Monthly Cybersecurity Newsletter

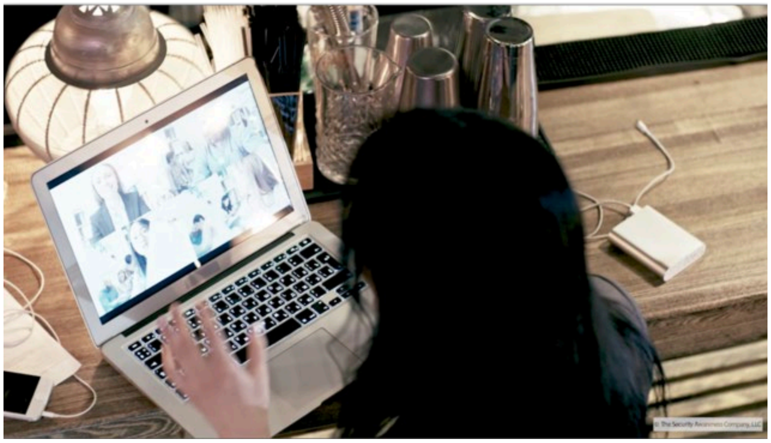
December 2024

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Torry Crass

How Attackers Use Google and Zoom for Phishing Attacks



Platforms such as Google Meet and Zoom rule the new wave of indespensible tools for collaboration and communication. As usage of such tools increases, so does their attractiveness to cybercriminals. It is easy for a cybercriminal to deploy a phishing attack on these platforms targeting unsuspecting users who place their complete trust in the security of the platform.

Let’s begin our conversation by focusing on Google services. Google offers a suite of popular tools, including Gmail, Google Docs and Google Drive, that attackers frequently exploit. Attackers like to re-create fake Google login pages to steal the credentials of unsuspecting users. They begin by creating phishing emails that mimic legitimate messages from Google, such as password reset requests and account vertification prompts. Once the user clicks the link, they are directed to the fake login page where their credentials are captured.

Even the use of malicious links in Google Drive has sparked a bit of concern. Since Google Drive links often appear trustworthy, users may click on them without suspicion. For instance, a phishing email may contain a link to a “shared document” that redirects to a fake login page or a malware-laden file. Users need to be aware before clicking on unknown links.

Attackers have also learned how to exploit Google Forms to leverage their attacks. Most people use Google Forms to create surveys or feedback forms. Users may not think that this would be a malicious act, yet fraudulent actors can create forms to ask for sensitive information such as login credentials or credit card details. These forms most often appear professional and are difficult to detect as fraudulent.

With the rise of remote work and virtual meetings, Zoom has become a prime target for attackers. Attackers create phishing emails to impersonate Zoom notifications, such as meeting invites and reminders, all of which contain links to malicious websites designed to steal Zoom login data or to distribute malware. Cybercriminals distribute fake Zoom software updates via phishing emails or compromised websites. When users download these updates, they inadvertently install malware on their devices.

Why are these attacks so effective? The simple answer is brand trust. Emails and links associated with these platforms are less likely to trigger suspicion. With millions of users worldwide, phishing campaigns targeting Google and Zoom services have a large pool of potential victims.

Defense against these type of attacks cannot be repeated enough. The user is the first line of defense. Updating your software regularly, using multifactor authentication, hovering over links and verifying authenitication are the best defenses you can use.

Unmasking Deceptive Media: Separating Fact from Fiction

How to figure out what is real and what is fake on social media has grown increasingly unclear. More and more of what we are witnessing on social media has been purposely designed to mislead and manipulate us all. We are talking about deceptions from deepfakes and altered images to fake news articles and misleading headlines.

What exactly is deceptive media? It refers to content deliberately crafted to distort one’s perception or to mislead one’s opinion by presenting false or altered information as credible or authentic. This can include fabricated stories, manipulated videos and even subtle changes to legitimate content that alters its context or meaning. Advances in technology, such as artificial intelligence, have made it easier to create convincing fake content, such deepfake videos that superimpose one person’s face onto another person's body in a highly realistic way.

