Monthly Cybersecurity Newsletter

September 2023
Issue

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

Rise of AI-Driven Malware: How Hackers Are Leveraging Artificial Intelligence

In today's rapidly evolving digital landscape, technology has become an integral part of our lives. From smart homes to autonomous vehicles, the adoption of artificial intelligence (AI) has revolutionized various industries. Unfortunately, as with any technological advancement, there are always those who seek to exploit it for malicious purposes. In recent years, hackers have started to harness AI's power to create sophisticated and highly effective malware, posing new challenges for cybersecurity professionals. In this article, we will explore the rise of AI-driven malware and the potential risks it presents.

AI offers hackers unprecedented opportunities to develop malware that is more stealthy, adaptable and evasive. By employing AI algorithms and machine learning techniques, attackers can automate many aspects of the malware creation process, making it more difficult for traditional defense mechanisms to detect and mitigate their actions.

This malware has the ability to adapt, learn and analyze target systems, making it much harder to detect and defend against. These advanced malware variants can exploit vulnerabilities, evade traditional security methods and even conduct intelligent attacks by mimicking human behaviors.

Moreover, AI-powered malware can utilize techniques like intelligent phishing, which can deceive users by generating highly convincing emails or messages customized to their preferences and interests. This makes it increasingly challenging for individuals and organizations to distinguish between legitimate and malicious communication.

Hackers can leverage AI algorithms to enhance brute-force attacks, making them faster and more targeted. AI can aid in generating more accurate guesses and optimizing the sequence of password guesses.

To combat this growing threat, it is crucial to have a multi-layered security approach. Here are some steps that you can take to protect your systems and your privacy:

- Be sure to keep your software up to date. Regular updates to your operating system, applications and security software will ensure that you have the latest security patches. Many of these updates contain fixes for vulnerabilities that could be exploited by AI-driven software.

- Always try to use reputable security software. Remember that some software packages are malware in disguise. Installing and regularly updating your security software can help detect and block AI-driven software before it can cause harm.

- Employ strong passwords and two-factor authentication. Be sure to use unique passwords for all accounts and not repeatable ones that could be used to brute-force other accounts. Using two-factor authentication on all your accounts makes it harder for hackers to enter your system or application by guessing passwords.

- Use caution when opening email attachments and downloads. Avoid opening or downloading files from unknown or suspicious sources as they may contain AI-driven malware, particularly when it comes from unrecognizable sources.

Taking extra precautions to secure your systems and applications, such as the above-mentioned methods, could safeguard you against AI-driven attacks.

OCR-Driven Malware Targets User Photos for Passwords

Malicious actors are continuously finding innovative ways to exploit vulnerabilities. One such emerging threat is optical character recognition (OCR)-driven malware, which utilizes OCR technology to scan a victim's photos for potentially valuable login credentials, such as passwords and PINs.

To understand how this malware works, we must first understand how OCR works. OCR is a technology that converts printed or handwritten text into machine-readable text. It enables a computer to interpret and process visual data from scanned images or photos. OCR is widely used across various industries for

document digitization, data extraction and text recognition purposes. However, as with any technology, if it falls into the wrong hands, it can be weaponized and exploited for malicious purposes.

A newly identified malware, CherryBlos, masquerades itself within Bitcoin mining apps and other AI computing platforms to steal sensitive data from unsuspecting victims using OCR technology. One thing that most of us are guilty of is taking photos of our passwords to various mobile applications to prevent from forgetting our login information. What we must realize is that this data can be extracted through OCR and used to infiltrate our login credentials.

CherryBlos takes advantage of applications within the Android or Apple Marketplace, where victims unknowingly install it thinking the application is harmless. It attaches itself to the user's mobile device like a hidden rootkit and scans photos for login credentials using OCR technology. In other words, this malware remains dormant on the user's system until the user downloads or opens an image file.

CherryBlos was most recently used in cryptocurrency applications to redirect funds intended for a specific recipient to the malicious account by changing the email address before the transfer occurred.

