dexian

CYBERCHAT

Cybersecurity Trend Report Q2 | 2026

Welcome to Dexian CyberChat, a quarterly newsletter that keeps you updated on relevant news stories, cybersecurity threats, and solutions to help protect against these malicious activities.

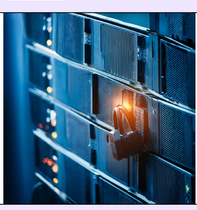
Anthropic Finds 22 Firefox Vulnerabilities Using Claude Opus 4.6 AI Model

Though plenty of high-profile stories showcase how AI is upending cybersecurity strategies, Anthropic recently demonstrated the defensive value of the right AI tools. In a security partnership with Mozilla, the AI company identified 22 vulnerabilities in the Firefox web browser in just two weeks. The majority of the bugs that the Claude Opus 4.6 model identified were patched for Firefox 148 in February with the remaining bugs to be resolve in subsequent versions.

KEY TAKEAWAYS

- Of the 22 vulnerabilities identified: 14 were high-severity, seven were moderate severity, and one was low-severity.
- In just the first 20 minutes, the Claude Opus 4.6 model identified a use-after-free bug in the browser's JavaScript that hackers could have used for malicious exploits.
- Human researchers validated these vulnerabilities in a virtualized environment to rule out false positives before developing fixes.
- Anthropic also tasked Opus 4.6 with creating practical exploits for each of the Mozilla vulnerabilities to determine how difficult it would be to use these bugs.
- After carrying out several hundred tests and spending about $4,000 in API credits, Opus 4.6 was only able to produce working exploits for two vulnerabilities.
- Anthropic said, "This behavior signaled two important aspects: the cost of identifying vulnerabilities is cheaper than creating an exploit for them, and the model is better at finding issues than at exploiting them."

LEARN MORE >>



Amazon: AI-Assisted Hacker Breached 600 Fortinet Firewalls in 5 Weeks

More than 600 FortiGate firewalls across 55 countries have been breached as part of a 5-week AI-fueled attack campaign. These attacks managed to compromise systems without using any known exploits and instead used brute force attacks against organizations with weak MFA protection and exposed management interfaces. The Amazon Integrated Security team discovered the server hosting malicious tools specifically targeting Fortinet FortiGate firewalls.

KEY TAKEAWAYS

- Organizations across South Asia, Latin America, the Caribbean, West Africa, Northern Europe, and Southeast Asia were impacted by the attack.
- The attacks were opportunistic rather than targeted against specific industries or businesses.
- The threat actor extracted SSL-VPN user credentials with recoverable passwords, administrative credentials, firewall policies and internal network architecture, IPsec VPN configurations, network topology, and routing information.
- After extracting the configuration files, the hacker appears to have used AI-assisted Python and Go tools to parse and decrypt the data.
- Researchers identified the malicious reconnaissance tool as AI-generated due to the source code being filled with simplistic architecture that prioritizes formatting over functionality and redundant comments that restate function names.
- Amazon said, "While functional for the threat actor's specific use case, the tooling lacks robustness and fails under edge cases—characteristics typical of AI-generated code used without significant refinement."

LEARN MORE >>

LLMs Can Unmask Pseudonymous Users at Scale with Surprising Accuracy

Say goodbye to any vestiges of online anonymity. Researchers from across the public and private sectors have explored the capabilities of large language models (LLMs) to deanonymize users across various profiles, potentially uncovering pseudonyms people once trusted for their privacy. LLMs can potentially make it easier for bad actors and authoritarian governments to dox, stalk, and profile people based on their account information.