The problem with deceptive media is that it erodes trust in information sources, spreads misinformation and can have serious consequences. Fake news stories have been known to influence elections, spark social unrest and/or damage reputations. Manipulated images and videos can create false narratives, while fabricated social media posts can perpetuate harmful stereotypes.

So, how can you really decipher fact from fiction? Here are a few ways to identify fake media.

- Verify the source. Check to see if the content comes from a credible source. If multiple credible sites align with the narrative, there is a greater chance that the information is true.
- Examine the content. Look for signs of manipulation, such as inconsistencies in lighting, shadows or audio syncing.
- Cross-check the information. Use trusted fact-checking websites to confirm claims.
- Be skeptical. Overly dramatic headlines are a red flag for misinformation.
- Leverage technology. Using tools such as reverse image searches can help identify whether a photo or video is authentic or has been reused in a misleading context.

As long as technology continues to advance, so will the deceitful tactics used by cybercriminals to create deceptive media. However, if we can spot the deceptions and foster awareness among ourselves and our peers, we can be better prepared to combat this growing threat.

SteelFox: The New Kid on The Block

SteelFox is a malware discovered in August that has infected more than 11,000 Microsoft Windows devices worldwide, with significant activity in countries including Brazil, China, Russia and Mexico.

Its ability to evade detection and its global reach make it a formidable threat to users of widely used applications such as AutoCad, JetBrains and Foxit PDF Editor. The malware was dubbed SteelFox due to its ability to steal sensitive data, evade detection and enable unauthorized access to compromised systems.

Cybersecurity News describes this malware as a complex strain combining data-stealing capabilities and cryptocurrency mining functions. It is distributed through forums and torrent trackers, masquerading as software activators or “cracks” for widely used applications. Once installed, this malware infiltrates the system, steals data and uses system resources for unauthorized cryptocurrency mining.

So how do you know if your system is infected by this malware? First, you will notice unexplained slowdowns or crashes due to resource-intensive mining activities. Then, you will see unexpected login attempts or changes in system settings. The last sign is increased outbound traffic as the malware begins to communicate with its command-and-control servers. You will also notice unknown processes being used in the task manager.

Now that we have covered signs of a SteelFox infection, let’s talk about how it actually works. This malware primarily spreads through phishing emails, malicious software updates and infected USB drives. It is delivered through malicious email links or attachments. Once executed, the malware installs itself deep within the operating system, disguising its presence as a legitimate system file.

After installation, SteelFox connects to a command-and-control server to receive instructions and upload the stolen data. The command-and-control communication is heavily encrypted, making detection difficult. This malware uses keylogging, clipboard monitoring and browser injection techniques to steal login credentials, payment information and other sensitive data. It can also search for and exfiltrate documents stored on the device.

The malware employs advanced evasion techniques, such as code obfuscation, anti-debugging and sandbox detection, to avoid being discovered by antivirus software. It also establishes persistence mechanisms, ensuring it remains active even after the system reboots. It has the ability to spread laterally across networks, compromising additional devices. This makes it particularly dangerous for organizations with interconnected systems.

Whom does this malware target? It predominately targets small- and medium-sized businesses with less sophisticated cybersecurity measures, government agencies with classified or sensitive information and individual users who lack robust security practices. They are all targets for this malware.

So how do we protect ourselves from a SteelFox infection?

- The first line of defense is making sure you update all operating systems, antivirus software and applications with patches for known vulnerabilities.
- Be sure to use endpoint detection and response solutions capable of identifying and mitigating these threats.
- Train your end users on how to recognize phishing emails and to avoid downloading attachments and clicking on suspicious links.
- Use network segmentation to restrict the spread of the malware within your network. This helps to protect critical systems and data.
- Strong passwords with multifactor authentication will assist with preventing unauthorized access to accounts and systems.
- Keep an eye on unusual network traffic. Monitor your network for activity that might indicate a malware infection or command-and-control communication.

The SteelFox malware campaign is one of many that reminds us of how sophisticated the tactics deployed by cybercriminals are. It also shows how we must always be one step ahead of the adversary. We must block 100% of the attempts on our systems, but it only takes one breach by an adversary to do serious harm.

