15 Jul 22

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

China's Tonto Team Increases Espionage Activities Against Russia

The state-sponsored threat actor group Tonto Team, which has been linked to China-backed cyber operations, is ramping up its spying campaign against Russian government agencies. The campaign, which involves an email, a Word document file in RTF (Rich Text File) format, and a backdoor payload, starts off with socially engineering recipients to convince them to open a malformed attachment, triggering the execution of an MS Office exploit.

https://blog.malwarebytes.com/hacking-2/2022/07/chinas-tonto-team-increases-espionage-activities-against-russia/

Mantis Botnet Behind the Record-Breaking DDoS Attack in June

The record-breaking distributed denial-of-service (DDoS) attack that Cloudflare mitigated last month originated from a new botnet called "Mantis," which is currently described as "the most powerful botnet to date." The botnet is extremely powerful despite relying on a small number of devices. Mantis targets servers and virtual machines, which come with significantly more resources. Mantis targets entities in the IT and telecom (36%), news, media, and publications (15%), finance (10%), and gaming (12%) sectors.

https://www.bleepingcomputer.com/news/security/mantis-botnet-behind-the-record-breaking-ddos-attack-in-june/

Search Here: Ransomware Groups Refine High-Pressure Tactics

Ransomware groups continue to refine the tactics they use to better pressure victims into paying. Psychological pressure remains a specialty. After infecting systems, many types of ransomware reboot infected PCs to a lock screen that lists the ransom demand, a cryptocurrency wallet address for routing funds and a countdown timer. Oftentimes such ransom notes include a threatening message, warning that all data will be wiped — or the ransom demand doubled or stolen data publicly leaked — should the countdown reach zero.

https://www.govinfosecurity.com/search-here-ransomware-groups-refine-high-pressure-tactics-a-19557

First Cyber Safety Review Board Report Finds Log4J Has Become an "Endemic Vulnerability"

The inaugural report by the Homeland Security Department's Cyber Safety Review Board found that, despite efforts by organizations across the federal and private sectors to protect their networks, Log4j has become an "endemic vulnerability" — meaning unpatched versions of the omnipresent software library will remain in systems for the next decade, if not longer.

https://therecord.media/first-cyber-safety-review-board-report-finds-log4j-has-become-an-endemic-vulnerability/

"Lives Are At Stake": Hacking of U.S. Hospitals Highlights Deadly Risk of Ransomware

The number of ransomware attacks on U.S. healthcare organizations increased 94% from 2021 to 2022. Last week, the U.S. government warned that hospitals across the United States have been targeted by an aggressive ransomware campaign originating from North Korea since 2021.

https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals

Microsoft Published Exploit Code for a MacOS App Sandbox Escape Flaw

Microsoft published an exploit code for a vulnerability in macOS that can allow an attacker to escape the sandbox. Microsoft publicly disclosed technical details for an access issue vulnerability, tracked as CVE-2022-26706, that resides in the macOS App Sandbox.

https://securityaffairs.co/wordpress/133211/hacking/macos-sandbox-bypass-exploit.html

New Retbleed Speculative Execution Attack Impacts Both Intel and AMD Chips

Researchers warn of a new vulnerability, dubbed "Retbleed," that impacts multiple older AMD and Intel microprocessors. An attacker can exploit the flaw to bypass current defenses and perform Spectre-based attacks. The Retbleed vulnerability is tracked as CVE-2022-29900 (AMD) and CVE-2022-29901 (Intel).

https://securityaffairs.co/wordpress/133211/hacking/macos-sandbox-bypass-exploit.html