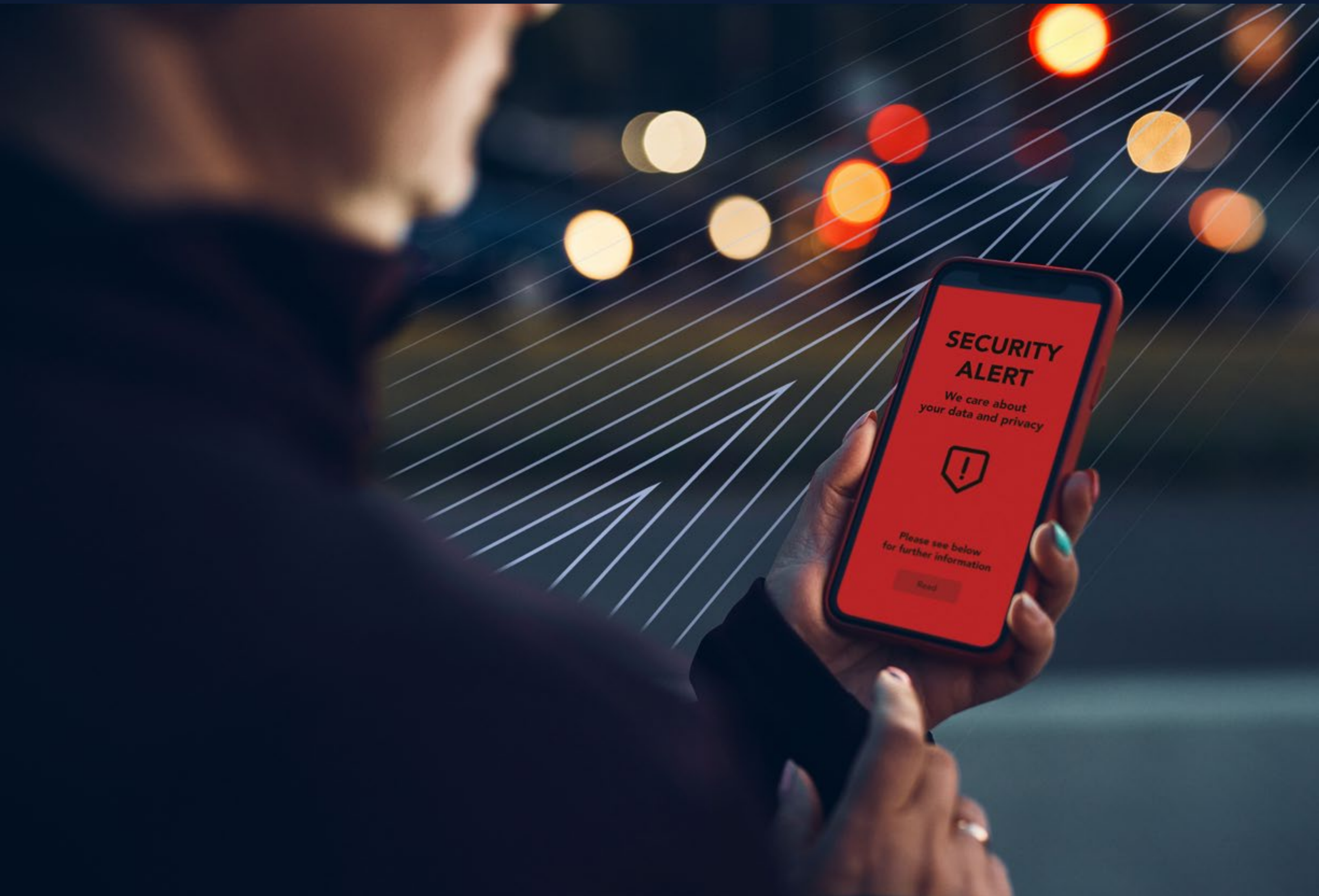
JULY 2025

CBIZ Quarterly Cyber Threat Report

The CBIZ Quarterly Threat Report provides a detailed overview of the most significant cyber threats and trends observed over the past three months. Our goal is to offer valuable insights that will help you understand the evolving threat landscape and its potential implications for your organization.