Ransomware Gangs Evolve: They're Now Recruiting Penetration Testers

A new concerning cybersecurity trend has emerged. According to the latest Q3 2024 Cato CTRL SASE Threat Report from Cato Networks, ransomware gangs are now actively recruiting penetration testers to enhance the effectiveness of their attacks.

This development signals a significant shift in the tactics employed by cybercriminals and underscores the need for organizations to remain vigilant in their defense strategies.

Traditionally, penetration testers, or "pen testers," have been employed by organizations to identify vulnerabilities in their systems. However, the report reveals that threat actors are now seeking these skilled professionals to join ransomware affiliate programs such as Apos, Lynx, and Rabbit Hole. This move mirrors legitimate software development practices, where testing is crucial before deployment.

"Ransomware is one of the most pervasive threats in the cybersecurity landscape," Etay Maor, chief security strategist at Cato Networks, said. "It impacts everyone – businesses and consumers – and threat actors are constantly trying to find new ways to make their ransomware attacks more effective."

The report also highlights the growing concern of "shadow AI" – the unauthorized use of artificial intelligence applications within organizations. This practice poses significant risks, particularly regarding data privacy. Cato CTRL identified 10 AI applications being used without proper vetting, including Bodygram, Craiyon and Otter.ai. Organizations must be aware of the potential exposure of sensitive information through these unsanctioned AI tools.

Another critical finding from the report is the underutilization of transport layer security (TLS) inspection. Only 45% of the participating organizations in the report have enabled TLS inspection, and a mere 3% inspect all relevant TLS-encrypted sessions. This gap in security leaves organizations vulnerable to attacks hidden within encrypted traffic.

The report found that 60% of attempts to exploit known vulnerabilities were blocked in TLS traffic during the third quarter of 2024. Moreover, organizations that enabled TLS inspection blocked 52% more malicious traffic compared to those without it.

As ransomware gangs continue to evolve their tactics, it's clear that organizations must adapt their cybersecurity strategies accordingly. The recruitment of penetration testers by threat actors represents a significant escalation in the sophistication of ransomware attacks.

To stay ahead of these threats, businesses should:

- Implement comprehensive TLS inspection protocols.
- Be vigilant about shadow AI usage within their organization.
- Regularly update and test their cybersecurity measures.
- Invest in employee training to recognize and report potential threats.

By staying informed and proactive, organizations can better protect themselves against the ever-evolving landscape of cyber threats.

This article is redistributed with permission from KnowBe4.

Phishing Attacks Exploit Microsoft Visio Files and SharePoint

Threat actors are exploiting Microsoft Visio files and SharePoint to launch two-step phishing attacks, according to researchers at Perception Point.

“Perception Point’s security researchers have observed a dramatic increase in two-step phishing attacks leveraging .vsdx files – a file extension rarely used in phishing campaigns until now,” the researchers explain.

“These attacks represent a sophistication of two-step phishing tactics, targeting hundreds of organizations worldwide with a new layer of deception designed to evade detection and exploit user trust.”

The attacks begin with phishing emails that appear to be important business requests, such as purchase orders and proposals. The emails are sent from legitimate, compromised accounts, so they are more likely to bypass security filters. The emails have Outlook attachments that lead to a Microsoft SharePoint page hosting a Visio (.vsdx) file.

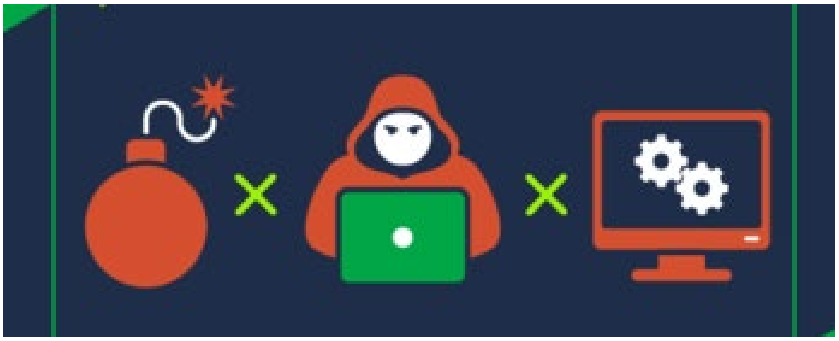
“Inside the Visio file, attackers embed another URL behind a clickable call to action. In most cases, we’ve observed it was a ‘View Document’ button,” the researchers write. “These files vary in appearance, with some even incorporating the breached user organization’s logos and branding to enhance credibility.

