Monthly Cybersecurity Newsletter

August 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

Global IT Outage Highlights Importance of Business Continuity Plans

On July 19, a software update to CrowdStrike's Falcon Sensor, designed to protect against cyberthreats, led to a global IT outage, disrupting businesses and daily life for millions of people.

The failure of the CrowdStrike update had profound implications worldwide, revealing our deep dependency on cybersecurity infrastructure.

Flights worldwide were canceled. People reported being unable to access their bank accounts, and media outlets struggled to broadcast. This widespread outage, caused by an update glitch, serves as a stark reminder of our reliance on technology truly testing our recovery methods.

This incident also highlights the need to have business continuity plans in place to ensure that our organizations can continue to operate through disruptions.

One could only imagine the cascading effects if business continuity plans were not in place during significant IT failures, such as this incident.

Business continuity ensures that organizations can maintain essential functions during and after a disruption, minimizing downtime, protecting data integrity, and ensuring user trust.

Massive Cyberattacks Disrupt French Train Network Ahead of Paris Olympics

In the days leading up to the 2024 Olympic Games in Paris, France's high-speed train network experienced a series of coordinated cyberattacks, severely disrupting travel across the country.

According to reports on X (formerly known as Twitter), French Prime Minister Gabriel Attal stated that "sabotage" had occurred on the network: "Nerve points were attacked, demonstrating a form of knowledge of the network."

The attacks targeted signal box installations on key rail lines connecting major cities to Paris. This attack led to widespread chaos as thousands of passengers, including Olympic spectators, faced significant delays and cancellations.

Deutsche Welle (known as DW) provided extensive coverage of the event. According to its reports, the attacks began on the night before the Olympics' opening ceremony, with arsonists setting fire to cabling boxes at strategic junctions. This caused a rippling report that disrupted the entire network, affecting approximately 800,000 passengers.

This incident highlights the vulnerability of critical infrastructure to cyberattacks, especially during high-profile events like the Olympics. It also highlights the need for tougher cybersecurity measures to protect national transportation systems and ensure the safety and reliability of public transport services.

Phishing Campaigns Continue to Exploit CrowdStrike Outage

As expected, threat actors are taking advantage of the global IT outage caused by a faulty CrowdStrike update, SC Media reports.

Cybercriminals quickly registered dozens of phishing domains related to the outage, including "crowdstrike-helpdesk[.]com" and "crowdstrikefix[.]com."

CrowdStrike issued an advisory warning that threat actors are conducting the following activity:

- Sending phishing emails posing as CrowdStrike support to customers
- Impersonating CrowdStrike staff in phone calls
- Posing as independent researchers, claiming to have evidence the technical issue is linked to a cyberattack and offering remediation insights
- Selling scripts purporting to automate recovery from the content update issue

CrowdStrike is also tracking a phishing campaign that is targeting customers in Latin America with Spanish-language instructions to remediate the issue. The threat actor instructs victims to download a file called "crowdstrike-hotfix.zip," which will install the RemCos remote access trojan.

The U.S. Cybersecurity and Infrastructure Security Agency, the UK's National Cyber Security Centre and the Australian Signals Directorate (ASD) have each issued warnings on increased phishing activity.

The ASD stated: "An increase in phishing referencing this outage has already been observed, as opportunistic malicious actors seek to take advantage of the situation."

Security firm Bolster has also observed threat actors setting up domains that impersonate law firms offering to file legal claims against CrowdStrike.

"Given the financial losses likely to be incurred due to the widespread outage, many individuals and businesses may seek to recoup their losses through legal action or government assistance, creating a fresh opportunity for threat actors to strike," SC Media writes.

"Business leaders should remain wary of potential scams such as phony recovery funds or websites impersonating law firms as they work to recover from the incident."

Smart TVs Can Be Targets for Cybercriminals

As smart TVs become more sophisticated by integrating features such as internet connectivity, voice commands and built-in cameras, they bring with them both convenience and potential security risks.

Above all, the most alarming concern for security professionals is the potential for cybercriminals to use the cameras on these devices for spying.

So, how does this happen?

Smart TVs are essentially computers, and like any connected device, they can be vulnerable to hacking. Cybercriminals can exploit security flaws in the TV's software, gaining remote access to the camera and microphone. Once inside, they can watch and listen to unsuspecting users, collect sensitive information or capture private moments.

The manufacturers of smart TVs also pose a security risk to their users. Some smart TVs come with terms and conditions that allow the manufacturers to collect data for marketing purposes. This might include voice commands or viewing habits, which can be unsettling for privacy-conscious individuals.

While smart TVs offer advanced capabilities, it is important to think about how these items affect our security. Taking a few precautionary measures can prevent unauthorized access, allowing us to enjoy our smart TVs without compromising our privacy.

