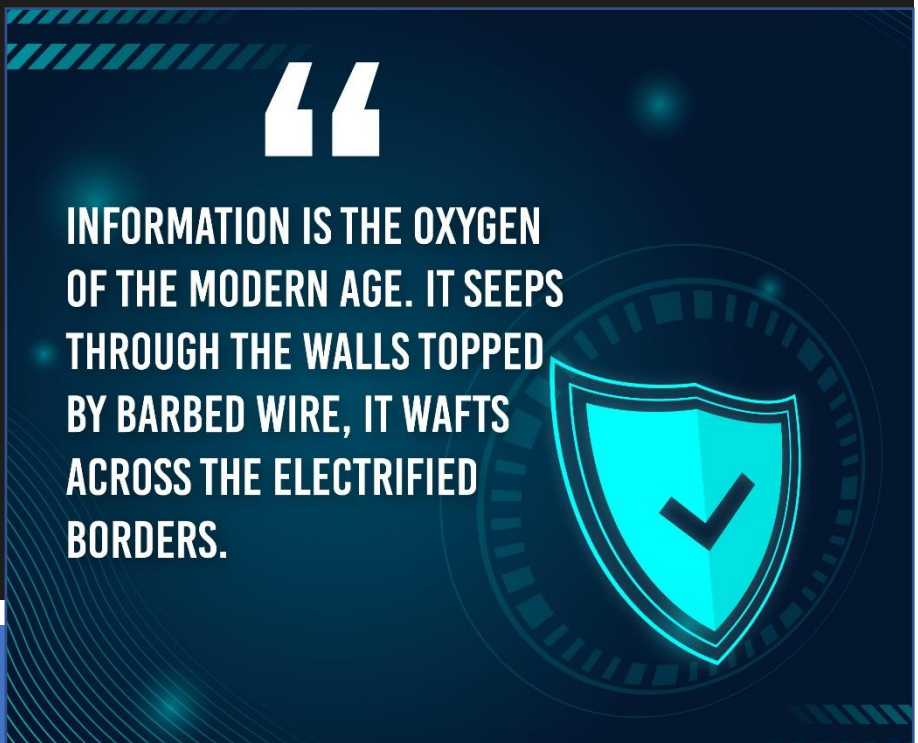
flatworld solutions®

Infopercept

INFOPERCEPT NEWSLETTER

ISSUE -16 August 2021

Contents



Patches Notes

NINE CRITICAL AND HIGH-SEVERITY VULNERABILITIES PATCHED IN SAP PRODUCTS

- Two cross-site scripting (XSS) weaknesses and an SSRF flaw in NetWeaver Enterprise Porta are among the high-severity vulnerabilities addressed by SAP.
- An authentication flaw impacting all SAP systems accessible through a Web Dispatcher, a task hijacking hole in the Fiori Client mobile app for Android, and a missing authentication flaw in SAP Business One are among the other high-severity vulnerabilities.

MICROSOFT AUGUST 2021 PATCH TUESDAY FIXES 3 ZERO-DAYS, 44 FLAWS

- With today's update, Microsoft has patched 44 vulnerabilities (51 of which are related to Microsoft Edge), seven of which are classed as critical and 37 as important.
- Thirteen of the 44 flaws are remote code execution flaws, eight are information disclosure flaws, two are denial of service flaws, and four are spoofing flaws.

PULSE SECURE VPNS GET NEW URGENT UPDATE FOR POORLY PATCHED CRITICAL FLAW

- To address an insufficient patch for an actively exploited hole, Pulse Secure has released a fix for a major post-authentication remote code execution (RCE) vulnerability in its Connect Secure virtual private network (VPN) appliances.
- An uncontrolled archive extraction vulnerability in the Pulse Connect Secure appliance allows an attacker to overwrite arbitrary files, resulting in Remote Code Execution as root.

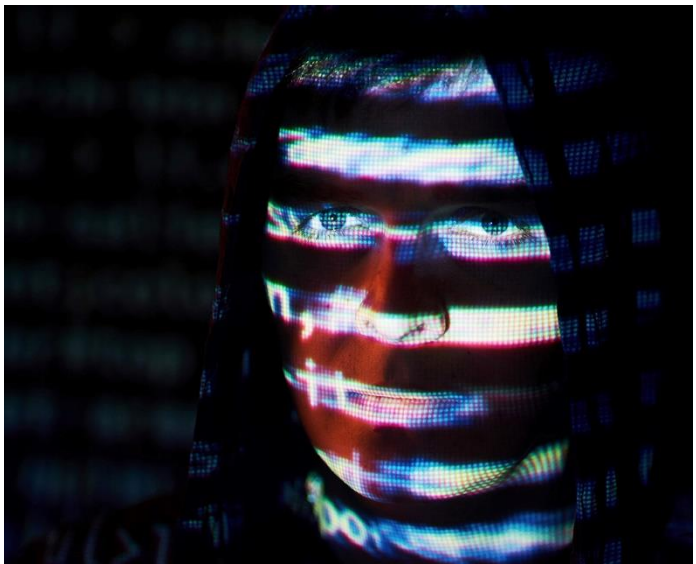
CYBER ATTACKS

CRYTEK CONFIRMS EGREGOR RANSOMWARE ATTACK, CUSTOMER DATA THEFT

- In breach notification letters issued to impacted individuals earlier this month, the corporation admitted the attack, which was revealed with Bleeping Computer today by one of the victims.
- Crytek also believes that people who attempted to download the stolen material were put off by the "high risk" of malware encoded in the documents corrupting their systems.