“To access the embedded URL, victims are instructed to hold down the Ctrl key and click – a subtle yet highly effective action designed to evade email security scanners and automated detection tools. Asking for the Ctrl key press input relies on a simple interaction that a human user can perform, effectively bypassing automated systems that are not designed to replicate such behaviors.”

After clicking the link, the victim is sent to a spoofed Microsoft 365 login page designed to steal their credentials.

This article is redistributed with permission from KnowBe4.

Nation-State Threat Actors Rely on Social Engineering



A new report from ESET has found that most nation-state threat actors rely on spear phishing as their primary initial access technique.

In the second and third quarters of 2024, state-sponsored advanced persistent threats from China, Russia, Iran and North Korea used social engineering attacks to compromise their targets.

Iranian threat actors continued to conduct cyber espionage against countries across the Middle East, Europe and the U.S. They also expanded their targeting to hit financial companies in Africa.

"We observed indications that Iran-aligned groups might be leveraging their cyber capabilities to support diplomatic espionage and, potentially, kinetic operations," ESET says.

"These groups compromised several financial services firms in Africa – a continent geopolitically important to Iran; conducted cyber espionage against Iraq and Azerbaijan, neighboring countries with which Iran has complex relationships; and increased their interest in the transportation sector in Israel. Despite this seemingly narrow geographical targeting, Iran-aligned groups maintained a global focus, also pursuing diplomatic envoys in France and educational organizations in the United States."

The Russian threat actor Sednit (also known as APT28 or Fancy Bear) launched phishing attacks designed to compromise Roundcube servers in a variety of sectors.

"We discovered new Sednit spear phishing waves, which are part of the already known Operation RoundPress campaign directed against Roundcube webmail servers," the researchers write.

"In the past several months, we observed such spear phishing waves against governmental, academic and defense-related entities in Cameroon, Cyprus, Ecuador, Indonesia, Romania and Ukraine. Sednit used a wide range of lures, from legitimate news articles to a commercial brochure for thermal optics."

The researchers note that North Korean threat actors often establish trust with their victims using phony employment offers before tricking them into installing malware.

"Another distinctive feature of many attacks that we attribute to North Korea-aligned groups is the gradual building up of the relationship with the victim," ESET says. "Both Lazarus and Kimsuky used fake job offers to approach the targeted individuals. Only after the victim responds and a relationship is established is a malicious package sent to the victim."

This article is redistributed with permission from KnowBe4.

Training & Continued Learning Resources

- Cybersecurity & Infrastructure Security Agency Learning: https://learning.cisa.gov/login/index.php
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS Training: https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note:*** *You must have a valid state employee Microsoft 365 account.*

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Upcoming Training & Events

- **Dec 4:** SANS Webinar: Three Keys to Becoming a Cyber Risk Officer
- **Dec 6:** SANS Webinar: Cloud Security Convergence Report Webcast & Forum: How Control Models for A Robust Cloud Security Stack Are Changing
- **Dec 11:** SANS Webinar: Detection Engineering in the Cloud: A Defender's Wonderland
- **Dec 12:** SANS Webinar: What You Need to Know About The Cybersecurity Maturity Model Certification (CMMC)
- **Dec 16** SANS Webinar: SANS Cyber Defense Initiative 2024: SANS@Night – Cybersecurity at the Crossroads: Trends, Challenges, and Leadership Solutions

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on X (formerly known as Twitter), Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. Remember … Stop. Think. Connect.

Disclaimer: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.