CBIZ.COM


SECURITY ALERT
We care about your data and privacy
Please see below for further information
Read

The global cyber threat landscape remains highly elevated, with significant impacts reverberating across organizations of all sizes and sectors. Attackers persistently seek out vulnerable targets, often within industries historically underinvested in cybersecurity defenses. As these malicious actors hone their strategies, the repercussions of each attack become more severe, particularly as they set their sights on higher-value objectives.

Contents

01 RokRat

02 Havoc: Using SharePoint with Microsoft Graph API

03 BitM Session Stealing

04 Phishing Leads to Demon Agent

05 RolandSkimmer

06 Fake Zoom Ends in BlackSuit Ransomware

07 SuperCard X

08 Phishing Campaign spreads Infostealer Malware

09 Malicious Payloads Disguised as Bitmap Resources

10 Horabot

11 UNC 6032

RokRat

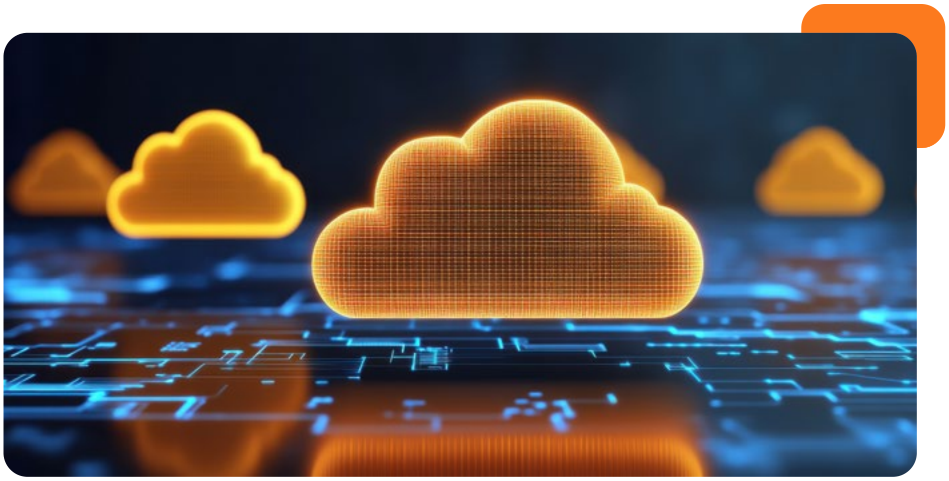
APT37, known as "Reaper," is a North Korean hacking group active since at least 2012. Their focus on cyber-espionage has expanded from South Korean targets to healthcare and manufacturing industries.

The group uses a variety of advanced tools and techniques such as zero-day exploits (vulnerabilities that are not yet known or patched), however generally an attack begins with phishing emails that appear legitimate and contain malicious links or attachments. Users who interact with these emails inadvertently install malware on their systems.

Once inside, they conduct thorough reconnaissance to map out the network and identify valuable data. They also employ obfuscation techniques such as encryption to hide malware from security tools and use persistence mechanisms to ensure malware remains active.

Some of the tools they use include RokRat. A RAT (Remote Access Tool) is used to take control of compromised systems, enabling the attackers to execute various commands, capture screenshots, log keystrokes, and steal sensitive files. RokRat is notable for its ability to use cloud platforms like Dropbox and Yandex for command-and-control operations, making it harder to detect and disrupt as these are generally trusted websites.

FinalRecon is also used to collect detailed system information, providing attackers with insights into hardware, software, and network configurations. This helps with further exploitation of the target environment.



DOGCALL, another reconnaissance tool, captures screenshots, logs keystrokes, and steals files, offering significant intelligence from the infected system, including credentials and confidential communications. This malware provides a comprehensive view of user activities and stored data. Beyond these, APT37 uses various other malware variants designed to disable security software, evade detection, and maintain long-term access to compromised networks.

Thankfully, end-user vigilance and good security practices, chief among them phishing prevention, provide a tremendous bulwark against these attacks. Additionally, simple adherence to timely system patching is also a significant preventative measure.

> *RokRat is notable for its ability to use cloud platforms like Dropbox and Yandex for command-and-control operations, making it harder to detect and disrupt as these are generally trusted websites.*

Havoc: Using SharePoint with Microsoft Graph API

Havoc, used in red teaming and attack campaigns, is a powerful, open-source command-and-control (C2) framework available on GitHub that is used to gain control over targets. Recently, FortiGuard Labs discovered a phishing campaign that combines ClickFix and multi-stage malware to deploy a modified Havoc Demon Agent using a SharePoint site to obscure C2 communications.