Protecting Yourself

- Keep your device's software updated. Manufacturers often release updates to patch security vulnerabilities, ensuring that the TV's firmware is up to date.
- If you do not use the camera or the microphone feature on your TV, disable them in the system settings.
- When you are not using the camera, cover it. Using a physical cover or tape could prevent unauthorized access.
- Make sure to secure your home Wi-Fi network with a strong password and encryption. Avoid connecting your TV to public networks.
- Go through your TV's privacy settings and disable the data collection features.

Is Your Bank Really Calling? How to Protect Yourself from Financial Impersonation Fraud

Protecting your financial information has never been more crucial. With the rise of sophisticated scams, it's becoming increasingly difficult to distinguish between legitimate bank communications and fraudulent attempts to access your accounts. So, how can you be sure it's really your bank contacting you?

The Vulnerability of Personal Information

First, it's important to understand that our personal details are more accessible than we might think. Previous data breaches have potentially exposed many people's names, addresses and even Social Security or bank account numbers to cybercriminals.

This means that they may already have a wealth of your personal information at their fingertips when they contact you, making their scams seem more legit.

For example, they may pretend to call from your bank using all the above-listed details to “identify” themselves to you, warning you about a suspicious transaction coming off your account. They will try to get you into a stressed or panicked state, which makes you more likely to comply with their demands.

Red Flags to Watch Out For

- **Requests for passwords or OTPs:** Remember, legitimate banks will never ask for your password or one-time password (OTP) over the phone. If someone claiming to be from your bank asks for this information, it's a major red flag.
- **Suspicious links or downloads:** Be wary of emails or text messages from your bank that include links or files to download. These are very likely phishing attempts aimed at installing malware or stealing your login credentials.
- **Pressure tactics:** Cybercriminals often create a sense of urgency or panic to cloud your judgment. If you feel rushed or pressured during a call, it's likely not your bank calling.
- **Unsolicited calls:** Banks rarely make unsolicited calls to customers. They prefer to communicate through secure channels such as official banking apps.

When banks do need to verify your details, they typically use automated systems rather than direct phone conversations. For promotional calls, they follow strict verification protocols that don't involve asking for sensitive information over the phone.

Protecting Yourself

Here are some tips if you receive suspicious calls or are worried about your account's security.

- If you have any doubts, end the call immediately.
- Contact your bank directly using its official phone number or banking app.
- Don't be fooled by local accents or personal details the caller might know.
- Trust your instincts. If something feels off, it probably is.

Remember, it's always better to be cautious. A quick call to your bank's official number can resolve any uncertainties and potentially save you from financial loss. By recognizing the signs of scam attempts and understanding how banks actually communicate, you can protect your hard-earned money and maintain peace of mind in your financial dealings.

Scammers Exploit Interest in Generative AI Tools

Researchers at Palo Alto Networks' Unit 42 are tracking phishing attacks exploiting interest in generative AI tools. The researchers observed spikes in suspicious domain registrations over the past year that correlated with current news.

"The domain registration trend is clearly correlated to the fluctuating popularity of the topic, with data peaks aligning with major ChatGPT milestones," the researchers write.

"Following Microsoft's announcement of ChatGPT integration with Bing on Feb. 7, 2023, we observed a surge in the number of new domains where many of them contain both trademarks (e.g., msftchatgpt[.]com). Another significant spike occurred on March 14, 2023, coinciding with the official release of GPT-4. The next peak corresponds to the announcement of new GPTs on Nov. 6, 2023, during which numerous related domains, like gptsotre[.]com, were registered."

The term "gpt" is used by the majority of these sites, since ChatGPT is one of the most well-known generative AI tools.

"The most abused keyword is 'gpt,' whose suspicious rate is 76%," the researchers explain. "This word, though not exclusively related to the GenAI topic, demonstrates a significant correlation with it. After filtering out domains unrelated to GenAI, this term was rarely used for domain creation prior to 2023, while its popularity surged along with the GenAI trend."

The researchers also observed many suspicious domains themed around tutorials for prompt engineering.

"As interest in GenAI grows and more people seek to become experts in its use, prompt engineering emerges as a hot topic," Unit 42 says. "We also observed that 'prompt' frequently coexists with 'gpt' and 'engineering' in domain names. Our findings suggest that people must exercise caution when visiting websites offering tutorials on prompt engineering, as a significant percentage of them are shady."

Training & 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/

Upcoming Training & Events

- **Aug. 13:** SANS Webinar: Elevating Your Audit Strategy: Insights from the CRF Audit Framework
- **Aug. 13:** SANS Webinar: Demystifying Base64: A Detailed Beginner's Guide to Encoding and Decoding
- **Aug. 14:** SANS Webinar: SANS Chicago 2024: SANS@Night - How to Perform Effective OT Cyber Security Risk Assessments
- **Aug. 20:** SANS Webinar: Empowering a Modern SOC With AI: Practical Use Cases
- **Aug. 21:** SANS Webinar: Exploring the Link Between Corruption and Cybercrime
- **Aug. 21:** SANS Webinar: Human-Powered Security with HackerOne

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.
