Cloud
Consultancy
For Digitalization & Security

CCDS CYBER SECURITY PICKS

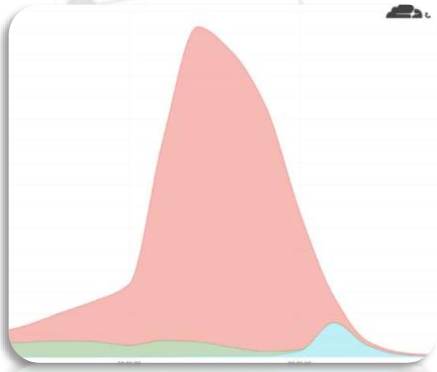
37th Release April 2022

Cybercriminals Using New Malware Loader 'Bumblebee' in the Wild

Cybercriminal actors previously observed delivering BazaLoader and IcedID as part of their malware campaigns are said to have transitioned to a new loader called Bumblebee that's under active development.

"Threat actors using Bumblebee are associated with malware payloads that have been linked to follow-on ransomware campaigns," the researchers said.

Source:
https://thehackernews.com/2022/04/cybercriminals-using-new-malware-loader.html

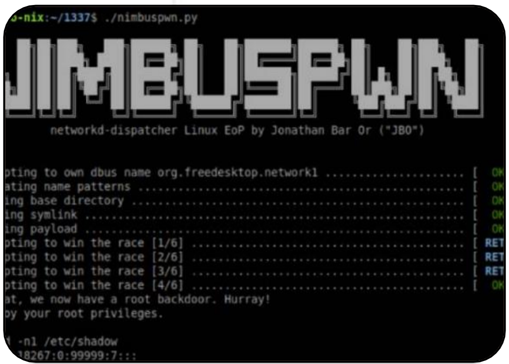


Cloudflare Thwarts Record DDoS Attack Peaking at 15 Million Requests Per Second

Cloudflare on Wednesday disclosed that it acted to mitigate a 15.3 million request-per-second (RPS) distributed denial-of-service (DDoS) attack. The web infrastructure and website security company called it one of the "largest HTTPS DDoS attacks on record."

The volumetric DDoS attack is said to have lasted less than 15 seconds and targeted an unnamed Cloudflare customer operating a crypto launchpad.

Source:
https://thehackernews.com/2022/04/cloudflare-thwarts-record-ddos-attack.html



```
o-nix:~/1337$ ./nimbuspwn.py
JIMBUSPWN
        networkd-dispatcher Linux EoP by Jonathan Bar Or ("JBO")

pting to own dbus name org.freedesktop.network1 ..................... [  OK
ating name patterns ................................................. [  OK
ing base directory .................................................. [  OK
ing symlink ......................................................... [  OK
ing payload ......................................................... [  OK
pting to win the race [1/6] ......................................... [ RET
pting to win the race [2/6] ......................................... [ RET
pting to win the race [3/6] ......................................... [ RET
pting to win the race [4/6] ......................................... [  OK
at, we now have a root backdoor. Hurray!
oy your root privileges.

d -n1 /etc/shadow
18267:0:99999:7:::
```

Microsoft Discovers New Privilege Escalation Flaws in Linux Operating System

Microsoft on Tuesday disclosed a set of two privilege escalation vulnerabilities in the Linux operating system that could potentially allow threat actors to carry out an array of nefarious activities.

Collectively called "Nimbuspwn," the flaws "can be chained together to gain root privileges on Linux systems, allowing attackers to deploy payloads, like a root backdoor, and perform other malicious actions via arbitrary root code execution," Jonathan Bar Or of the Microsoft 365 Defender Research Team said in a report.

Source:
https://thehackernews.com/2022/04/microsoft-discovers-new-privilege.html

Emotet Testing New Delivery Ideas After Microsoft Disables VBA Macros by Default

The threat actor behind the prolific Emotet botnet is testing new attack methods on a small scale before co-opting them into their larger volume malspam campaigns, potentially in response to Microsoft's move to disable Visual Basic for Applications (VBA) macros by default across its products.

Source: https://thehackernews.com/2022/04/emotet-testing-new-delivery-ideas-after.html

Iranian Hackers Exploiting VMware RCE Bug to Deploy 'Core Impact' Backdoor

An Iranian-linked threat actor known as Rocket Kitten has been observed actively exploiting a recently patched VMware vulnerability to gain initial access and deploy the Core Impact penetration testing tool on vulnerable systems.

Tracked as CVE-2022-22954 (CVSS score: 9.8), the critical issue concerns a case of remote code execution (RCE) vulnerability affecting VMware Workspace ONE Access and Identity Manager.

Source: https://thehackernews.com/2022/04/iranian-hackers-exploiting-vmware-rce.html

FBI Warns of BlackCat Ransomware That Breached Over 60 Organisations Worldwide

The U.S. Federal Bureau of Investigation (FBI) is sounding the alarm on the BlackCat ransomware-as-a-service (RaaS), which it said victimized at least 60 entities worldwide between as of March 2022 since its emergence last November.

Also called ALPHV and Noberus, the malware is notable for being the first-ever ransomware written in the Rust programming language, which is known to be memory safe and offer improved performance.

Source: https://thehackernews.com/2022/04/fbi-warns-of-blackcat-ransomware-that.html

Five Eyes Nations Warn of Russian Cyber Attacks Against Critical Infrastructure

The Five Eyes nations have released a joint cybersecurity advisory warning of increased malicious attacks from Russian state-sponsored actors and criminal groups targeting critical infrastructure organizations amidst the ongoing military siege on Ukraine.

"Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks," authorities from Australia, Canada, New Zealand, the U.K., and the U.S. said.

Source: https://thehackernews.com/2022/04/five-eyes-nations-warn-of-russian-cyber.html

Cloud Consultancy
For Digitalization & Security

Contact Us

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.