The attack begins with a phishing email containing an attachment that deceives users into executing a malicious PowerShell command. This command downloads and runs a script hosted on SharePoint, which checks if the environment is a sandbox, manages registry entries, ensures Python is installed, and runs a hidden Python script.

Havoc conceals C2 communication within Microsoft services by encrypting the victim's information and sending it to the C2 server. The TransportSend function communicates with the C2 server using SharePoint files, which updates requests and retrieves responses.

This example highlights the need for vigilance against phishing emails and guided messages encouraging safe use of terminal or PowerShell applications. The campaign demonstrates how public services like SharePoint and the Microsoft Graph API are integrated with modified Havoc Demon to hide malicious activities, complicating detection efforts.

The attack begins with a phishing email containing an attachment that deceives users into executing a malicious PowerShell command.

BitM Session Stealing

Browser-in-the-Middle (BitM) attacks present a growing security threat, allowing attackers to efficiently compromise user sessions across multiple web applications. These attacks exploit authentication mechanisms to hijack sessions, often bypassing security controls while evading detection. While multi-factor authentication (MFA) remains a critical defense measure, attackers have developed advanced social engineering tactics to circumvent it by targeting session tokens. Once an attacker obtains a valid session token, they can gain access without requiring additional authentication, rendering MFA ineffective in such scenarios.

Attackers frequently use tools like Evilginx2, a transparent proxy that intercepts authentication traffic between users and legitimate services. This technique allows adversaries to capture credentials and session tokens in real time, ultimately granting them full access to the victim's account. BitM attacks take this approach further by leveraging an attacker-controlled browser, where victims unknowingly authenticate within an environment completely under the attacker's control. Unlike traditional token theft, this method provides attackers with live access to accounts, making it particularly effective.

To mitigate these risks, organizations must adopt stronger security measures. Implementing client certificates binds authentication to specific devices, making unauthorized access significantly more difficult. Deploying FIDO2-compatible security keys offers an additional layer of protection, preventing session hijacking even if credentials are compromised. Furthermore, enforcing strict access controls and adopting a layered security approach ensures resilience against evolving threats.

BitM attacks highlight the need for continuous advancements in authentication security. By integrating hardware-based MFA, certificate-based authentication, and stringent access management practices, organizations can greatly reduce their vulnerability to session hijacking and safeguard sensitive data.

> *These attacks exploit authentication mechanisms to hijack sessions, often bypassing security controls while evading detection.*

Phishing Leads to Demon Agent

FortiGuard Labs has identified a phishing attack using a blend of ClickFix and multi-stage malware to deploy a modified Havoc Demon Agent. The attacker conceals each malware stage behind a SharePoint site and employs Microsoft's Graph API to mask communications within trusted services. A fake error message prompts users to run a malicious PowerShell command, which downloads and executes a script from SharePoint. The script verifies its environment and manipulates the computer, then runs another script that hides its activity. This one is used to load and execute harmful code.

The attacker uses the open-source Havoc framework, altered to evade detection, and employs the Microsoft Graph API for secure communication with a command-and-control server. The malware gathers and sends victim information encrypted with AES-256 to the attacker's server. The attacker's commands are received and executed by the infected system. Users are advised to be cautious with email prompts to run terminal or PowerShell commands as they may inadvertently execute harmful actions.

RolandSkimmer

FortiGuard Labs discovered RolandSkimmer, a sophisticated credit card skimming operation via malicious browser extensions for Chrome, Edge, and Firefox. The campaign begins with a deceptive email with a file containing a shortcut that leads to a disguised .jpg URL. This script establishes covert access, performs system reconnaissance, and customizes its behavior based on the victim's environment.

The malware downloads and installs malicious browser extensions. For Microsoft Edge, a fake extension named "Disable Content Security Policy" is installed with excessive permissions to monitor and exfiltrate credit card data. Chrome and Firefox are similarly attacked using tailored archives that simulate legitimate extension environments and auto-import malicious scripts.

The malware evades detection by using various techniques to execute payloads, persistently stores identifiers and encrypted data locally, and exfiltrates information. Edge browser shortcuts are replaced to maintain control without modifying core binaries. Logs from the attacker's server reveal infection paths that adapt depending on detected software. The campaign demonstrates advanced use of legitimate system tools (e.g., msedge.exe, mshta.exe) to maintain stealth and persistence.

