# CCDS CYBER SECURITY PICKS

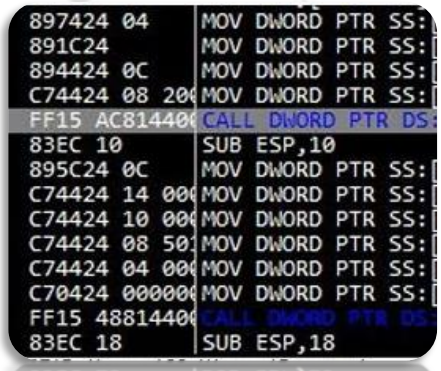
35th Release February 2022

## New Wiper Malware Targeting Ukraine Amid Russia's Military Operation

Cybersecurity firms ESET and Broadcom's Symantec said they discovered a new data wiper malware used in fresh attacks against hundreds of machines in Ukraine, as Russian forces formally launched a full-scale military operation against the country.

The Slovak company dubbed the wiper "HermeticWiper" (aka KillDisk.NCV), with one of the malware samples compiled on December 28, 2021, implying that preparations for the attacks may have been underway for nearly two months.

Source:
https://thehackernews.com/2022/02/new-wiper-malware-targeting-ukraine.html




## Hackers Backdoor Unpatched Microsoft SQL Database Servers with Cobalt Strike

Vulnerable internet-facing Microsoft SQL (MS SQL) Servers are being targeted by threat actors as part of a new campaign to deploy the Cobalt Strike adversary simulation tool on compromised hosts.

"Attacks that target MS SQL servers include attacks to the environment where its vulnerability has not been patched, brute forcing, and dictionary attack against poorly managed servers," South Korean cybersecurity company AhnLab Security Emergency Response Center (ASEC) said in a report published Monday.

Source:
https://thehackernews.com/2022/02/hackers-backdoor-unpatched-microsoft.html

## Iran's MuddyWater Hacker Group Using New Malware in Worldwide Cyber Attacks

Cybersecurity agencies from the U.K. and the U.S. have laid bare a new malware used by the Iranian government-sponsored advanced persistent threat (APT) group in attacks targeting government and commercial networks worldwide.

"MuddyWater actors are positioned both to provide stolen data and accesses to the Iranian government and to share these with other malicious cyber actors," the agencies said.

Source:
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html


## VMware Issues Security Patches for High-Severity Flaws Affecting Multiple ProductsCybersecurity

VMware on Tuesday patched several high-severity vulnerabilities impacting ESXi, Workstation, Fusion, Cloud Foundation, and NSX Data Center for vSphere that could be exploited to execute arbitrary code and cause a denial-of-service (DoS) condition.

Source: https://thehackernews.com/2022/02/vmware-issues-security-patches-for-high.html

## New Chrome 0-Day Bug Under Active Attack – Update Your Browser ASAP!

Google on Monday rolled out fixes for eight security issues in the Chrome web browser, including a high-severity vulnerability that's being actively exploited in real-world attacks, marking the first zero-day patched by the internet giant in 2022.

The shortcoming, tracked CVE-2022-0609, , if successfully exploited, could lead to corruption of valid data and the execution of arbitrary code on affected systems.

Source: https://thehackernews.com/2022/02/new-chrome-0-day-bug-under-active.html

## U.S. Cybersecurity Agency Publishes List of Free Security Tools and Services

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday published a repository of free tools and services to enable organizations to mitigate, detect, and respond effectively to malicious attacks and further improve their security posture.

The "Free Cybersecurity Services and Tools" resource hub comprises a mix of 101 services provided by CISA, open-source utilities, and other implements offered by private and public sector organizations across the cybersecurity community.

"Malicious actors may use tactics — such as misinformation, disinformation, and malinformation —" CISA said.

Source: https://thehackernews.com/2022/02/us-cybersecurity-agency-publishes-list.html

## 4 Cloud Data Security Best Practices All Businesses Should Follow Today

These days, businesses all around the world have come to depend on cloud platforms for a variety of mission-critical workflows. They keep their CRM data in the cloud. They process their payrolls in the cloud. They even manage their HR processes through the cloud. And all of that means they're trusting the bulk of their privileged business data to those cloud providers, too.

And while most major cloud providers do a decent job of keeping data secure, the majority of business users take an upload-it-and-forget-it approach to their data security needs. And that — needless to say — is dangerous.

Source: https://thehackernews.com/2022/02/4-cloud-data-security-best-practices.html

Cloud Consultancy

*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.**