23 Sep 22

Cyber Threat Roundup

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

Contents

Articles

Anonymous Hits Iranian State Sites, Hacks More Than 300 CCTV Cameras

Dubbed “OpIran” (“Operation Iran”) by Anonymous; the hacktivists have taken down a number of top government websites and hacked more than 300 security cameras in different parts of the country. The first major Iranian government institution to suffer a cyberattack from Anonymous hackers was its Forensic Research Center. In the latest attack, Anonymous has claimed to have compromised 300 security camera installations by exploiting a 5.4 severity score vulnerability. Iranian CCTV cameras were apparently controlled by Anonymous. This, however, is not the first time hackers have hacked into CCTV cameras in Iran. Since launching OpIran, Anonymous has carried out a series of DDoS attacks against Iranian state institutions.

https://www.hackread.com/opiran-anonymous-iran-state-sites-cctv-camera-hack/

Fake Banking Rewards Apps Install Info-Stealing RAT on Android Phones

According to Microsoft researchers, malware has been delivered in a currently active SMS campaign in India, masquerading as a banking rewards app. A message contains a malicious link redirecting the user to download a fake banking rewards application. The research team identified many other campaigns targeting Indian bank customers. The fake bank SMS with a malicious link delivers a malicious app that asks for permission, then asks for user data. According to Microsoft’s blog post, what makes this new version different is the inclusion of additional RAT (remote access trojan) capabilities. The malware can steal all SMS messages and other data, such as OTP (one-time-password) and PII (personally identifiable information), to help steal sensitive information associated with email accounts.

https://www.hackread.com/fake-banking-rewards-android-info-stealing-rat/

CISA, Industry Expanding Effort to Secure Operational Technology

When shipping container company Maersk fell victim to a cyber attack in 2017, it cost the company around $300 million, disrupted operations for two weeks, and briefly shut down the largest cargo terminal at the Port of Los Angeles. While not the only attack on operational technology (OT) over the past 10 years, it may have served as a wake-up call to federal agencies whose dependence on OT has made them increasingly vulnerable as infrastructure has evolved into more internet-based systems.

https://federalnewsnetwork.com/cybersecurity/2022/09/cisa-industry-expanding-effort-to-secure-operational-technology/

Researchers Unearth Hacking Group That's Been Active yet Undetected for Years

During a recent investigation of a series of cyber intrusions into an unnamed high-value target, threat intelligence researchers with SentinelOne’s SentinelLabs team discovered nearly ten hacking groups associated with China and Iran.

https://www.cyberscoop.com/researchers-discover-new-hacking-group/

CircleCI, GitHub Users Targeted in Phishing Campaign

CircleCI has sent out a notice to its customers that a phishing email scam is targeting their users, along with GitHub's, in an attempt to harvest credentials. The CircleCI security alert included a copy of the malicious email that attempted to deceive recipients into believing that the companies were working together to launch new terms of service on CircleCI and GitHub accounts.

https://www.darkreading.com/attacks-breaches/circleci-and-github-customers-targeted-phishing-campaign

Palo Alto Networks' 5G-Native Security Now Available on Microsoft Azure Private Multi-Access Edge Compute

Palo Alto Networks, a Microsoft Azure private MEC ecosystem partner, today announced availability of VM-Series Virtual Next-Generation Firewall (NGFW) technology on the Azure Marketplace. Delivering end-to-end Zero Trust security at the enterprise edge, VM-Series virtual firewalls can now extend best-in-class NGFW capabilities to help protect Azure private MEC applications, providing centralized defense against cyberattacks.

https://www.darkreading.com/cloud/palo-alto-networks-5g-native-security-now-available-on-microsoft-azure-private-multi-access-edge-compute

The Auto-Delete Attack

In this attack brief, researchers at Avanan, a Check Point Software company, will discuss how threat actors are compromising accounts, creating more users in an organization to send more attacks, and then auto-deleting emails to cover their tracks.

https://www.avanan.com/blog/the-auto-delete-attack

Australian Telco Company Optus Suffers Data Breach

Australian telecommunications company Optus has suffered an apparent data breach. The breach is believed to be quite large since Optus has nearly 9.7 million customers, but the exact number of accounts that have been affected is unknown at this time. While the collective behind the attack has not been named, it is believed that the incident can be attributed to a state sponsored group, according to *The Guardian*. Access was gained when the group breached the company's firewall, targeting only customer information while leaving day-to-day services unharmed.

https://www.binarydefense.com/threat_watch/australian-telco-company-optus-suffers-data-breach/