As this begins with phishing attempts, it is advised to educate end users on avoiding clicking on links or downloading unknown files from unknown sources. It is best if the environment restricts unverified browser extensions and uses security tools that detect abnormal script behaviors to help prevent threats like this.

> *It is best if the environment restricts unverified browser extensions and uses security tools that detect abnormal script behaviors to help prevent threats like this.*

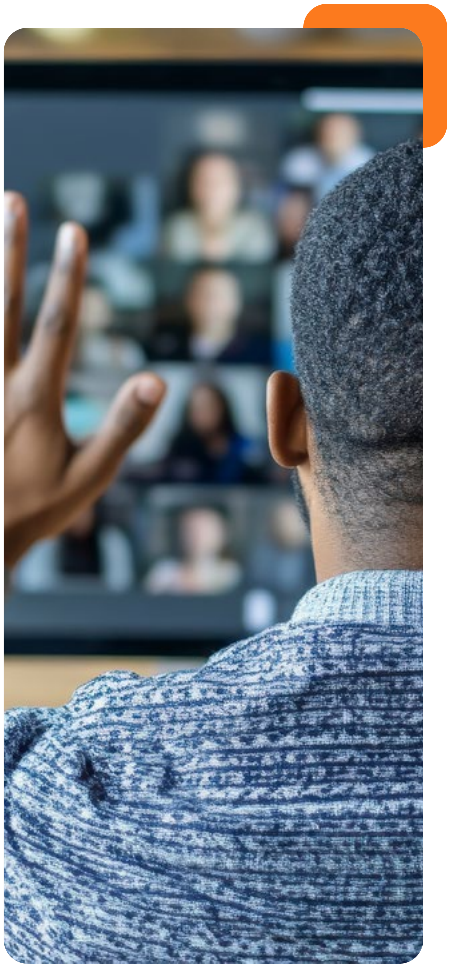
Fake Zoom Ends in BlackSuit Ransomware

A recent cyberattack that leverages fake Zoom installations began when a user downloaded a malicious installer from a website impersonating the app. The attacker crafted the installer using Inno Setup, which launched a batch script that instructed Windows Defender to ignore the payload folder, bypassing it. The script then connected to a Steam Community page (a gaming platform) to retrieve two archive files. One archive contained a legitimate Zoom installer, which, upon execution, led the user to believe the installation was legitimate. The second archive, however, housed an IDAT loader and an encrypted payload. Once executed, the malware injected SectopRAT into MSBuild.exe (a known Windows executable), allowing the attacker to essentially "ride" the reputation of MSBuild.exe to further infiltrate the system and install additional tools like Cobalt Strike and Brute Ratel.

After approximately nine days of undetected activity, the attacker escalated their operations by deploying QDoor, a malware with proxy capabilities, to enable movement to other assets in the environment via RDP (Remote Desktop Protocol) which allows users/machines to connect to others in the environment. Leveraging multiple remote services, including RDP, the attacker moved across the compromised network. To ensure persistence, they used WinRAR to archive files and uploaded them to the cloud-based application Bublup.

The attacker exfiltrated sensitive data before deploying BlackSuit ransomware across all Windows systems found using PsExec, yet another valid Windows system executable. BlackSuit is a known ransomware strain that demands exorbitant ransoms, with some demands reaching as high as $500 million. It encrypts files and threatens to publish or sell stolen data if the ransom is not paid. The FBI and CISA have issued warnings about BlackSuit's tactics, including phishing emails, exploiting vulnerable applications, and utilizing persistence tools like SystemBC and GootLoader.

This attack highlights the growing complexity of modern cyberattacks, where attackers use trusted platforms like Zoom and others such as Steam and Bublup to distribute malware, gain unauthorized access, and deploy ransomware. Organizations are urged to implement strong cybersecurity measures like verification of software sources, continuous monitoring of network activity, and training for users to identify phishing attempts. The latter remains the most important as the initial access in an attack this devastating was simple end-user carelessness.



BlackSuit is a known ransomware strain that demands exorbitant ransoms, with some demands reaching as high as $500 million.

SuperCard X

SuperCard X has been identified as a growing threat in mobile payment fraud. This sophisticated Android Trojan, which utilizes NFC relay attacks to exploit contactless (tap-to-pay) payment systems, is a recent example of how cybercriminals are continually adapting. By covertly bridging the gap between an attacker's device and a user's actual card, this malware enables fraudulent transactions to take place without ever touching the card.

