News from Tuesday, February 13, 2024. Reported on Wednesday, February 14, 2024.

Live links are embedded throughout today's briefing. To see the actual URL, hover your mouse over the link for a moment before clicking. These links were copied directly from the web site of the source article. Tyler Cybersecurity has not performed any testing on the sites / links for security.

Sources	Articles
CISA	**CISA Adds Two Known Exploited Vulnerabilities to Catalog** CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. ▪ CVE-2024-21412 Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability ▪ CVE-2024-21351 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the Known Exploited Vulnerabilities Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for more information. **CISA Releases One Industrial Control Systems Advisory** CISA released one Industrial Control Systems (ICS) advisory on February 13, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ▪ ICSA-24-044-01 Mitsubishi Electric MELSEC iQ-R Series Safety CPU
Bleeping Computer	**Prudential Financial breached in data theft cyberattack** Prudential Financial has disclosed that its network was breached last week, with the attackers stealing employee and contractor data before being blocked from compromised systems one day later. This leading global financial services Fortune 500 company manages roughly $1.4 trillion in assets, and it provides insurance, retirement planning, as well as wealth and investment management services to over 50 million customers across the United States, Asia, Europe, and Latin America. As the second-largest life insurance company in the U.S., it employs 40,000 people worldwide and reported revenues of more than $50 billion in 2023. **Hackers used new Windows Defender zero-day to drop DarkMe malware** Today Microsoft has patched a Windows Defender SmartScreen zero-day exploited in the wild by a financially motivated threat group to deploy the DarkMe remote access trojan (RAT). The hacking group (tracked as Water Hydra and DarkCasino) was spotted using the zero-day (CVE-2024-21412) in attacks on New Year's Eve day by Trend Micro security researchers. "An unauthenticated attacker could send the targeted user a specially crafted file that is designed to bypass displayed security checks," Microsoft said in a security advisory issued today. "However, the attacker would have no way to force a user to view the attacker-controlled content. Instead, the attacker would have to convince them to take action by clicking on the file link."

Sources	Articles
	Trend Micro security researcher Peter Girnus, credited for reporting this zero-day, revealed that the CVE-2024-21412 flaw bypasses another Defender SmartScreen vulnerability (CVE-2023-36025). CVE-2023-36025 was patched during the November 2023 Patch Tuesday, and, as Trend Micro revealed last month, it was also exploited to bypass Windows security prompts when opening URL files to deploy the Phemedrone info-stealer malware. **200,000 Facebook Marketplace user records leaked on hacking forum** A threat actor leaked 200,000 records on a hacker forum, claiming they contained the mobile phone numbers, email addresses, and other personal information of Facebook Marketplace users. BleepingComputer verified some of the leaked data by matching the email addresses and phone numbers on random records within the sample data shared by IntelBroker, the threat actor who leaked the data online. A Meta spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today. **Integris Health says data breach impacts 2.4 million patients** Integris Health has reported to U.S. authorities that the data breach it suffered last November exposed personal information belonging to almost 2.4 million people. The organization is Oklahoma's largest not-for-profit healthcare network, operating hospitals, clinics, and emergency care units across the state. On December 26, 2023, the organization confirmed it suffered a cyberattack after patients started receiving extortion emails informing that their sensitive personal information. Unless Integris Health met the attacker's demands, the stolen data would be sold to other cybercriminals on January 5, 2024. The emails the patients received from the threat actor contained accurate information and linked to a website in the Tor network hosting the stolen details, but access was not free. Visitors could pay $50 and trust the attacker's word on removing the details or pay $3 to view information belonging to any other impacted individual.
The Hacker News	**PikaBot Resurfaces with Streamlined Code and Deceptive Tactics** The threat actors behind the PikaBot malware have made significant changes to the malware in what has been described as a case of "devolution." "Although it appears to be in a new development cycle and testing phase, the developers have reduced the complexity of the code by removing advanced obfuscation techniques and changing the network communications," Zscaler ThreatLabz researcher Nikolaos Pantazopoulos said. PikaBot, first documented by the cybersecurity firm in May 2023, is a malware loader and a backdoor that can execute commands and inject payloads from a command-and-control (C2) server as well as allow the attacker to control the infected host. **Bumblebee Malware Returns with New Tricks, Targeting U.S. Businesses** The infamous malware loader and initial access broker known as Bumblebee has resurfaced after a four-month absence as part of a new phishing campaign observed in February 2024. Enterprise security firm Proofpoint said the activity targets organizations in the U.S. with voicemail-themed lures containing links to OneDrive URLs. "The URLs led to a Word file with names such as "ReleaseEvans#96.docm" (the digits before the file extension varied)," the company said in a Tuesday report. "The Word document spoofed the consumer electronics company Humane."

