network, the more chances for the adversary to find misconfigured systems and vulnerable nodes. Lateral movement is largely dependent on authenticated malicious users executing code on vulnerable systems found after they establish initial access.

Adversaries made over 155 million attempts to move laterally across our customers' networks. Remote services were used 51 million times to gain access to vulnerable systems. Coupled with 42 million Remote Code execution attempts and privilege escalation, adversaries have a good chance of expanding from a single compromised PC across other targets within the local network. We also saw more than 104 million arbitrary command execution attempts made to hide the launch of remote admin services and various exploit attempts against SQL and SMB vulnerabilities to move laterally through customer networks.

We detected and contained 188,118 attempted exploits of domain controllers, which if successful, would grant adversaries with persistent access to other users and systems within a network.

Fileless Malware

Some of the lateral moves were accomplished with the help of approximately 4 million "fileless" malware techniques that Comcast Business was able to detect, disrupt, and contain.[15] Fileless malware is particularly dangerous because it uses legitimate, everyday tools to do the dirty work, in particular the Windows PowerShell command line interface and Windows Management Interface (WMI).

4M
'Fileless' malware techniques

15. During 2022, Comcast Business detected and stopped 3,921,515 "fileless" malware attacks.

Command and Control

Once adversaries land, they establish communications with Command and Control servers to direct the attack remotely. Comcast Business blocked 14 billion remote C&C connection attempts from malware and botnets in 2022.

Adversaries often equip backdoor malware with Domain Generation Algorithm (DGA) capabilities. DGA makes detection of C&C connections more difficult by periodically changing the destination's domain address. In addition, we observed malware keeping an irregular communication cadence with C&C, helping to evade detection by firewalls and other network security tools that inspect outbound perimeter traffic for risky domains.

How hackers remain hidden

There are few scenarios where an adversary wants to drop in and drop right back out. At a minimum, they install malware or scan for exploitable vulnerabilities to decide whether it is worth further effort.

Adversaries try to evade detection and remain hidden following initial access. It's not easy, especially when threat hunters continually look for evidence and Indicators of Compromise (IOCs), but there are some techniques, like DGA, that attackers are increasingly turning toward. Techniques vary but here are some of the more popular ones we observed last year:

Domain Generation Algorithms

We discussed tunneling earlier in the report. It's the pipeline that backdoor malware establishes for attacker C&C communication, data and credential exfiltration, and malware downloads. To ensure the backdoor malware is not detected, adversaries often arm the malware with DGA capabilities.

Attackers create DGA algorithms to randomly generate large amounts of domain names daily to hide their true IP address. Botnets employ FastFlux DNS to hide behind an ever-changing network of compromised hosts acting as proxies. Malware armed with DGA capabilities were detected and blocked over 821 million times by Comcast Business before they could cause significant impact.[16]

16. Comcast Business stopped 821,153,436 outbound connections in 2022 caused by FastFlux DNS. See here.

07.

Examining potential impact

The exfiltration and impact stages of a breach are where the rubber meets the road for an attacker. The MITRE ATT&CK© framework defines "Impact" as a collection of techniques used by adversaries to disrupt availability or compromise integrity by manipulating business and operational processes.[17] This ranges from denial of service to hijacking resources to data encryption or data destruction.

During 2022, Comcast Business prevented over 10 billion exfiltration and impact attack events including data destruction, encryption, and DDoS attacks.

Exfiltration

Data stored on devices and servers is what most adversaries are after. We observed over 143 million later-stage events designed to steal critical and sensitive information. In particular, we stopped 89,667 attempts to exfiltrate Personal Identifiable Information (PII) and Payment Card Industry (PCI) credit card data.

Holding data as hostage

It's hard to say which malicious activity has the greatest impact on your business, but data encryption and data destruction are high on the pain threshold. 521,071,208 attempts to install malware or worms known to encrypt data, specifically for ransomware attacks, were detected and blocked in 2022. 807,222 attempts to destroy data were also blocked. Eleven different types of malwares were identified, of which the necurs botnet (known to install locky ransomware) and Sodinokibi/REvil malware (known to target Windows systems) were most prolific.