SuperCard X operates by infecting a victim's phone with a malicious "reader" app that is frequently passed off as a genuine tool. The app silently records the card information when the victim unintentionally taps their payment card to their device, either at the app's request or as a result of social engineering. The attacker's "tapper" app receives these details in real time over encrypted channels, which are frequently secured with mutual TLS. At an ATM or point-of-sale terminal, this app then imitates the victim's card, possibly from a different location.

This threat is particularly concerning because of its stealth. It frequently goes undetected by the victim and doesn't require rooting or special device permissions.

As contactless technologies become more deeply embedded in our lives, the threat landscape shifts accordingly. When installing apps, users should exercise caution, especially if they ask for NFC access or provide features related to cards that they are unfamiliar with. All installations of mobile security software should originate from reputable sources, like the Google Play Store, and should be kept up to date. Businesses are urged to make sure endpoint security tools are in place to protect mobile devices that access company systems and to train staff and clients on mobile threat awareness.

> *SuperCard X operates by infecting a victim's phone with a malicious "reader" app that is frequently passed off as a genuine tool.*

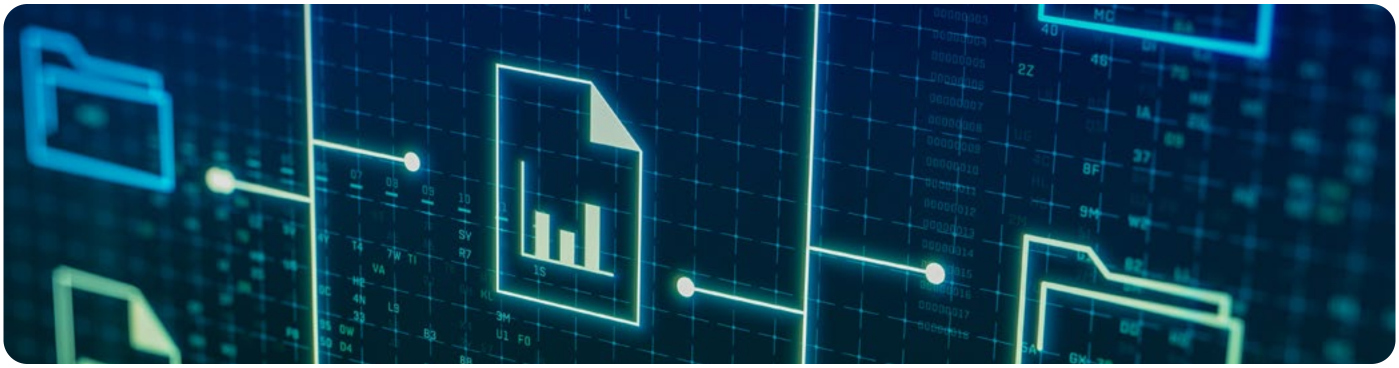
Phishing Campaign Spreads Infostealer Malware

FortiGuard Labs recently discovered a phishing attack using a fake sales order email to trick people into opening a harmful Word document. The document takes advantage of a known security weakness in Microsoft software (CVE-2017-11882) to install Formbook malware on Windows computers. This malware steals personal information like passwords, keyboard inputs, and data from the user's clipboard.

Once the Word document is opened, it secretly runs a file that downloads and installs the malware. To avoid detection, Formbook runs without writing anything to the computer's hard drive. Instead, it uses a sneaky technique called "process hollowing" to hide within a legitimate program called ImagingDevices.exe.

The malware cleverly changes the computer's processes to run the hidden code, making it hard for security programs to spot. Formbook then quietly operates in the background, collecting sensitive information without the user knowing. This attack shows how cybercriminals can use simple phishing emails and known vulnerabilities to deliver sophisticated malware.

This attack shows how cybercriminals can use simple phishing emails and known vulnerabilities to deliver sophisticated malware.



Malicious Payloads Disguised as Bitmap Resources

Cybercriminals are continuously developing new techniques to bypass traditional security measures, one of the latest involving embedding malicious payloads within bitmap image files. These files, commonly used for visual elements like icons and logos, can be used to hide malicious code within their data and appear benign to all but unreasonably intense scrutiny from an end-user. With this method, attackers can stealthily deliver malware without raising suspicion from end-users.

