

THREAT INTEL INSIGHTS


OCTOBER 2022



1

MICROSOFT CONFIRMED 'BLUEBLEED' DATA LEAK

Microsoft announced that a misconfigured Microsoft server accessible through the Internet exposed some of its customers' sensitive information. The exposed information includes names, email addresses, email content, company name, and phone numbers, as well as data related to business between impacted customers and Microsoft or a Microsoft-authorized partner.



2

WHOLESALE GIANT METRO HIT BY A CYBERATTACK, SUFFERS IT OUTAGE

The global wholesale giant METRO suffered infrastructure problems and issues with store payments following a recent cyberattack. The IT infrastructure was affected in all Metro Cash & Carry wholesale stores for food service purchases due to the attack. Metro employs around 95,000 people in 681 stores globally, the majority of which are in Germany.

3

DAIXIN TEAM TARGETING HEALTH ORGANIZATIONS WITH RANSOMWARE

The Daixin Team cybercrime gang is actively pursuing ransomware operations against U.S. companies, mostly in the Healthcare and Public Health (HPH) Sector. The group concentrated its ransomware activities on the HPH Sector with the goal of distributing ransomware, exfiltrating patient health information (PHI), and threatening to reveal the stolen data if a ransom is not paid.

4

WITCHETTY APT GROUP HIDES BACKDOOR MALWARE IN WINDOWS LOGO

The Witchetty cyber espionage threat actor group employed steganography to conceal backdoor malware in the Windows logo in its latest campaign. The gang attacked governments in the Middle East through the backdoor. Witchetty is believed to have close links to the Chinese threat actor APT10.

5

MICROSOFT EXCHANGE ZERO-DAY ACTIVELY EXPLOITED IN THE WILD

Microsoft verified that two zero-day vulnerabilities in Microsoft Exchange discovered by researchers are being actively exploited in the wild. The first flaw, tracked as CVE-2022-41040, is a Server-Side Request Forgery (SSRF) issue. The second vulnerability, tracked as CVE-2022-41082, allows remote code execution (RCE) when PowerShell is accessible to the attacker.

6

COMM100 CHAT PROVIDER HACKED TO SPREAD MALWARE IN SUPPLY CHAIN ATTACK

A threat actor with ties to China has been attributed to a novel supply chain attack involving the deployment of a trojanized installer for the Comm100 Live Chat application to distribute a JavaScript backdoor. The attacker used a signed Comm100 desktop agent program for Windows that could be downloaded from the company's website.

7

SOPHISTICATED COVERT ATTACK CAMPAIGN TARGETING MILITARY CONTRACTORS

A recent cyberattack campaign motivated by cyber espionage targeted many military and weapons contractor businesses using spear-phishing emails to start a multi-stage infection process meant to deliver an unidentified payload on infected workstations. This campaign has targeted many European weapons firms, including a potential supplier to the US F-35 Lightning II fighter aircraft programs.