2022 Threat Intelligence Report

CYBERFORCE

EXECUTIVE SUMMARY

In this report, we present summary observations from our Collective Security Operations Center (SOC) during 2022. One of the core tenets is that we are stronger together and our efforts should protect our individual organizations and the broader community too. This report is shared with the intent that it will educate, inform, and help improve your cybersecurity program in 2023 and beyond. It's also shared with gratitude for each SOC participant and their contributions of information, analysis, tactics, and automations. Near the end of every year the SOC participants convene for a workshop. The insights derived from information shared, similar to what is contained in this report, inform our innovation calendar for the next year. We then work together daily to accelerate and advance our collective capabilities. Quite simply put – in a world where cybersecurity professions often have way too much on their plates, this is one way to get more done and get it done faster. Please enjoy this report and if you would like to explore becoming part of our Collective Force for Good in the Cyber Realm give us a call.

The escalation of global conflict and cyber-crime has made businesses and security teams more vigilant. As a result, business executives have come to view cybersecurity as a business issue, rather than just a technical one, and have taken steps to address the risks accordingly. We are dedicated to protecting critical infrastructure organizations from a range of threats. This commitment is more important than ever in light of the recent increase in global conflict and cyber-crime. During 2022, we welcomed multiple new organizations, many of which are major players in their respective SMB industry verticals.

One of the most significant events of 2022 was the outbreak of the Russia-Ukraine war, which quickly escalated into a cyber conflict with widespread consequences. This isolated conflict soon gave rise to a surge in cyber-attacks targeting organizations outside of Eastern Europe, with critical infrastructure being particularly vulnerable. Threat actors recognized the potential for causing widespread disruption by targeting critical infrastructure, and subsequently developed and deployed malware for this purpose. These attacks were often successful in achieving the attackers' goals, leading to significant disruptions in services. Threat actors are also increasingly aware of enterprise cyber defense capabilities and are using new techniques to evade detection.

In addition to regularly updating our clients on internal developments, we also believe in the importance of sharing insights. Information sharing can also help to build a more comprehensive and accurate picture of the threat landscape, which can inform the development of more effective cyber security strategies and policies.

TLP: Clear - Unlimited disclosure, this information can be shared publicly with everyone.

TABLE OF CONTENTS

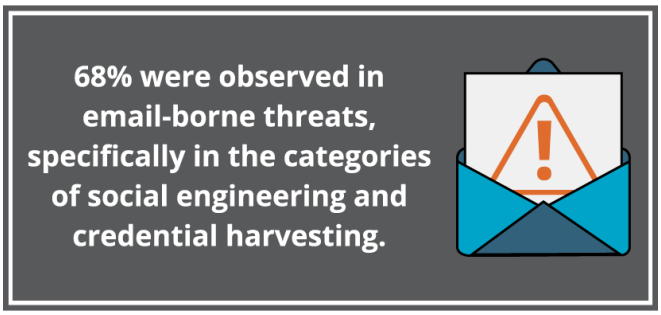
STATISTICS/TRENDS

INDICATOR OF COMPROMISE (IOC) TYPE BREAKDOWN

Indicators of Compromise (IOCs) are forensic evidence of potential intrusions on a host system or network, such as IP addresses, email addresses, domain names, and file hash values. They allow cybersecurity professionals and system administrators to detect intrusion attempts or other malicious activities and can provide actionable threat intelligence to improve incident response and remediation strategies.

Our automation of the collection and dissemination processes through workflow platform integrations allows us to share this information more granularly with our clients daily. This quick turnover is valuable because it keeps everyone informed of emerging trends with tactical intelligence.

Throughout 2022, we gathered IOCs from a range of attack types. Among these, 68% were observed in email-borne threats, specifically in the categories of social engineering and credential harvesting. Figure 1 presents a comprehensive breakdown of the top attack types that we gathered IOCs for.