Formats like .bmp and .png contain not only image data but also additional metadata, formatting, and other spaces where this code can be concealed. This obfuscation can make it difficult to detect or otherwise analyze the malware.

Composed emails contained .exe files with names related to procurement, the compromised organization's name, or the date of a specific transaction. A common tactic in these attacks was embedding malicious payloads as bitmap resources in seemingly benign 32-bit .NET applications. There were other obfuscation techniques included, some as advanced as dynamically generating the malicious code at runtime. These techniques greatly strengthen the resilience of malicious .NET applications against reverse engineering.

First, the malicious bitmap resource is unhidden and loaded. Then, as "sv" it is loaded into a .dll file (TL.dll) which is another loader that on its own has no resources and unpacks yet another resource "rbzR" from the first process. The sv resource loaded into TL.dll, another loader, then unpacks the .NET bitmap resource rbzR into Montero.dll, now three stages of obfuscation deep. Montero.dll then unpacks further resources into a final payload, called Remington.exe, using encryption to hide the resource it unpacked. The final payload is an Agent Tesla variant which exfiltrates data via SMTP email and the attack is complete. Using bitmap resources to hide malicious payloads is a prevalent steganography technique in malspam campaigns. Despite all of the advanced obfuscation techniques present, many of which can be used to evade detection, this still relies on an unsuspecting user executing a piece of malware themselves. Once again, proper end-user training will largely eliminate this risk.

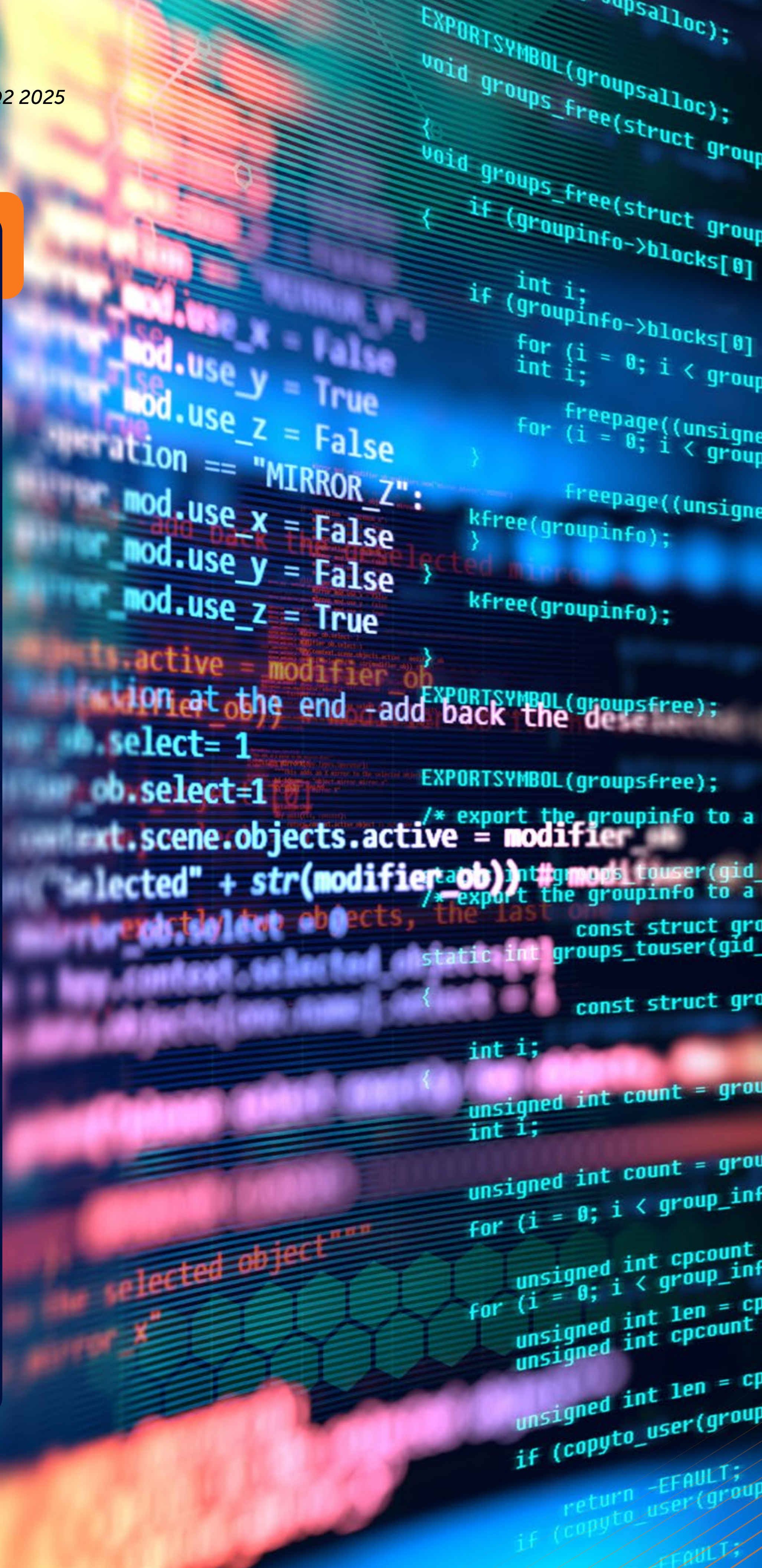
> *Formats like .bmp and .png contain not only image data but also additional metadata, formatting, and other spaces where this code can be concealed.*