The most notable ransomware we observed was of the "fileless" category. Based on our analysis of customer logs, we believe these were delivered as the final deployment in the attack by the Get2 loader malware. Get2 facilitates the download of different malicious tools like COBALT STRIKE, FlawedAmmyy, and SD BOT, all three of which we saw in our logs. These tools enable adversaries to conduct reconnaissance and move laterally within your networks. Once the adversary is ready for the final blow, Get2 delivers the fileless ransomware malware.

Denial of Service

Denial of service attacks were used over 210 million times in an attempt to hurt business operations by shutting down critical database servers and network resources. The impact varied across organizations, depending on the services affected, but all DoS attacks can cost businesses precious time and resources. To compound the impact, DoS attacks also often affect external-facing infrastructure like websites, leading to lapses in customer experience and sharp upticks in customer support issues, as well as an erosion of trust.

+210 M

Denial of service attacks

Service Stop

Another method of disruption and impact is the disabling or stopping of high importance individual services. Similar to DoS, this tactic is often used to encrypt, steal, or destroy data.

17. MITRE ATT&CK© Framework

Resource hijacking

Crypto Mining

Resource hijacking is a favorite tactic, particularly when it comes to using machines to mine cryptocurrency. Unlike ransomware, the adversary's goal is not destruction, but leveraging resources for profit, most often for cryptocurrency validation. We identified 242,649,194 crypto mining-related botnet activities in our customer logs. That may not be a large number when you think about resources at enterprise scale organizations, but for small to medium-sized organizations, hijacking just a few resources can completely derail operations.

243M

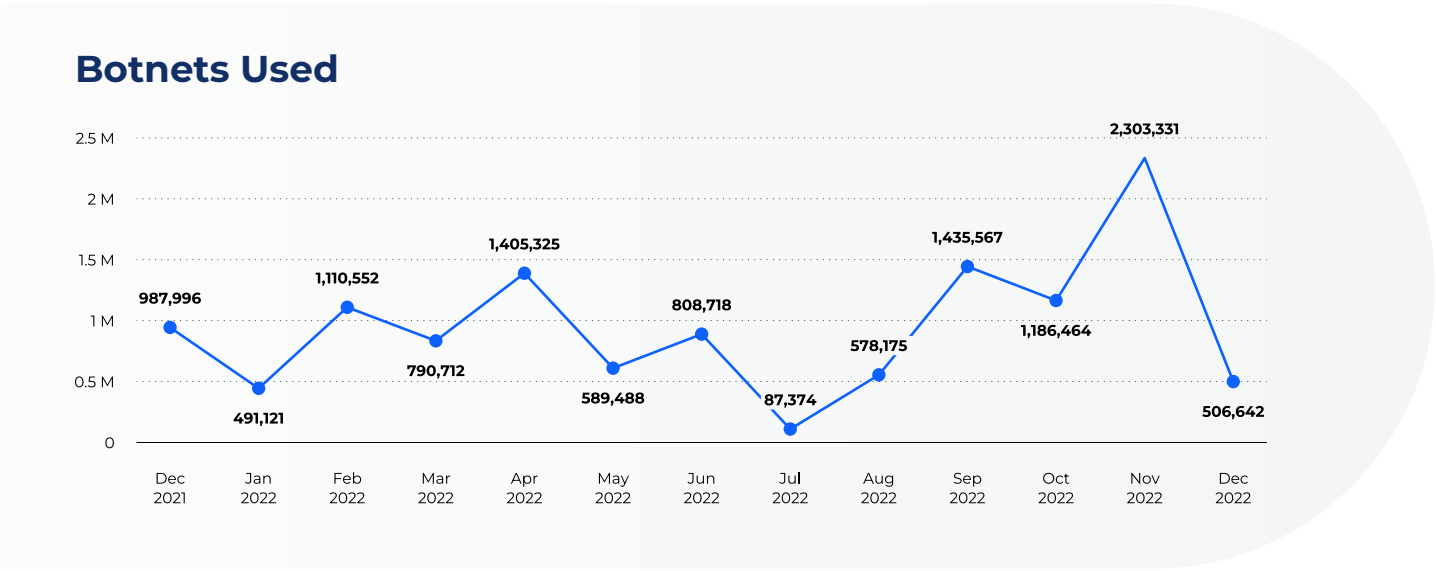
Crypto mining-related botnet activities identified in Comcast Business customer logs