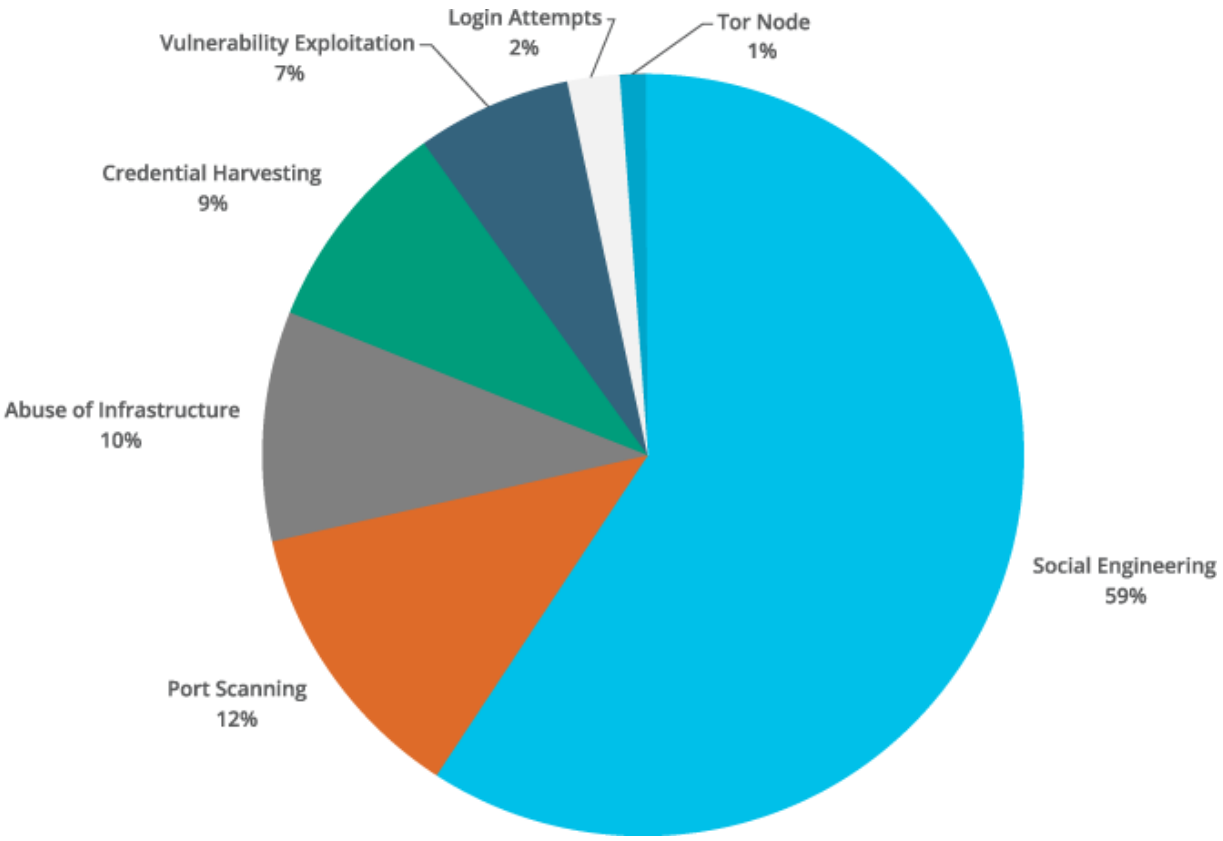


Figure 1: *A breakdown of the top attack types that we gathered IOCs for in 2022.*

- **Social Engineering (59%)** is a type of psychological manipulation that is used to influence or deceive individuals into divulging sensitive information or performing certain actions, such as revealing login credentials, financial information, or other sensitive data. Social engineering attacks can take many forms, including phishing emails, phone calls, or in-person interactions. The threat actor may use various tactics to persuade the target user, such as creating a sense of urgency, posing as a trusted authority figure, or exploiting the victim's emotions or trust.

- **Port Scanning (12%)** is the process of attempting to connect to various ports on a device or network to determine which ones are open and available for communication. Port scanning is often used by threat actors to identify vulnerabilities in a system or to gather information about the system or network. It can also be used by security professionals to assess the security of a system or network.

- **Abuse of Infrastructure (10%)** refers to the use of a network or system in a manner that is not in accordance with its intended purpose or that infringes on the rights of others. This can take many forms, but generally includes any activity that is intended to harm or exploit a network or system, or that utilizes the resources of the network or system in a way that is not authorized or that causes harm to other users.

- **Credential Harvesting (9%)** is an attempt trick a user into revealing sensitive information, such as login credentials or financial information. This is usually done by sending the user a link to a fake website that appears to be from a legitimate source, such as a bank or online service, and asking the user to enter their login information or other personal details.

- **Vulnerability Exploitation (7%)** is the process of taking advantage of a weakness or flaw in a computer system or network to gain unauthorized access or perform malicious actions. Vulnerabilities can exist in software, hardware, or even organizational processes, and can be exploited by threat actors to gain access to systems, steal data, or disrupt operations. To exploit a vulnerability, a threat actor typically needs to have some level of knowledge about the weakness and how it can be exploited. This may involve using specialized tools or techniques to identify and exploit the vulnerability. In general, the goal of vulnerability exploitation is to compromise the security of a system or network in some way, either for personal gain or to cause harm.