Sources	Articles
	Opening the document leverages VBA macros to launch a PowerShell command to download and execute another PowerShell script from a remote server that, in turn, retrieves and runs the Bumblebee loader. **Ubuntu 'command-not-found' Tool Could Trick Users into Installing Rogue Packages** Cybersecurity researchers have found that it's possible for threat actors to exploit a well-known utility called command-not-found to recommend their own rogue packages and compromise systems running Ubuntu operating system. "While 'command-not-found' serves as a convenient tool for suggesting installations for uninstalled commands, it can be inadvertently manipulated by attackers through the snap repository, leading to deceptive recommendations of malicious packages," cloud security firm Aqua said in a report shared with The Hacker News. Installed by default on Ubuntu systems, command-not-found suggests packages to install in interactive bash sessions when attempting to run commands that are not available. The suggestions include both the Advanced Packaging Tool (APT) and snap packages. When the tool uses an internal database ("/var/lib/command-not-found/commands.db") to suggest APT packages, it relies on the "advise-snap" command to suggest snaps that provide the given command.
InfoSecurity Magazine	**Microsoft Fixes Two Zero-Days in February Patch Tuesday** Microsoft has landed system administrators with a busy February after releasing updates for 73 vulnerabilities, including two zero-day flaws currently under active exploitation. February's Patch Tuesday update round yesterday saw fixes for five critical vulnerabilities and 30 remote code execution (RCE) flaws. However, both zero-days were security feature bypass bugs. The first, CVE-2024-21412, is related to Internet Shortcut Files. With a CVSS score of 8.1, it is only rated as "important" as it requires user interaction to be successful, according to Mike Walters, president of Action1. The second zero-day (CVE-2024-21351) involves bypassing the SmartScreen security feature in Microsoft Defender. It is rated as having a moderate impact, with a CVSS score of 7.6. Although it's being exploited in the wild, there's currently no proof-of-concept available, according to Walters.
Dark Reading	**Glupteba Botnet Adds UEFI Bootkit to Cyberattack Toolbox** The widespread, multitooled Glupteba malware has adopted a Unified Extensible Firmware Interface (UEFI) bootkit, allowing it to stealthily persist inside of Windows systems despite reboots, by manipulating the process by which the operating system is loaded. Glupteba is a malware behemoth: a combination backdoor-infostealer-loader-cryptominer-malvertiser-botnet, built modularly to allow even more components to be added at will by its operators. Among its many capabilities are some extra-special features, too, such as using the Bitcoin blockchain as a backup command-and-control (C2) system and being able to hide itself with Windows kernel drivers. Its latest shiny feature is an upgrade on that last bit. In a campaign observed by Palo Alto Networks' Unit 42 last November, Glupteba came fitted with an incisive bootloader implant, ensuring that it can start running on infected Windows machines even before Windows itself does.