Hijacking botnets to attack targets

Resource hijacking takes another turn when used to conduct Distributed Denial of Service (DDoS) attacks. DDoS attacks leverage rented or commandeered botnets from the dark web marketplaces to overload and disrupt critical systems and services at another target organization. These are the same botnets created during earlier breaches by other adversaries and monetized through the dark web. If the backdoor stays open, the armies of "zombie" resources can be controlled remotely by the attacker's C&C.

2022 was the first year we started tracking botnet activity in DDoS attacks against our customers. Over 12 million hijacked botnets combined with private resources were used to conduct these attacks. This is not a huge number of botnets but their worldwide distribution and the fact that a lot originate from private networks (hidden IP addresses) make them hard to identify, locate, and block. Their pervasiveness points to an overwhelming need to focus on prevention: it's much harder to get them out after they get in.

Figure 10: Botnet involvement in DDoS attacks detected by Comcast Business in 2022



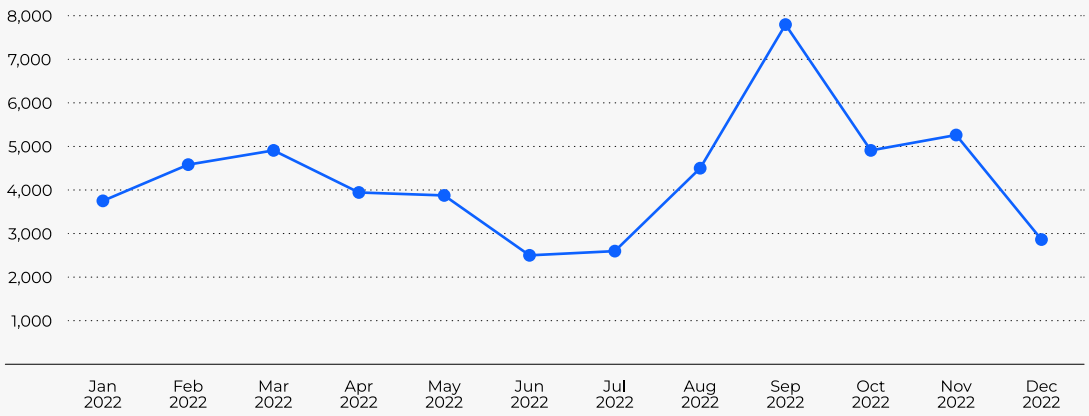
Hijacking resources to attack other organizations

Comcast Business stopped over 9 billion attempted queries to find and weaponize machines within our customer base for DNS amplification campaigns against other targets. These queries came from domains known to launch DNS amplification and DDoS attacks using hijacked resources from a network of vulnerable companies.

DDoS attacks & mitigations

The year 2022 saw a slight decline in worldwide DDoS attacks. That doesn't mean, however, that they aren't still a major concern for nearly every type of business. We've observed evolving ebbs and flows in DDoS activities, with greater concentration occurring in certain industries. In 2022, Comcast Business detected a total of 51,915 DDoS attacks.