- **Login Attempts (2%)** refers to the act of trying to gain access to a user's account by repeatedly entering different passwords in an attempt to "guess" the correct one, potentially without the authorized user's permission. This process is often referred to as "brute forcing" the password.

- **Tor Node (1%)** is a server that is part of the Tor network, a decentralized network of servers that is designed to enable anonymous communication and browsing on the internet. Tor nodes can be a concern for organizations because they can be used to bypass network security measures and access restricted resources. Since traffic is encrypted and bounces through multiple nodes before reaching its destination, it can be difficult for organizations to monitor and block.

TOP PHISHING DOMAINS

Phishing attacks can be a major risk for organizations and individuals. In the past, the perpetrators of these attacks often used malicious domains for their communication infrastructure, but these were easily detected and blocked by security measures. In response, phishers have become more sophisticated and now often use trusted domains, such as those belonging to Google, Apple, and Microsoft, to bypass email security defenses, as these domains are often implicitly permitted by organizations. This means that even if an organization has robust security tools in place, it is still important for employees to be vigilant and carefully evaluate each email they receive.

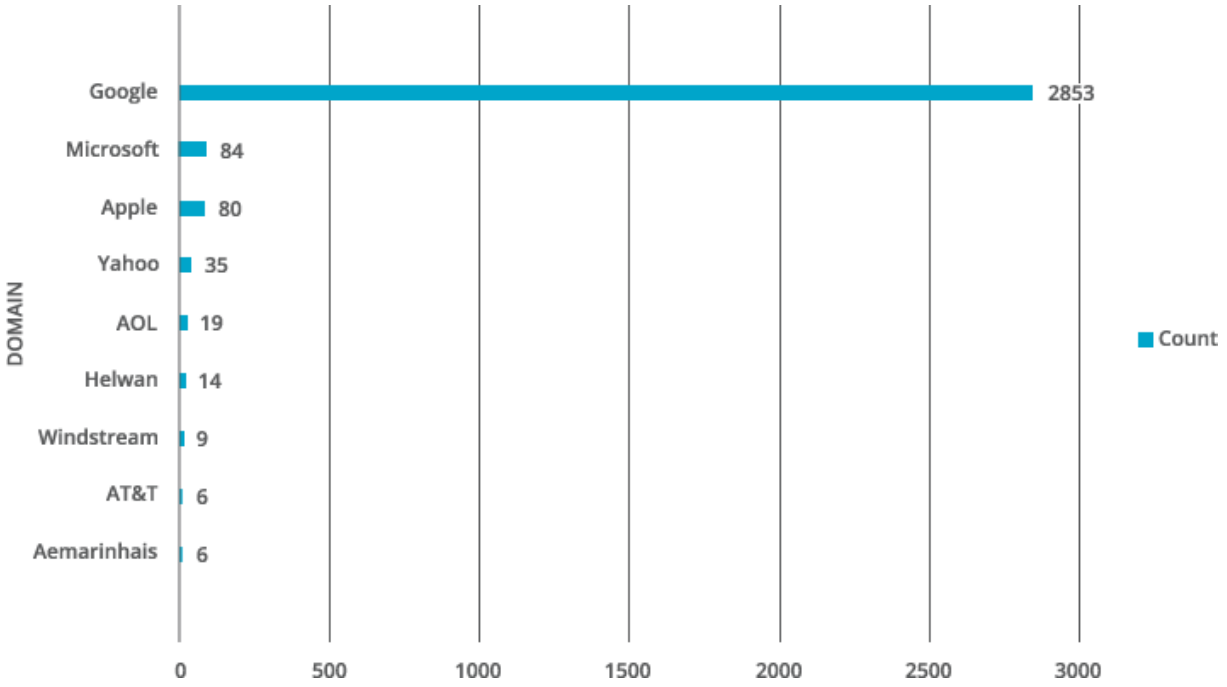


Figure 2: *Our top domains observed in 2022.*

There are a few concerns to consider. One concern is that these platforms are widely trusted, and phishing perpetrators can exploit this trust to their advantage. For instance, if a cybercriminal sends a phishing email from a Gmail account, the recipient may be more likely to trust the email and click on any links or attachments it contains. Even if the recipient is directed to a malicious website, the phishing email can still get through to them if the sender's address is hosted by a trusted service provider.