Horabot

In April, FortiGuard Labs identified Horabot malware being spread via phishing emails containing malicious HTML files, targeting Spanish-speaking users primarily in Latin America. The malware impersonates invoices or financial documents to deceive victims into opening harmful attachments. It is capable of stealing email credentials, gathering contact lists, and installing banking trojans.

Phishing emails appear to be from legitimate senders in Mexico and reference attached invoices, with the attachment being a malicious ZIP file. The embedded HTML file directs users to a URL that downloads more malicious files. Besides data theft, Horabot also deploys fake pop-up windows to capture user login credentials.

Horabot represents a sophisticated threat, with phishing attacks growing more advanced in Latin America. It spreads via fake Spanish-language emails posing as invoices, tricking users into opening dangerous attachments. The malware conceals its operations, steals login details, and collects email contacts. The malware then propagates further using Outlook, infiltrating corporate and personal networks. Due to its subtle integration into typical Windows and Outlook behavior, detection is challenging. Organizations are advised to block suspicious emails, monitor unusual file activity, and educate employees on phishing dangers.



UNC 6032

Cybercriminal group UNC6032 has been exploiting the growing popularity of AI video generation tools by creating fake websites that mimic legitimate services such as Luma AI, Canva Dream Lab, and Kling AI. These fraudulent sites are promoted through malicious social media ads, particularly on platforms like Facebook and LinkedIn. When users click on the ads, they are directed to download what appears to be an AI tool but is actually a ZIP file containing malware.

The file typically uses a deceptive double-extension to trick users into thinking it's a video file. Upon execution, the malware displays an error message to prompt the user to run it again, fully launching the infection. Once installed, the malware can monitor activity, capture keystrokes, and access sensitive information - including stored passwords.

The attack begins with a Rust-based dropper called STARKVEIL, which unpacks and runs additional malware. Key payloads include COILHATCH (a Python dropper), GRIMPULL (a .NET-based downloader with anti-analysis features), XWORM (a backdoor with keylogging and USB-spreading capabilities), and FROSTRIFT (a .NET backdoor that attempts persistence and targets password manager extensions).

Investigators identified over 120 malicious ads tied to this campaign, with an estimated reach exceeding two million impressions in the EU alone. The U.S. was the most targeted region. The malware uses Tor to hide its command and control traffic, complicating detection and response efforts.

Users are advised to avoid downloading tools from unverified sources, be cautious with AI-related ads, and maintain up-to-date security software. Suspicious activity should be reported to the hosting platforms.

> *Users are advised to avoid downloading tools from unverified sources, be cautious with AI-related ads, and maintain up-to-date security software.*

Contact CBIZ's Cybersecurity Team Today

Our team of highly trained professionals at CBIZ prioritizes excellence and innovation to deliver solutions for organizations at every level. As the full-service technology arm of the seventh largest accounting firm in the U.S., we combine state-of-the-art tools, contemporary methodologies, and a seasoned ensemble of cybersecurity professionals to navigate this intricate space and deliver confidence and security to our clients. CBIZ is your trusted partner in the vast landscape of cybersecurity threats.

Learn more at CBIZ.COM

CBIZ is a consulting, tax and financial services provider that works closely with CBIZ CPAs P.C., an independent CPA firm that provides audit, review and other attest services.