Cloud
Consultancy
For Digitalization & Security

CCDS CYBER SECURITY PICKS

38th Release May 2022

Experts Detail New RCE Vulnerability Affecting Google Chrome Dev Channel

Details have emerged about a recently patched critical remote code execution vulnerability in the V8 JavaScript and WebAssembly engine used in Google Chrome and Chromium-based browsers.

The issue relates to a case of use-after-free in the instruction optimization component, successful exploitation of which could "allow an attacker to execute arbitrary code in the context of the browser."

Source: https://thehackernews.com/2022/05/experts-detail-new-rce-vulnerability.html

Hackers Trick Users with Fake Windows 11 Downloads to Distribute Vidar Malware

Fraudulent domains masquerading as Microsoft's Windows 11 download portal are attempting to trick users into deploying trojanized installation files to infect systems with the Vidar information stealer malware.

"The spoofed sites were created to distribute malicious ISO files which lead to a Vidar info-stealer infection on the endpoint," Zscaler said in a report.

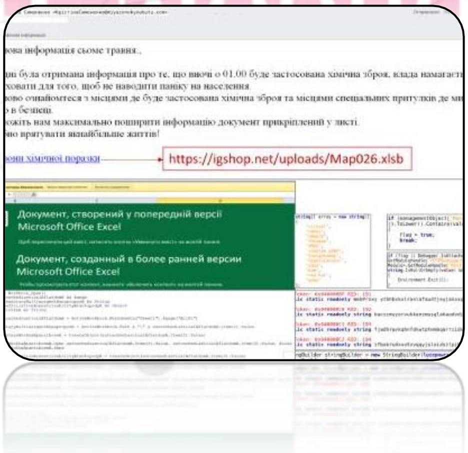
Source: https://thehackernews.com/2022/05/hackers-trick-users-with-fake-windows.html

U.S. Proposes $1 Million Fine on Colonial Pipeline for Safety Violations After Cyberattack

The U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) has proposed a penalty of nearly $1 million to Colonial Pipeline for violating federal safety regulations, worsening the impact of the ransomware attack last year.

The $986,400 penalty is the result of an inspection conducted by the regulator of the pipeline operator's control room management (CRM) procedures from January through November 2020.

Source: https://thehackernews.com/2022/05/us-proposes-1-million-fine-on-colonial.html



нова інформація сьоме травня.,

ція була отримана інформація про те, що вночі о 01.00 буде застосована хімічна зброя, влада намагаєт
ховати для того, щоб не наводити паніку на населення.
ново ознайомтеся з місцями де буде застосована хімічна зброя та місцями спеціальних притулків де ми
о в безпеці.
можіть нам максимально поширити інформацію документ прикріплений у листі.
ємо врятувати якнайбільше життів!

зони хімічної поразки → https://igshop.net/uploads/Map026.xlsb

Документ, створений у попередній версії Microsoft Office Excel

Документ, созданный в более ранней версии Microsoft Office Excel

T-Mobile Admits Lapsus$ Hackers Gained Access to its Internal Tools and Source Code

Telecom company T-Mobile on Friday confirmed that it was the victim of a security breach in March after the LAPSUS$ mercenary gang managed to gain access to its networks.

T-Mobile, in a statement, said that the incident occurred "several weeks ago, with the "bad actor" using stolen credentials to access internal systems.

Source: https://thehackernews.com/2022/04/t-mobile-admits-lapsus-hackers-gained.html

Ukrainian CERT Warns Citizens of a New Wave of Attacks Distributing Jester Malware

The Computer Emergency Response Team of Ukraine (CERT-UA) has warned of phishing attacks that deploy an information-stealing malware called Jester Stealer on compromised systems.

The mass email campaign carries the subject line "chemical attack" and contains a link to a macro-laced Microsoft Excel file, opening which leads to computers getting infected with Jester Stealer.

Source: https://thehackernews.com/2022/05/ukrainian-cert-warns-citizens-of-new.html

How to Protect Your Data When Ransomware Strikes

Ransomware is not a new attack vector. In fact, the first malware of its kind appeared more than 30 years ago and was distributed via 5.25-inch floppy disks. To pay the ransom, the victim had to mail money to a P.O. Box in Panama.

A ransomware attack isn't just a single event; it's a persistent threat. To secure your organization, you need a full picture of what is happening with your endpoints, users, apps and data.

Step-by-step: how to protect against ransomware

1 — Block phishing attacks and cloak web-enabled apps
2 — Detect and respond to anomalous behaviors
3 — Render data useless for ransom with proactive encryption

Source: https://thehackernews.com/2022/05/how-to-protect-your-data-when.html

The Myths of Ransomware Attacks and How to Mitigate Risk

As organizations continue to evolve, in turn so does ransomware. To help you stay ahead, Lookout Chief Strategy Officer, Aaron Cockerill met with Microsoft Chief Security Advisor, Sarah Armstrong-Smith to discuss how remote work and the cloud have made it more difficult to spot a ransomware attack, as well as how deploying behavioral-anomaly-based detection can help mitigate ransomware risk. Access the full interview.

The first step to securing data is knowing what's going on. It's hard to see the risks you're up against when your users are everywhere and using networks and devices you don't control to access sensitive data in the cloud.
Source: https://thehackernews.com/2022/05/the-myths-of-ransomware-attacks-and-how.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.