Moreover, trusted platforms are frequently abused in social engineering attacks, such as internal impersonation and spoofing. These attacks seek to deceive employees into thinking the message is being sent by an internal employee, in order to obtain sensitive information or commit fraud without using any links for a user to click on. This can be achieved by compromising an employee's account or exploiting an organization's vulnerable email security protocols.

Additionally, these platforms may have more advanced security measures in place to protect against spam and phishing attacks, making it harder for law enforcement or security professionals to track and identify the threat actors. This can make it more difficult to protect against and prevent future attacks.

So, what are a couple of steps organizations can take protect against modern phishing attempts?

Educate employees about phishing. It's important for employees to be aware of the tactics that today's phishers use and how to identify and report phishing emails. Conducting simulated phishing attacks can be a useful way to help employees understand how to recognize and respond to these types of attacks. Providing employees with examples of real phishing emails can also be helpful in understanding the tactics that are used and how to identify them.

Encourage employees to report any suspicious emails to the appropriate authority. By providing regular training and resources, organizations can effectively educate their employees about phishing and help protect their organization.

Implement DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework). DKIM works by adding a digital signature to an email message, which can be used to verify that the message was actually sent by the domain it claims to be from. When a recipient's mail server receives a message with a DKIM signature, it can use the signature to verify that the message was not modified during transit and that it was actually sent by the domain it claims to be from.

SPF works by allowing a domain owner to specify a list of servers that are authorized to send email on behalf of the domain. When a recipient's mail server receives an email from a domain with an SPF record, it can check the SPF record to see if the server that sent the email is on the list of authorized servers. If the server is not on the list, the email can be flagged as potentially suspicious.

Both DKIM and SPF can help protect against phishing attacks by making it more difficult for attackers to send malicious emails that appear to come from a legitimate domain. However, it's important to note that these measures are not foolproof, and organizations should also use other security measures.

GEOLOCATION ANALYSIS: PORT SCANNING ACTIVITY

As our second most detected threat category in 2022, port scanning is commonly used by threat actors to find vulnerabilities in an organization's online assets. These intrusive scans can consume resources and create "noise" that makes it harder to detect more serious threats. While port scanning is not a high-level threat, it is still important for security teams to monitor this activity and use firewalls to block it.

We conducted an analysis of port scanning activity directed at our client organizations over the past year, using Indicators of Compromise (IOC) data. We then created a heat map with colors to visualize the geographical locations from which these scans originated. While this analysis is not comprehensive as some clients did not provide IOC data, it allows us to gain insight into the scope of the activity and identify geographical patterns.

Understanding the geographical extent of this activity can help identify trends and potential sources. It may also help organizations identify which regions or countries they should be particularly vigilant in protecting against. Additionally, knowing the location of the source IP addresses of the port scans can assist in determining the motivations and goals of the threat actors, as well as inform decisions on resource allocation for threat prevention and response measures.

