

### CCDS CYBER SECURITY PICKS

41st Release August 2022



# FBI Warns Investors to Take Precautions with Decentralized Financial Platforms

The U.S. Federal Bureau of Investigation (FBI) on Monday warned of cyber criminals increasingly exploiting flaws in decentralized finance (DeFi) platforms to plunder cryptocurrency.

"The FBI has observed cyber criminals exploiting vulnerabilities in the smart contracts governing DeFi platforms to steal investors' cryptocurrency," the agency said in a notification

Source: https://thehackernews.com/ 2022/08/fbi-warns-investors-totake-precautions.html



#### New Golang-based 'Agenda Ransomware' Can Be Customized For Each Victim

A new ransomware strain written in Golang dubbed "Agenda" has been spotted in the wild, targeting healthcare and education entities in Indonesia, Saudi Arabia, South Africa, and Thailand.

"Agenda can reboot systems in safe mode, attempts to stop many server-specific processes and services, and has multiple modes to run," Trend Micro researchers said in an analysis last week.

Source: https://thehackernews.com/2 022/08/new-golang-based-agendaransomware-can.html

1010100100101001F10100100101001	01010016016IBC1010100100100
1000000110100 100000011010001	100 00011010301159 100110100011
010101001001101 010100100110 0001	0 30100170100010100100
10011101011111101001110 01111101001	11010111110190111010111111010011
110110111111000101010101111100010101	1011111000101010111111000101011
1111011110110011111011110111101111	10111101100111111011110110611111
1101010001000100101010001000100010101	01000100010010101010001000100101010
10010111110100010010111110101001001	0111110100010010111110100010010
1010100000001101010100000001101010	100000001101013100000001101010101
1900811100101001080011100101001000	0111001010010009111051010010000
0001110011100000001110011100000001	1100111000009011100111000000011
100111000001001001110000010001001	1100000100010011100300102010011
0210818181811100011081010101101000110	010101011000110010101010110001100
1001100G111D1 <b>0000</b> 01100011101000001	100011101090001100811181000031
3000166116881 <b>60000</b> 6100110001000000	10011000100000001001100010000001
3016016161111101001901010111101010	0101511110 <b>100100X<del>01</del>01111101</b> 00100
3808218152115 <b>0189</b> 30010100110010000	0101001100100000101BGIIBGIBGOCC
00111111111111111111111111111111111111	1111001010000111111001010000111
11111521BBBB <b>60</b> 0111110110000000111	11011000000011111011080808681111
00110000001110 <b>0</b> 10011000001110010011	00000111001001100000111100100110
1001001000111001001001001001	00:0001110010010010061110010010
011111111111111111111111111111111111111	111101011011011111111111111111111111111
01 10 01 10 11 10	11001101110111011001101111

## Okta Hackers Behind Twilio and Cloudflare Breach Hit Over 130 Organizations

The threat actor behind the attacks on Twilio and Cloudflare earlier this month has been linked to a broader phishing campaign aimed at 136 organizations that resulted in a cumulative compromise of 9,931 accounts.

The activity has been condemned Oktapus by Group-IB because the initial goal of the attacks was to "obtain Okta identity credentials and two-factor authentication (2FA) codes from users of the targeted organizations."

Source: https://thehackernews.com/ 2022/08/okta-hackers-behindtwilio-and.html





#### Researchers Warn of AiTM **Attack Targeting Google G-Suite Enterprise Users**

The threat actors behind a largescale adversary-in-the-middle (AiTM) phishing campaign targeting enterprise users of Microsoft email services have also set their sights on Google Workspace users."This campaign specifically targeted chief executives and other senior members of various organizations which use [Google Workspace]," Zscaler researchers Sudeep Singh and Jagadeeswar Ramanukolanu detailed in a report published this month.

Source: https://thehackernews.co m/2022/08/researchers-warn-ofaitm-attack.html

#### **CISA Warns of Active Exploitation of Palo Alto Networks' PAN-OS Vulnerability**

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a security flaw impacting Palo Alto Networks PAN-OS to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. The high-severity vulnerability, tracked as CVE-2022-0028 (CVSS score: 8.6), is a URL filtering policy misconfiguration that could allow an unauthenticated, remote attacker to carry out reflected and amplified TCP denial-of-service (DoS) attacks

Source:https://thehackernews.co m/2022/08/cisa-warns-of-activeexploitation-of.html

#### The Rise of Data Exfiltration and Why It Is a **Greater Risk Than Ransomware**

Ransomware is the de facto threat organizations have faced over the past few years. Threat actors were making easy money by exploiting the high valuation of cryptocurrencies and their victims' lack of adequate preparation.

Think about bad security policies, untested backups, patch management practices not up-to-par, and so forth. It resulted in easy growth for ransomware extortion, a crime that multiple threat actors around the world perpetrate.

Something's changed, though. Crypto valuations have dropped, reducing the monetary appeal of ransomware attacks due to organizations mounting a formidable defense against ransomware.

Source: https://thehackernews.com/2022/08/the-rise-ofdata-exfiltration-and-why.html

#### Microsoft Issues Patches for 121 Flaws, **Including Zero-Day Under Active Attack**

As many as 121 new security flaws were patched by Microsoft as part of its Patch Tuesday updates for the month of August, which also includes a fix for a Support Diagnostic Tool vulnerability that the company said is being actively exploited in the wild.

Of the 121 bugs, 17 are rated Critical, 102 are rated Important, one is rated Moderate, and one is rated Low in severity. Two of the issues have been listed as publicly known at the time of the release.

Topping the list of patches is CVE-2022-34713 (CVSS score: 7.8), a case of remote code execution affecting the Microsoft Windows Support Diagnostic Tool (MSDT)

Source: https://thehackernews.com/2022/08/microsof t-issues-patches-for-121-flaws.html



Cloud Consultancy for Digitalization & Security - CCDS's is a Specialized Company in IT and Information Security Services, which has its international headquarters in the UAE. It also has branch offices throughout the MENA Region with its premier office in Saudi Arabia. Innovative and professional in its approach, it always partners with best-in-class products and services, to identify and solve security threats and issues for its clients.

Contact Us











