dexian

CYBERCHAT

Cybersecurity Trend Report Q3 | 2025

Welcome to Dexian CyberChat, a quarterly newsletter that keeps you updated on relevant news stories, cybersecurity threats that may put organizations at risk, and tips and solutions that can help protect against these malicious activities.

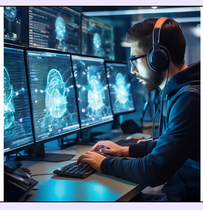
Scammers Spread False Support Info Using Legitimate Websites

When problems occur on a digital platform or service, consumers often Google the customer support line, connecting with an agent or chatbot without a second thought. A story from Dark Reading suggests that this nonchalant habit might jeopardize consumers. Cybercriminals are now using a fraudulent tactic where they imitate major brands in Google-sponsored ads to trick people into giving away personal information.

KEY TAKEAWAYS

- These attacks are known as search parameter injection attacks, using malicious URLs to hijack a user's experience.
- Instead of diverting traffic to a fake site, these fraudsters send victims to the intended brand's website but overlay fake information as needed.
- When consumers call the fake number given, they encounter a scammer who phishes for personal data, card details, or even remote access to their device.
- Consumers can avoid scams by looking for any suspicious messages emphasizing emergencies or a need to call now.
- The best protection is often to follow official links from company emails to official pages to avoid any injection attacks.

LEARN MORE >>



North Korean Hackers Deepfake Execs in Zoom Calls to Spread Mac Malware

Is that really your CEO on the other end of a Zoom call? Maybe not. Bleeping Computer recently shared a story about a growing trend where hackers create deepfakes to pose as company executives and trick employees into downloading malicious files. BlueNoroff, a North Korean hacking gang, is using this tactic to compromise systems undetected and extract sensitive data.

KEY TAKEAWAYS

- Hackers start by sending Calendly invites to employees through messaging applications, luring them to a fake Zoom domain that the hackers control.
- Upon entering the Zoom meeting, employees will see photorealistic deepfakes of their senior leadership (so that requests appear credible) as well as representatives of an "external company."
- Hackers fabricate technical issues and then tell employees to download a Zoom extension, which links to a legitimate Zoom SDK page, but also executes a malicious command.
- The malicious command disables bash history logging so that hackers can reduce the detection of their actions.
- Eight malware tools are injected into the system to help evade scrutiny, maintain the malware's configuration state, decrypt encrypted information, surveil keystrokes, and extract sensitive information.

LEARN MORE >>

ChainLink Phishing: How Trusted Domains Become Threat Vectors

People often put their trust in trusted domains for their reliability and security measures, but now hackers are finding ways to use those as attack vectors. ChainLink phishing can trick even security-aware employees, funneling them through chained sequences that start with trusted infrastructure, but end in compromise.

KEY TAKEAWAYS

- Google Drive and Dropbox links are often the starting point for deceiving users, which allows them to sail past email and network filters.
- After clicking on the link, users are guided through a series of prompts until they give their business credentials to criminals.
- ChainLink phishing attacks often simulate CAPTCHA and email automation as a way of maintaining trust until credentials are stolen.
- Endpoint tools tend not to detect this attack strategy because hackers don't deploy malware, just collect credentials.
- Organizations that can overcome this threat will need to do so at the browser level.

LEARN MORE >>

AHA Warns Hospitals as Play Ransomware Targets RMM Tool Vulnerability

Last year, 238 of the 444 cyberattacks on healthcare organizations were from ransomware. Though this threat isn't new, hackers are changing their tactics to maximize profits. A recent Healthcare IT News article dug into how the Play ransomware group is currently using a double-layered extortion model that not only encrypts your systems, but also steals your sensitive data.

KEY TAKEAWAYS

- By creating unique hashes for each deployment of their ransomware, the malicious code is difficult to decrypt and presents a challenge for anti-malware and anti-virus programs to detect.
- Play has a habit of gaining network access by abusing valid accounts which they then use to manipulate public-facing applications.
- Play has exploited vulnerabilities in FortiOS, Microsoft Exchange, and SimpleHelp (which they are using for remote code execution).
- Enabling multi-factor authentication for webmail, VPN and accounts that access critical systems can provide an essential layer of protection to stop this attack.

LEARN MORE >>

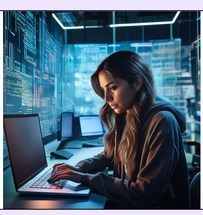
How Hackers Are Turning Tech Support into a Threat

When cybercriminals want to attack retailers and other big brands, they have a secondary line of attack as an option: outside call centers. Hackers are now trying an assortment of strategies to trick customer agents across call centers to accidentally help them bypass two-factor authentication techniques so these criminals can access bank accounts, credit card numbers, and other online portals. Coinbase and other companies using outsourced call centers have already been targeted.

KEY TAKEAWAYS

- Cybercriminals masquerade as high-level executives demanding system access, use malicious software to scrape data, or even pay call center employees for help.
- Coinbase experienced an attack where call-center workers were paid for access, resulting in data losses for 97,000 customers and potentially $400 million in pledged reimbursements.
- Once criminals bought the stolen Coinbase information, they called up victims and posed as Coinbase employees, selling the scam by verifying PII and account balances. Victims were then convinced to create new crypto wallets with encryption keys that the criminals would know.
- According to Coinbase, criminals used social media and Telegram chats, providing offers of $2,500 for help from insiders to breach the system.
- Cybercriminals would also contact insiders for information on all the software on their computers, finding the extensions and programs that had vulnerabilities they could use to sneak data exfiltration tools into the system.

LEARN MORE >>



Russian APT29 Exploits Gmail App Passwords to Bypass 2FA in Targeted Phishing Campaign

Russian-sponsored hacking groups have stayed active and are continuing to target prominent academics and critics of the current state. In the hopes of gaining access to their targets' emails, they have started employing social engineering techniques to gain access to the application specific passwords feature in Google. Though their targeting methodology is slow and steady, it has garnered results in the goal of bypassing two-factor authentication.

KEY TAKEAWAYS

- Researchers studied the attacks and found that cybercriminals built a solid rapport with their targets and created tailored lures over a series of weeks to ease their suspicions.
- Many of these emails had multiple fake State Department addresses in the CC bar to lend a sense of legitimacy, abusing the fact that the DOS email server accepts all addresses without bouncing back.
- Victims of these attacks were convinced to create a 16 digit application-specific password (ASP) under the pretense of accessing a secure State Department platform.
- Google claims it has taken steps to secure the accounts compromised by this and other Russian campaigns.

LEARN MORE >>