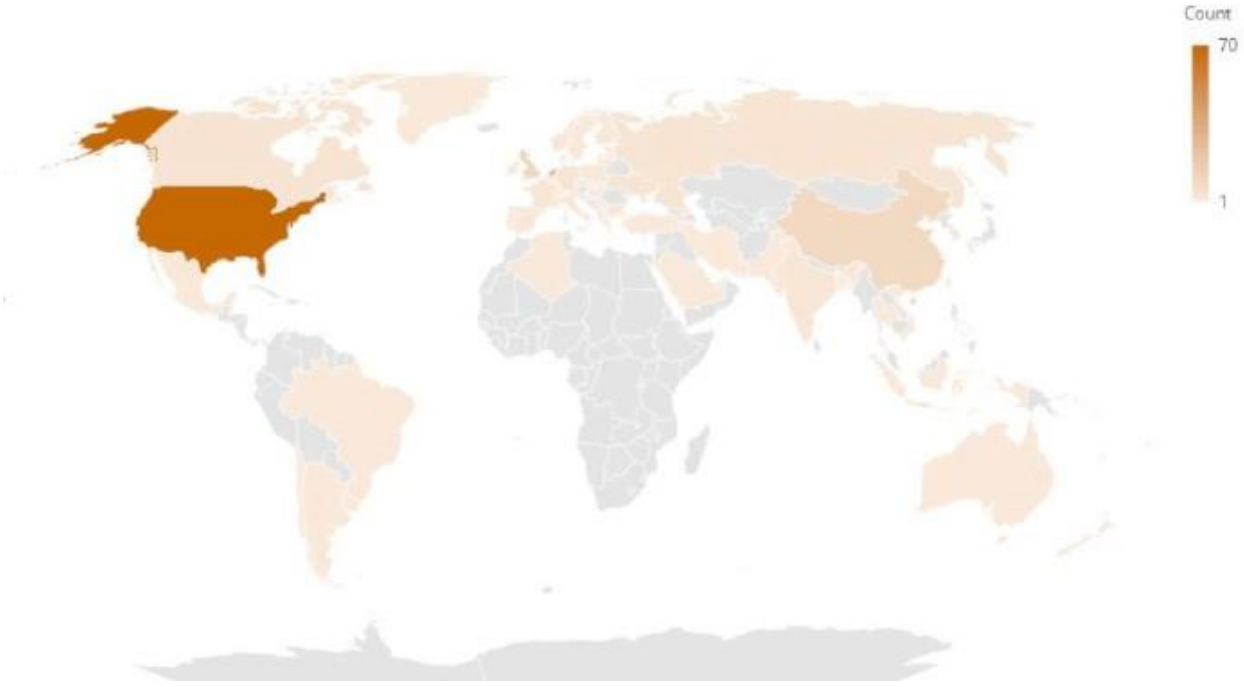


Figure 3: *A heat map displaying the geographic origins of all port scanning traffic in 2022 based on collected IOC data.*

Most of the traffic originated in the United States (22%), followed by the Netherlands (9%), United Kingdom (4%), and China (3%). Port scanning traffic can be a concern for organizations as it can indicate that threat actors are attempting to gather information about an organization's networks and systems for the purpose of launching a targeted attack or identifying open ports and services that can be exploited in a later attack. Port scanning can also be used to identify servers or devices that can be used in a Denial of Service (DoS) attack to disrupt service.

In general, it is important for organizations to monitor their networks for any unusual or suspicious activity, including port scanning traffic, and to have appropriate security measures in place to protect against potential threats.

Actionable steps to mitigate risk:

- Implement firewall rules that clearly define which types of network traffic are permitted and which are not. If feasible, consider using geo-blocking to further restrict access.
- Disable unnecessary services and protocols and utilize secure configurations for necessary servers and devices to enhance security.
- Network access control (NAC) systems can be used to enforce policies for accessing network resources and can help to prevent unauthorized devices or users from connecting to the network.

By implementing these and other security measures, organizations can significantly reduce their risk of being successfully targeted.

TOP DETECTION USE CASES

In today's digital landscape, where the number, speed, and sophistication of cyber threats are constantly increasing, security teams must be able to quickly identify and respond to threats or breaches while minimizing the impact of a security incident on the organization.

One way to achieve this is by strategic detection engineering. This is a process of designing and implementing systems and processes that can identify and alert security professionals to potential security threats or breaches. These systems and processes are designed to continuously monitor for signs of compromise or unusual activity and provide alerts when potential threats are detected. The goal of detection engineering is to create an automated system of threat detection that is customizable, flexible, repeatable, and produces high fidelity alerts for security teams to act upon. This approach is critical in helping organizations to protect their systems, data, and assets from cyber threats, and to minimize the impact of a security incident.

An effective asset management strategy involves maintaining a comprehensive inventory of all assets, continuously monitoring, and tracking those assets, and being able to quickly detect and respond to any potential unauthorized activity. By doing so, an organization can proactively identify and mitigate potential threats. This helps to minimize the potential impact of a security breach and protect the organization's assets and data.

Here are three examples of detection use cases that have been effective in our organizations, along with the tactic used by threat actors in each case:

ANOMALOUS LOGIN GEOLOCATION

TACTIC: INITIAL ACCESS

Threat actors may use compromised credentials to gain unauthorized access to systems and resources within a network. They may use these credentials to bypass security controls and gain initial access, maintain persistence, escalate privileges, or evade detection. Compromised credentials may also allow them to remotely access systems and services such as VPNs, Outlook Web Access, network devices, and remote desktop for prolonged periods of time.

