5 Aug 22

Cyber Threat Roundup

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

Contents

Articles

Large-scale AiTM Attacks Targeting Enterprise Users to Steal Login Credentials

There has been a phishing campaign exploiting AiTM techniques to conduct a new and large-scale attack. The threat actors use the AiTM technique to bypass multifactor authentication. An HTML attachment is sent to the targets via email containing a phishing URL embedded in it, which when clicked on will take you to a phishing page or website that appears to be a Microsoft Office login screen with a Microsoft Office logo on it.

https://cybersecuritynews.com/large-scale-aitm-attacks-targeting-enterprise/

New Linux Malware Brute-forces SSH Servers to Breach Networks

A new botnet called “RapperBot” has been used in attacks since mid-June 2022, focusing on brute-forcing its way into Linux SSH servers to establish a foothold on the device. RapperBot proved to be a Mirai fork, but with its own command and control (C2) protocol, unique features, and atypical (for a botnet) post-compromise activity.

https://www.bleepingcomputer.com/news/security/new-linux-malware-brute-forces-ssh-servers-to-breach-networks/

GwisinLocker Ransomware Targets South Korean Industrial and Pharma Firms

Taking its name from “Gwisin”, a Korean term for “ghost” or “spirit”, “GwisinLocker” is a new ransomware family that targets South Korean industrial and pharmaceutical companies. ReversingLabs researchers discovered a new ransomware family targeting Linux-based systems. The malware, dubbed “GwisinLocker”, was detected in successful campaigns targeting South Korean industrial and pharmaceutical firms.

https://securityboulevard.com/2022/08/gwisinlocker-ransomware-targets-south-korean-industrial-and-pharma-firms/

Disruptive Cyberattacks on NATO Member Albania Linked to Iran

The recent cyberattacks that disrupted government systems in NATO member Albania have been linked by threat intelligence giant Mandiant to Iran. The ransomware has been named “Roadsweep”. While they could not confirm that the ransomware was indeed used in the attack, the malware encrypts files on compromised systems and then drops a ransom note suggesting that its target is the Albanian government.

https://www.securityweek.com/disruptive-cyberattacks-nato-member-albania-linked-iran/