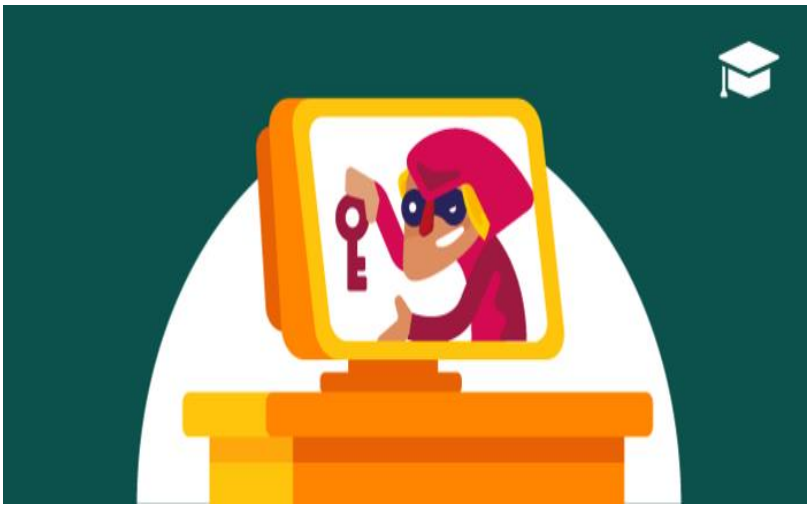
To prevent the download of this malware, you must be cautious about what you install on your system. Keep patches and antivirus software up to date, and exercise caution when downloading files through the play store and email attachments.

Ransomware Attacks Rise 69% and 1,500 Organizations Feel the Hurt

A new report from Rapid7 has found that the number of ransomware attacks increased by 69% in the first half of 2023. Rapid7 incident response data found that at least 1,500 organizations were attacked by ransomware during this period.

The report analyzed data from public disclosures and "leak site communications" -- email, chat and social media channels used by threat actors to market stolen data, coordinate attacks with each other and communicate with victims.

The increase in ransomware attacks is attributed to several factors, including the growing sophistication of ransomware gangs, the increasing availability of ransomware tools and kits and the willingness of some organizations to pay ransoms despite FBI recommendation not to.



Common initial access vectors used by ransomware gangs included remote access (39%), followed by vulnerability exploitation (27%), phishing payloads (13%), supply chain compromise (6%) and insider threat incidents (4%).

Organizations need to be aware of these common initial access vectors and take steps to mitigate them. These include implementing strong security controls such as multi-factor authentication and educating employees about phishing and social engineering attacks.

The report tracked 79 known state-sponsored attacks in H1 2023. The most common technique used by these groups was spear phishing and the abuse of valid accounts.

State-sponsored actors have targeted critical infrastructure, or industries essential to our way of life. A cyberattack on any of them – energy, water, chemical, sewage, transportation, healthcare, financial services, government facilities, food and agriculture, nuclear – could have devastating consequences on our economy, our security and our health.

2021 was a watershed year for critical industry-related attacks, alerting the federal government to the urgency to shore up cybersecurity efforts.

- On February 5, 2021, a water treatment plant in Florida was attacked by the Wizard Spider ransomware group, which briefly released excess chlorine into the water supply.

- On May 30, 2021, JBS Foods, the largest meat processing company in the world, paid $11 million in ransom to REvil after the ransomware group shut down plants in the United States, Canada and Australia. The FBI were able to claw back a paltry $2.3 million of the ransom.

Organizations need to be aware of the growing threat of these attacks and protect themselves by implementing strong security controls, educating employees about social engineering and having an incident plan in place. Additionally, organizations should:

- Educate employees about the consequences of cyber threats. Employees should be taught how to identify and report phishing emails and social media fraud.

- Enable phishing-resistant multi-factor authentication, and use password managers to generate strong passwords and change them regularly.