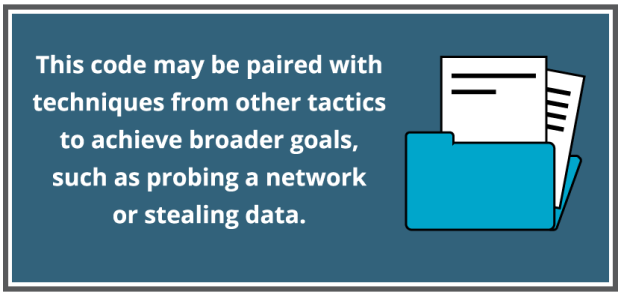
Unusual login times or locations can be useful indicators of potential security breaches, issues with account access or authentication processes, and inefficiencies in business operations. While it is possible for a user's login location to be disguised by means such as a compromised server, VPN, or proxy, geolocation detection can still be used to identify potentially suspicious login behavior.

Organizations should be aware of unusual login times or locations, as these can be indicators of potential security breaches or other issues. By monitoring for these types of anomalies and taking appropriate action when they are detected, organizations can help to identify and mitigate unauthorized access to systems and resources, protect against data loss and theft, and maintain the integrity and security of the organization's network.

SUSPICIOUS FILE OR PROCESS ACTIVITY ON A HOST

TACTIC: EXECUTION

Threat actors may use legitimate system tools and commands to blend in with regular system activity and evade detection. A user may inadvertently download a malicious file disguised as a legitimate program, which may then install and execute remote access scripts, backdoors, ransomware, spyware, or adware.



During the execution phase of an attack, the threat actor's code is attempting to run. This code may be paired with techniques from other tactics to achieve broader goals, such as probing a network or stealing data. It is important to detect this activity because identifying and blocking unauthorized access to one host may prevent the compromise of multiple systems.

Threat actors may use command and script interpreters such as PowerShell, the Unix or Windows command shell, to run commands, scripts, or binaries. To detect this activity, you can monitor command-line arguments for script execution and subsequent behavior. This may be related to network and system information discovery, collection, or other script-based post-compromise behaviors, and can serve as indicators of the source script. These scripts may have various effects on the system and may generate events, depending on the type of monitoring in place.

To detect malicious or suspicious files, you can use signature-based, behavioral-based, and/or heuristics-based detection. This involves using a database of known malicious software "signatures" to identify and block known threats, monitoring the behavior of programs, and flagging any suspicious activity, and using algorithms to identify patterns that are typical of malicious software. It's important to note that no single method is foolproof, and it's best to use a combination of these techniques to detect and protect against malicious software.

To ensure the security and welfare of the organization, measures must be implemented to protect the organization's assets such as data and systems. Endpoint monitoring plays a crucial role in this process as it helps identify and address today's security threats promptly, minimizing the likelihood of data breaches and other security incidents.

PRIVILEGED USER-CREATED USER ACCOUNTS

TACTIC: PERSISTENCE

Threat actors may leverage their access to a privileged user account, such as an administrator account, to create an additional account on a victim system to maintain access without the need to use remote access tools, which are often easily detected and flagged as suspicious. By using a secondary account, they can continue to have access to the system without drawing as much attention to their activities. This can also allow them to maintain access even if their primary method of access is discovered or blocked.

To detect this type of activity, you can monitor executed commands and arguments for actions related to account creation, such as net user or useradd, and newly executed processes associated with account creation, such as net.exe. You can also monitor newly created user accounts through account audits to identify suspicious accounts that may have been created by an unauthorized individual. Additionally, you can collect data on account creation using network logs or Windows Event ID 4720 (which is triggered when a user account is created on a Windows system and domain controller).

It is crucial for organizations to monitor this type of activity because it can indicate the presence of an unauthorized individual or group with malicious intent on their systems. If a threat actor is able to create a new account on a victim system, it can allow them to maintain a foothold within the system and continue to carry out malicious activities without being detected. This can lead to the theft of sensitive data, disruption of critical systems, and other damage to the organization. By monitoring the creation of new accounts, organizations can identify potential threats and take steps to mitigate them before they can cause harm.

INFORMATION SHARES

Information sharing is an important aspect of cyber threat intelligence because it allows organizations to better understand and protect against cyber threats. When organizations share information about current cyber threats, they can learn from each other's experiences and take steps to prevent similar attacks from happening to them. This can include sharing information about specific threats, such as malware or phishing campaigns, as well as sharing information about the tactics, techniques, and procedures (TTPs) that threat actors use.

By sharing information, organizations can improve their situational awareness and better understand the threats they face. This can help them prioritize their defenses and allocate resources more effectively. Additionally, information sharing can facilitate the development of new technologies and tactics for combating cyber threats, as well as the creation of partnerships and collaborations with other organizations.