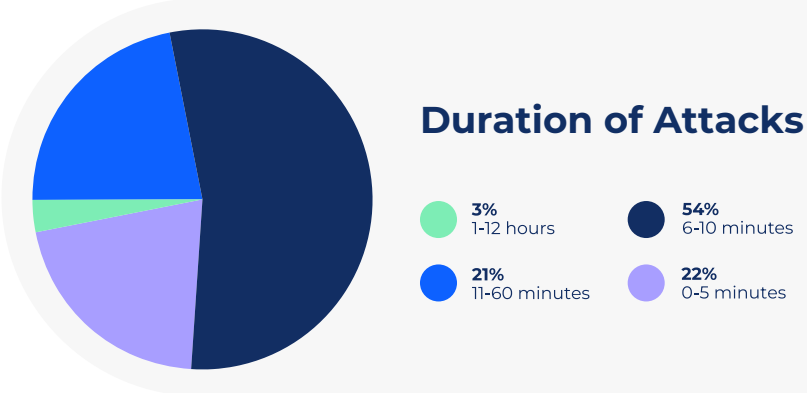
Figure 11: Number of DDoS attacks detected by Comcast Business per month in 2022



Short-burst attacks dominate

Once again, the bulk of the attacks were under ten minutes long. The trend of short-burst attacks has continued since the prior year. Short-burst attacks are harder to detect, especially if organizations try using firewall rate-limiting policies to stop them, rather than carrier-grade services. Multiple short-duration attacks exhaust IT resources because the next one starts before the organization can deal with the last one. While IT remains in an endless loop of dealing with multiple attacks, adversaries can use the distraction as a smokescreen to execute more insidious attacks elsewhere.

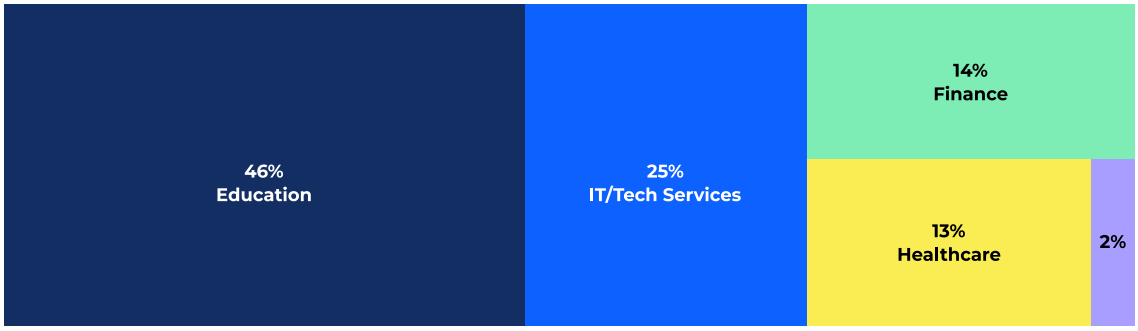
Figure 12: Duration of DDoS attacks among Comcast Business customers in 2022



Attacks by industry

Education is a significant target area for DDoS attacks, while IT and Technical Services market segments also saw jumps in DDoS attempts, replacing Government in our top four sectors attacked in 2022. One other notable sector targeted by DDoS attacks more recently is healthcare, prompting the U.S. government to issue a special advisory notice in early 2023.

Figure 13: DDoS attacks by industry segment detected by Comcast Business in 2022



Threat vectors and attack volume

Adversaries did not change their tactics much during 2022. Most attacks still used low-complexity, high-impact flooding techniques. This is validated by NetScout's review of all 9.4 million DDoS attacks they tracked last year, which identified total traffic, UDP, and TCP Sync as the top three vectors used.[18]

Multi-vector attacks take DDoS to the next level, allowing adversaries to create more sophisticated attacks. Their usage is on the rise. However, they require expertise to pull off, which is why we believe the tried-and-true techniques still dominate.

31% of Comcast Business detected attacks in 2022 were multi-vector attacks. 82% of all multi-vectors contained DNS amplification vectors.

As expected, malicious volumetric traffic was successfully used to flood networks and remained the most popular method of attack we observed in 2022.

Total traffic accounted for 85% of DDoS attacks, and while amplification attacks continued to play a role, they represented a much smaller percentage of attack traffic.

Figure 14: Vectors used in DDoS attacks detected by Comcast Business in 2022

Vectors Responsible for Generating DDos Traffic

18. Netscout DDoS Attack Map

09.

