26 Aug 22

Cyber Threat Roundup

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

Contents

Articles

Thousands of Organizations Remain at Risk From Critical Zero-Click IP Camera Bug

The bug (CVE-2021-36260) is a command injection vulnerability that is present in the Web server of several Hikvision cameras. The organizations using the unpatched devices are at risk of network compromise, and potentially even physical attack; attackers could use the zero-click vulnerability to take complete control of affected Hikvision cameras.

https://www. darkreading.com/vulnerability-management/thousands-organizations-risk-critical-ip-camera-bug

Microsoft Uncovers New Post-Compromise Malware Used by Nobelium Hackers

The threat actor behind the SolarWinds supply chain attack has been linked to yet another "highly targeted" post-exploitation malware that could be used to maintain persistent access to compromised environments. Dubbed "MagicWeb" by Microsoft's threat intelligence teams, the development reiterates Nobelium's commitment to developing and maintaining purpose-built capabilities.

https://www.thehackernews.com/2022/08/microsoft-uncovers-new-post-compromise.html

Researchers Uncover Kimusky Infra Targeting South Korean Politicians and Diplomats

The North Korean nation-state group Kimusky has been linked to a new set of malicious activities directed against political and diplomatic entities located in its southern counterpart in early 2022. Included among the potential victims are South Korean university professors, think tank researchers, and government officials.

https://www.thehackernews.com/2022/08/researchers-uncover-kimusky-infra.html?&web_view=true

Hackers Adopt Sliver Toolkit as a Cobalt Strike Alternative

Threat actors are dumping the Cobalt Strike penetration testing suite in favor of similar frameworks that are less known. However, malicious activity using Sliver can be detected using hunting queries drawn from analyzing the toolkit, how it works, and its components.

https://www.bleepingcomputer.com/news/security/more-hackers-adopt-sliver-toolkit-as-a-cobalt-strike-alternative/?&web_view=true

Twilio Hackers Scarf 10K Okta Credentials in Sprawling Supply Chain Attack

The hackers who breached Twilio and Cloudflare earlier in August also infiltrated more than 130 other organizations in the same campaign, vacuuming up nearly 10,000 sets of Okta and two-factor authentication (2FA) credentials. That's according to an investigation from Group-IB, which found that several well-known organizations were among those targeted in a massive phishing campaign that it calls "Oktapus".

https://www.darkreading.com/remote-workforce/twilio-hackers-okta-credentials-sprawling-supply-chain-attack

AlphV/Black Cat Attacks Airline Technology Provider Accelya

AlphV/Black Cat has been very busy this year with numerous attacks in various industries that include local governments, colleges, and energy companies, and has now moved on to the airline industry. In the current threat environment, it is likely ransomware groups will continue to create costly disruptions for companies of all industries and sizes.

https://www.binarydefense.com/threat_watch/alphv-black-cat-attacks-airline-technology-provider-accelya/

Threat Assessment: Black Basta Ransomware

Black Basta affiliates have been very active deploying Black Basta ransomware and extorting organizations since the ransomware first emerged. Based on multiple similarities in tactics, techniques and procedures (TTPs), and how quickly Black Basta amassed its victims, the Black Basta group could include current or former members of the Conti group.

https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/

New Golang Ransomware Agenda Customizes Attacks

Trend Micro recently discovered a new piece of targeted ransomware that was created in the Go programming language and that explicitly targeted one of Trend Micro's customers. This was evidenced by the specific email addresses and credentials the ransomware used.

https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html?&web_view=true

Cisco Patches High-Severity Vulnerabilities in Business Switches

Cisco this week announced patches for two vulnerabilities impacting the NX-OS software that powers its Nexus-series business switches. Tracked as CVE-2022-20824, the bug resides in the Cisco Discovery Protocol feature and impacts the FXOS software as well.

https://www.securityweek.com/cisco-patches-high-severity-vulnerabilities-business-switches

Mozilla Patches High-Severity Vulnerabilities in Firefox, Thunderbird

Mozilla this week patched several high-severity vulnerabilities in its Firefox and Thunderbird products. Firefox 104, as well as Firefox ESR 91.13 and 102.2, patches a high-severity address bar spoofing issue related to XSLT error handling.

https://www.securityweek.com/mozilla-patches-high-severity-vulnerabilities-firefox-thunderbird-0?&web_view=true

Palo Alto Warns of Firewall Vulnerability Used in DDoS Attack on Service Provider

Palo Alto warns of a firewall vulnerability used in a DDoS attack on service provider. Palo Alto Networks is urging customers to patch a line of firewall products after finding that the vulnerability was used in a distributed denial-of-service (DDoS) attack. Palo Alto Networks said it recently learned that an attempted reflected denial-

of-service, a version of a DDoS attack, was identified by a service provider and took advantage of susceptible firewalls from multiple vendors, including Palo Alto Networks.

https://www.therecord.media/palo-alto-warns-of-firewall-vulnerability-used-in-ddos-attack-on-service-provider/