Source	Long Form Article
Krebs on Security By Brian Krebs(5-6min)	**Fat Patch Tuesday, February 2024 Edition** Microsoft Corp. today pushed software updates to plug more than 70 security holes in its Windows operating systems and related products, including two zero-day vulnerabilities that are already being exploited in active attacks. Top of the heap on this Fat Patch Tuesday is CVE-2024-21412, a "security feature bypass" in the way Windows handles Internet Shortcut Files that Microsoft says is being targeted in active exploits. Redmond's advisory for this bug says an attacker would need to convince or trick a user into opening a malicious shortcut file. Researchers at Trend Micro have tied the ongoing exploitation of CVE-2024-21412 to an advanced persistent threat group dubbed "Water Hydra," which they say has being using the vulnerability to execute a malicious Microsoft Installer File (.msi) that in turn unloads a remote access trojan (RAT) onto infected Windows systems. The other zero-day flaw is CVE-2024-21351, another security feature bypass — this one in the built-in Windows SmartScreen component that tries to screen out potentially malicious files downloaded from the Web. Kevin Breen at Immersive Labs says it's important to note that this vulnerability alone is not enough for an attacker to compromise a user's workstation, and instead would likely be used in conjunction with something like a spear phishing attack that delivers a malicious file. Satnam Narang, senior staff research engineer at Tenable, said this is the fifth vulnerability in Windows SmartScreen patched since 2022 and all five have been exploited in the wild as zero-days. They include CVE-2022-44698 in December 2022, CVE-2023-24880 in March 2023, CVE-2023-32049 in July 2023 and CVE-2023-36025 in November 2023. Narang called special attention to CVE-2024-21410, an "elevation of privilege" bug in Microsoft Exchange Server that Microsoft says is likely to be exploited by attackers. Attacks on this flaw would lead to the disclosure of NTLM hashes, which could be leveraged as part of an NTLM relay or "pass the hash" attack, which lets an attacker masquerade as a legitimate user without ever having to log in. "We know that flaws that can disclose sensitive information like NTLM hashes are very valuable to attackers," Narang said. "A Russian-based threat actor leveraged a similar vulnerability to carry out attacks – CVE-2023-23397 is an Elevation of Privilege vulnerability in Microsoft Outlook patched in March 2023." Microsoft notes that prior to its Exchange Server 2019 Cumulative Update 14 (CU14), a security feature called Extended Protection for Authentication (EPA), which provides NTLM credential relay protections, was not enabled by default. "Going forward, CU14 enables this by default on Exchange servers, which is why it is important to upgrade," Narang said. Rapid7's lead software engineer Adam Barnett highlighted CVE-2024-21413, a critical remote code execution bug in Microsoft Office that could be exploited just by viewing a specially-crafted message in the Outlook Preview pane. "Microsoft Office typically shields users from a variety of attacks by opening files with Mark of the Web in Protected View, which means Office will render the document without fetching potentially malicious external resources," Barnett said. "CVE-2024-21413 is a critical RCE vulnerability in Office which allows an attacker to cause a file to open in editing mode as though the user had agreed to trust the file." Barnett stressed that administrators responsible for Office 2016 installations who apply patches outside of Microsoft Update should note the advisory lists no fewer than five separate patches which must be installed to achieve remediation of CVE-2024-21413; individual update knowledge base (KB)

Source	Long Form Article
	articles further note that partially patched Office installations will be blocked from starting until the correct combination of patches has been installed. It's a good idea for Windows end-users to stay current with security updates from Microsoft, which can quickly pile up otherwise. That doesn't mean you have to install them on Patch Tuesday. Indeed, waiting a day or three before updating is a sane response, given that sometimes updates go awry and usually within a few days Microsoft has fixed any issues with its patches. It's also smart to back up your data and/or image your Windows drive before applying new updates. For a more detailed breakdown of the individual flaws addressed by Microsoft today, check out the SANS Internet Storm Center's list. For those admins responsible for maintaining larger Windows environments, it often pays to keep an eye on Askwoody.com, which frequently points out when specific Microsoft updates are creating problems for a few users.