Here are two information shares that impacted our organization this year, along with actionable steps to mitigate risk:

MULTIPLE ATTEMPTS TO DISTRIBUTE EMOTET MALWARE OBSERVED

In November, CyberForce|Q observed multiple attempts to distribute and infect client systems with Emotet malware. Emotet is a globally distributed malware operation that is spread through widespread spam email campaigns with malicious Microsoft Office attachments. It was first discovered in 2014 and was initially used for foreign cyberespionage. After a 4-month disruption by international law enforcement, the malware and its associated criminal gang have resumed their operations. Emotet is widely considered the most dangerous malware operation of all time.

If a network is successfully compromised by Emotet, the operators may not only make critical business data inaccessible, but also attempt to extort the victim organization. If the organization does not pay the ransom, they may publicly disclose sensitive data they have obtained. According to CheckPoint researchers, Emotet infected approximately 1.5 million computers globally and caused an estimated $2.5 billion in damages at its peak. These damages include not only successful extortion attempts, but also business fines and

penalties, forensic and investigation costs, lost revenue from business downtime, and other expenses.

ACTIONABLE STEPS TO MITIGATE RISK

- Be cautious of unsolicited emails, especially ones that contain links or attachments. Don't click on links or open attachments from unknown senders.
- Enabling file extensions in your operating system's settings can help you detect potentially malicious files. By default, many systems hide file extensions, which can make it difficult to tell the difference between a legitimate image file and a disguised executable program. By showing file extensions, you can easily identify files that have unusual or suspicious extensions, such as .exe, and take appropriate action to protect your system from malware
- If your business requires the use of macros, be cautious and only enable them from trusted sources. If possible, disable the execution of macros to help protect your computer from malicious code.
- Use strong, unique passwords for all user accounts and enable multi-factor authentication (MFA) whenever possible. MFA adds an extra layer of security by requiring an additional piece of information, such as a code sent to your phone or a security key, in addition to your password when logging in. This can help prevent unauthorized access to your accounts and protect your sensitive information.

References:

1. Abrams, L. (2022, November 4). *Emotet botnet starts blasting malware again after 4 month break*. https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/emotet-botnet-starts-blasting-malware-again-after-4-month-break/amp/

SOCGHOLISH: JAVASCRIPT MALWARE AS FAKE BROWSER UPDATES

SocGholish is a JavaScript malware framework that has been observed since at least 2017 but is attributed to an ongoing infected website campaign. The malware is distributed through several malicious sites claiming to provide critical browser updates. In reality, these sites are designed to trick victims into downloading and installing malware — usually in the form of .zip or JavaScript (.js) files.

In August, we identified a file that was detected and blocked within a client's environment. This file was a JavaScript (.js) file containing a malicious macro, and our analysis showed that it was associated with a SocGholish campaign.

In November, a large number of regional and national news websites in the United States were infected with SocGholish malware due to a supply chain attack on one of their service providers. Over 250 news sites were affected, including cities such as Boston, New York, Chicago, Washington DC, Miami, Palm Beach, and Cincinnati. The malware was injected into a legitimate JavaScript file that was loaded by the news websites, which then prompted the website visitor to download a fake software update. In this campaign, the fake update was disguised as a browser update for Chrome, Firefox, Internet Explorer, Edge, or Opera.