Best practices for reducing cyber risks

So, what steps should organizations take to combat the threats and major trends seen last year? Understanding trends around past security and data breaches is critical to knowing how to avoid becoming a future victim. But knowing about the threats is only half the battle.

Technology teams today are best served through a comprehensive suite of powerful security solutions orchestrated to provide multiple layers of security, as well as managed security services provided by a trusted partner to augment or extend in-house capabilities. Such solutions and approaches are not only designed to keep adversaries out, but are equally important to hunt down and disrupt them when they do breach your perimeter.

No organization is perfect, but everyone needs a strategy and a roadmap. Many organizations have discrete security controls in place that leave substantial gaps and residual risks. In the same way attackers use multiple vectors to breach security controls, defenders need to take a "defense-in-depth" approach to mitigate risk. Here are some key guidelines on how best to prepare both for security and data breaches and where to focus resources on closing the gaps to improve your organization's security posture.

Key Areas of Cyber Risk Mitigation

1. PHISHING	Address phishing risks through mandatory security awareness training and an email gateway service that inspects every email for risky attachments and URLs.
2. CREDENTIALS	Require users to authenticate to all resources via a centralized Identity Broker with multi-factor authentication. Centralize directory management across the organization and create processes that tie directory listings to your human resources department. Audit Domain & Privileged Accounts.
3. ZERO-TRUST ACCESS	Implement Zero-Trust policies that block access to network, host, and application resources without proper authentication, especially for critical infrastructure and crown-jewel data.
4. PRIVILEGED ACCESS	Create a secure vault for managing and storing credentials used to access critical systems like jump servers. Store certificate private keys in a Hardware Security Module (HSM).

5. REMOTE ACCESS	Implement identity-based certificate access with MFA for your perimeter assets such as domain controllers, VPN controllers, publicly exposed Remote Desktop Protocol (RDP), and remote desktop management systems (e.g., LogMeIn).
6. DATA	Create a schedule for both full and incremental data backups using immutable storage that even administrators can't modify. Secure and encrypt the backup solution.
7. VULNERABILITIES	Conduct regular vulnerability scanning. Update and patch all software as soon as practical for your organization. Correlate known high-risk vulnerabilities against exploit attempts to prioritize patch management. Track open source and third-party software libraries in your patch management plans. Conduct periodic penetration testing.
8. CONFIGURATION	Lock down your server and desktops with a standard "gold image" configuration to reduce the attack surface. Push updates using a centralized configuration and patch management.
9. ENDPOINT SECURITY	Implement Endpoint Detection & Response. Traditional antivirus systems have improved, but any system that depends on scanning installed files is more likely to miss risky processes and fileless malware.
10. SEGMENTATION	Segment the network to minimize the potential blast radius reachable by an adversary, for example by creating separate IP addressing between front and back-office transaction processing systems or crown jewel databases.
11. NETWORK SECURITY	Deploy UTM firewall inspection at the network perimeter and across every network segment to help stop lateral movement. Implement DNS Security to help stop DGAs and prevent compromised users and hosts from reaching malicious domains and IP addresses.
12. MONITOR, DETECT & RESPOND	Monitor security events and risky behaviors throughout your environment. Consider a Managed Detection & Response (MDR) service to outsource security event detection, incident response, and threat hunting. Inventory security log sources and consolidate to a central location for monitoring.
13. INCIDENT RESPONSE	Develop an incident response plan to prepare for a data breach, including steps to restore systems, data, and business processes. Get everyone involved including senior organization leadership, legal counsel, and key business functions, not just the IT team. Document it on paper and hold annual desktop rehearsals and training.

How Comcast Business can help

COMCAST BUSINESS

Comcast Business offers an expanded suite of cybersecurity solutions to help guard businesses against fast-changing and malicious attacks. Comcast Business cybersecurity products and services include managed firewall services, secure remote access, DDoS mitigation, managed endpoint detection and response, vulnerability scanning and exposure management, managed detection and response, and more.

Learn more about our advanced cybersecurity solutions.

Learn more