KEY TAKEAWAYS

- In terms of recall (i.e., the share of users that the method correctly identified and deanonymized), LLMs had a 68% success rate.
- AI tools appear to surpass the manual work of skilled investigators as well as algorithmic matching from structured data sets gathered by humans.
- Starting only from free text, AI agents can browse the web and use simulated reasoning to match potential individuals until they have the full identity of a person.
- Some of these techniques build on the Netflix Prize Attack, which used information about user preferences to extrapolate things like political preferences and other sensitive information.
- "The average online user has long operated under an implicit threat model where they have assumed pseudonymity provides adequate protection because targeted deanonymization would require extensive effort. LLMs invalidate this assumption," the researchers concluded.

LEARN MORE >>

Qualcomm Zero-Day Exploited in Targeted Android Attacks

Getting caught flat-footed by an exploit is a nightmare situation. Case in point: a recently identified, high-severity Qualcomm bug is already being used in targeted attacks against vulnerable Android devices. The high-severity vulnerability, known as CVE-2026-21385, can cause memory corruption in Qualcomm's graphics kernels for a wide range of Android chipsets.

KEY TAKEAWAYS

- CVE-2026-21385 is an integer overflow issue (i.e., where arithmetic operations produce an integer that surpasses the max defined by a given programming language)
- This vulnerability received a score of 7.8 on the Common Vulnerability Scoring System (CVSS).
- According to Google, "There are indications that CVE-2026-21385 may be under limited, targeted exploitation."
- Qualcomm says, "Regarding their GPU-related research, fixes were made available to our customers in January 2026. We encourage end users to apply security updates as they become available from device makers."
- The biggest challenge is that consumers are reliant on the original equipment manufacturer (OEM) to fix an impacted device with a patch, something some OEMs are slow to do.

LEARN MORE >>

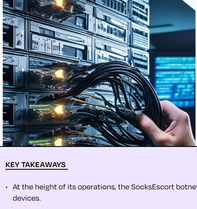
Hacked Prayer App Sends 'Surrender' Messages to Iranians Amid Israeli and US Strikes

Consumer and commercial applications are targets as much as public utilities and programs in today's modern warfare. As U.S. and Israel targeted physical infrastructure in Iran, digital operations compromised popular websites and applications. Most notably, users of the BadeSaba Calendar, a prayer-timing app downloaded more than 5 million times from the Google Play Store, sent unauthorized messages to users in Iran.

KEY TAKEAWAYS

- Users of BadeSaba Calendar received messages like "help has arrived" and "defend your brothers" within 30 minutes of the first explosions.
- "The compromise of assets [likely] happened some time ago, and these messages of 'help' were timed. This is not a smash-and-grab style of attack. It is nation-state versus nation-state and is being executed with intent and precision," said Morey Haber, Chief Security Advisor at BeyondTrust.
- In addition to widespread internet blackouts throughout Iran, several state-affiliated news agencies, including IRNA and ISNA, are down.
- "Many witnessed what it means when the internet goes dark, and there is no visibility, no documentation, and no outside attention. That fear is not theoretical for us; we have already lived through it," said Narges Keshavarznia, Digital Rights Researcher at The Miaan Group.

LEARN MORE >>



Law Enforcement Shuts Down Botnet Made of Tens of Thousands of Hacked Routers

In March, a global coalition of law enforcement agencies successfully shut down a botnet comprised of thousands of hacked consumer-grade and small-business routers worldwide. SocksEscort, a criminal proxy service, used these routers to commandeer the victims' bank and cryptocurrency accounts as well as file fraudulent unemployment insurance claims. According to the DOJ, this botnet cost Americans millions of dollars before it was finally stopped.

KEY TAKEAWAYS

- At the height of its operations, the SocksEscort botnet allegedly controlled more than 369,000 routers and IoT devices.
- Over half of the botnet's victims were in the United States or the United Kingdom.
- SocksEscort also facilitated ransomware and distributed denial of service (DDoS) attacks.
- Users of this criminal service were able to hide their original IP addresses by paying for licenses to this botnet, covering up their engagement in various criminal activities.
- More than just shutting down SocksEscort, the law enforcement agencies have said the infected routers have been disconnected from the service.

LEARN MORE >>