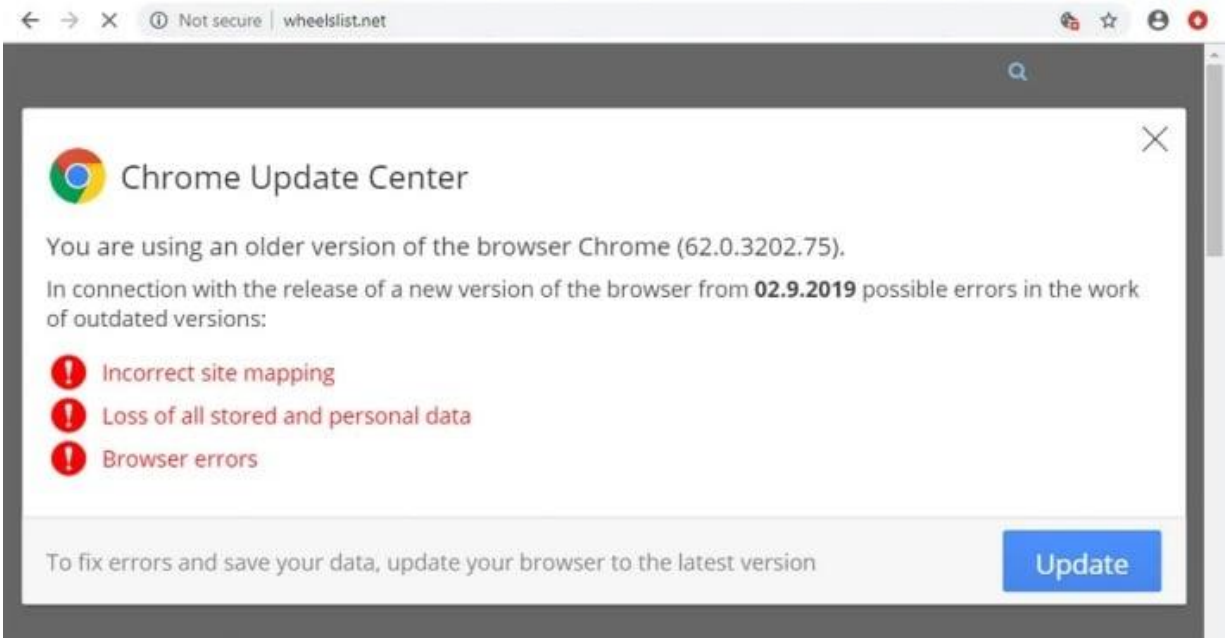


Figure 4: *Example of a fake Chrome browser update download prompt.*

There is strong evidence indicating that SocGholish and its infrastructure have close ties to significant attacks and criminal groups, particularly in Eastern Europe.

ACTIONABLE STEPS TO MITIGATE RISK

- Train employees to recognize and avoid fake browser or operating system updates, fake operating system error messages or prompts to call for assistance, and phishing and vishing messages that request them to download tools or software updates.
- If possible, block the execution of .js files. Removing the file association of JavaScript files, as well as other common suspicious file formats such as .iso, .cab, .wsf, and others can prevent users from accidentally executing files that are not commonly used.
- Implement rules within an EDR/MDR platform or application blocking software to detect wscript.exe activity with .zip and .js in the command line.

References:

1. Kovacs, E. (2023, November 3). *Over 250 US News Websites Deliver Malware via Supply Chain Attack | SecurityWeek.Com*. SecurityWeek - a Wired Business Media Publication. https://www.securityweek.com/over-250-us-news-websites-deliver-malware-supply-chain-attack
2. Page, C. (2022, November 3). *Crime group hijacks hundreds of US news websites to push malware*. TechCrunch. https://techcrunch.com/2022/11/03/hundreds-news-websites-malware/
3. Sinegubko, Denis. "SocGholish: 5+ Years of Massive Website Infections." *Sucuri Blog*, blog.sucuri.net, 16 Aug. 2022, https://blog.sucuri.net/2022/08/socgholish-5-years-of-massive-website-infections.html.

CLOSING REMARKS

As we look back on the past year, it is important to reflect on the threats that we have faced and the progress that we have made in mitigating them. The threat landscape is constantly evolving, and it is crucial that we stay vigilant and proactive in our efforts to protect our organization and our customers.

In this year's threat intelligence report, we have highlighted some of the key trends and developments in the world of cybersecurity, and we hope that the insights and information contained within will help you to better understand and prepare for the challenges ahead. We encourage you to use this report as a resource and a reference, and to continue to stay informed about the latest threats and best practices in the field.

As we move forward into the new year, it is essential that we continue to monitor and analyze the threat landscape, and that we work together as a team to develop and implement effective strategies to mitigate these threats.

At CyberForce|Q, we bring likeminded organizations together to learn about current cybersecurity challenges and share how to strategically address these situations to proactively protect their systems. Through this sharing of security intelligence, every participant continuously makes the collective stronger while advancing their own security posture. By taking part in daily meetings to contribute to the advancement of collective cybersecurity capabilities, and attending group training exercises, participating organizations achieve greater progress than they could alone.

CyberForce|Q does not have any competitors who employ our one-of-a-kind collective model, the way that we do. Participants have achieved proven results from the tactical and strategic sharing of expertise, resources, different perspectives, and ideas. The collective model allows participants to advance their capabilities measurably faster and continuously improve their cybersecurity.

If you have any questions or would like to learn more about our services, please don't hesitate to contact us.

CyberForce|Q LLC
47911 Halyard Drive, Suite #110
Plymouth, MI 48170
www.cyberforceq.com
Office: 248.837.1400|Fax: 248.837.1401
Email: solutions@cyberforceq.com