KASEYA'S UNIVERSAL REVIL DECRYPTION KEY LEAKED ON A HACKING FORUM

- An REvil decryptor was operating while presenting a base64 hashed'master sk' key, according to a screenshot on GitHub.
- When victims of REvil ransomware pay the ransom, they receive either a decryptor for a single encrypted file extension or a universal decryptor for all encrypted file extensions used in the campaign or attack.



CROSS-CHAIN DEFI SITE POLY NETWORK HACKED; HUNDREDS OF MILLIONS POTENTIALLY LOST

- Poly Network is a protocol that runs on the Binance Smart Chain, Ethereum, and Polygon blockchains, and was created by the founder of the Chinese blockchain project Neo.
- The hacker attempted to shift assets including USDT through the Ethereum address into liquidity pool Curve.fi around an hour after Poly declared the hack on Twitter, according to records. The deal was turned down.

Malware and Vulnerabilities

NEW ADLOAD MALWARE VARIANT SLIPS THROUGH APPLE'S XPROTECT DEFENSES

- Apple's YARA signature-based XProtect built-in antivirus technology is allowing a new AdLoad malware version to infect Macs as part of several campaigns.
- AdLoad will install a Man-in-the-Middle (MiTM) web proxy once it has infected a Mac in order to hijack search engine results and inject adverts into online pages for monetary benefit.

PROXYSHELL - ANOTHER MS EXCHANGE FLAW GAINING TRACTION AMONG ATTACKERS

- The Client Access Service (CAS), which runs on IIS on port 443, can be used to exploit the newly revealed vulnerabilities in Microsoft Exchange servers. The Autodiscover service and the Exchange PowerShell backend were among the components of Exchange Servers targeted by the attack chain.
- The attackers have continued to tweak and fine-tune their attack exploit. In addition, the attacker was seen using an auto-discovery tool to check for vulnerable exchange servers with a fresh request.

A FLAW WITH DNSAAS PROVIDERS EXPLOITED FOR INTELLIGENCE GATHERING

- Cybercriminals were able to steal sensitive information from corporate networks because to a DNS vulnerability affecting popular DNS-as-a-Service (DNSaaS) providers.
- A small portion of dynamic DNS traffic passing through managed DNS providers such as Amazon and Google could be intercepted by hackers. To take advantage of the weakness, attackers had to establish a domain and hijack a DNSaaS provider's...

XMRIG-BASED CRYPTOMINING WORM WITH 15% SPEED BOOST

- A new strain of the Golang crypto-worm has been discovered spreading Monero-mining malware to computers. The crypto-worm is based on XMRig and takes use of known web server flaws.
- The worm examines Unix and Linux-based web servers for known vulnerabilities, such as Oracle WebLogic Server or XML-RPC Server. Furthermore, the payload binaries have the ability to reduce the mining time by 15%.

CYBER TECH

DBREACH: A NEW ATTACK AGAINST DATABASES

- DBREACH is thought to be the first database system compression side-channel attack. An attacker can recover encrypted data using the DBREACH attack technique.
- A web interface can be used to update or insert the database table. Furthermore, with only a partial-select ability, the attacker can get the required rights.

FIREFOX 91 PRIVATE BROWSING HTTPS FEATURE

- Firefox will enable HTTPS by default in Private Browsing mode, Confirmed by Mozilla.
- It's when a user enters an insecure (HTTP) URL in Firefox's address bar, or clicks on an insecure link on a web page, Firefox will now first try to establish a secure, encrypted HTTPS connection to the specified website.

ENFILADE: OPEN-SOURCE RANSOMWARE FLAG TOOL

- An open-source tool that detects internet-facing MongoDB instances and whether they've been infected with ransomware or Meow malware has been launched.
- Which is primarily focused on the network service for MongoDB communication started on TCP port 27017

Infopercept

ABOUT INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

DISASTER RECOVERY AUTOMATION

In today's day and age, a company's online presence and operational consistency are the central components contributing to its marketing, branding, revenue generation, information, lead generation, sales and overall business. There is little doubt then, that most companies who want to succeed in this competitive market have to invest wisely and proactively into the stability and continuation of its business's critical-function apps.

Given the importance and benefit of digital business operations for the success of a business you would ideally want it to continue unabated so that you can perform your daily business operations conveniently. Due to this, the demand for DR automation is growing as businesses are looking for ways to reduce their operational downtime. A disaster recovery plan helps you achieve this very important task, by allowing you to continue or quickly resume and kickstart important business operations and functions in the event of a disaster happening.