- Segment the network so that if one part is compromised, the rest of the network is not affected.
- Keep software up to date with the latest security patches, and have a backup plan in place to help recover data if it is encrypted by ransomware.

This article is redistributed with permission from KnowBe4.

Duolingo Users Should Be on the Lookout for Targeted Phishing Attacks

Users of the language learning app Duolingo should be wary of targeted phishing attacks following a recent data leak, according to Anthony Spadafora at Tom's Guide. Criminals scraped the names and email addresses of 2.6 million Duolingo users earlier this year and are now selling the entire dataset on underground forums for approximately $2.13.

"With a real name and valid email address in hand, hackers have all the information they need to launch targeted phishing attacks against Duolingo's users," Spadafora writes. "Unlike regular phishing emails, these messages would be much more personalized since the hackers sending them out have more information to work with. At the same time, they could also try to impersonate Duolingo in their messages in the hope that potential victims would be more likely to click. Besides trying to steal your money, hackers could use these targeted phishing emails to get Duolingo users to install malware on their computers or to provide their credentials or even their payment information since the service does have a paid tier called Super Duolingo."

Spadafora notes that users should watch out for signs of social engineering attacks to protect themselves against potential scams.

“In order to avoid falling victim to phishing, you need to carefully examine all of the emails that arrive in your inbox,” Spadafora writes. “This means looking at the sender’s address and checking to see if it’s a legitimate email address used by Duolingo. From here, you'll want to look out for misspelled words and poor grammar as these are a major red flag when it comes to phishing emails. You also want to avoid clicking on any links or downloading any attachments these suspicious emails may contain. Likewise, you'll want to be on the lookout for language that tries to instill a sense of urgency as hackers and other cybercriminals often use your emotions against you. If you’re worried about a potential deadline or losing access to your Duolingo account, you’re more likely to reply or do what a scammer suggests in their phishing email.”

This article is redistributed with permission from KnowBe4.

Cybercriminals May Already Have Hacked Your LinkedIn Account

New reports show many LinkedIn users have reported complaints about accounts being taken over by bad actors. In a statement from Cyberint researcher Coral Tayar, "Some have even been pressured into paying a ransom to regain control or faced with the permanent deletion of their accounts."

The reported complaints are on other social media forum platforms, such as Reddit, Microsoft and X, with users expressing frustration due to the lack of response from the LinkedIn support team. Per Cyberint, they have also seen an increase of 5,000% in the last few months of search terms for "LinkedIn hack" or "recover record."

The access points cybercriminals are taking to infiltrate are through leaked credentials and/or brute force to attempt to access a large number of LinkedIn accounts.

If a user has strong passwords and/or two-factor authentication, such attacks will only result in a temporary account lock. If your account is poorly protected, then cybercriminals can quickly swap your listed email, so then you can no longer have access. When a high percentage of your C-level positions are using LinkedIn — and almost everyone is — this hack could pose a huge risk for your organization's reputation if the attack is successful.

It is highly recommended to enable two-factor authentication and update your LinkedIn password to something unique and long, ideally a pass-phrase of 25 characters or more. It is important to practice security awareness training to identify how to spot the red flags and learn how to secure your social platforms.

This article is redistributed with permission from KnowBe4.

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

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.*

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

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

Sept. 7: SANS Webinar: **Rapid Incident Response - Solving the Problem of Scale**

Sept. 14: SANS Webinar: **Threat Detection Trends 2023**

Sept. 14: SANS Webinar: **Filling the Human Gap with Technology - Artificial Intelligence May Know You Better Than You Know Yourself**

Sept. 19: SANS Webinar: **How Cloudflare Helps Financial Institutions Improve Visibility Into a Complex Threat Landscape - Q2 Case Study**

October: **Cybersecurity Awareness Month**

Oct. 3: SANS Webinar: **Network Security in the Hybrid Cloud Era**

Oct. 4: SANS Webinar: **How to Get Started With Cyber Security**

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on 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.*