Continue

Is "tri-quarterly" a real English word meaning 3 times a year? Are there any other words that mean 3 times a year? 5 China-linked APT24 hackers have been using a previously undocumented malware called BadAudio in a three-year espionage campaign that recently switched to more sophisticated attack methods. Since 2022, the malware has been delivered to victims through multiple methods that include spearphishing, supply-chain compromise, and watering hole attacks. Campaign evolution From November 2022 until at least September 2025, APT24 compromised more than 20 legitimate public websites from various domains to inject malicious JavaScript code that selected visitors of interest - the focus was exclusively on Windows systems. Researchers at Google Threat Intelligence Group (GTIG) say that the script fingerprinted visitors who qualified as targets and loaded a fake software update pop-up to lure them into downloading BadAudio. APT24's fake update pop-upSource: Google Starting July 2024, APT24 compromised multiple times a digital marketing company in Taiwan that provides JavaScript libraries to client websites. Through this tactic, the attackers injected malicious JavaScript into a widely used library that the firm distributed, and registered a domain name that impersonated a legitimate Content Delivery Network (CDN). This enabled the attacker to compromise more than 1,000 domains. From late 2024 until July 2025, APT24 repeatedly compromised the same marketing firm by injecting malicious, obfuscated JavaScript into a modified JSON file, which was loaded by a separate JavaScript file from the same vendor. Once executed, it fingerprinted each website visitor and sent a base64-encoded report to the attackers' server, allowing them to decide if they would reply with the next-stage URL. Overview of the supply chain attackSource: Google In parallel, starting from August 2024, APT24 launched spearphishing operations that delivered the BadAudio malware using as lures emails that impersonated animal rescue organizations. In some variants of these attacks, APT24 used legitimate cloud services like Google Drive and OneDrive for malware distribution, instead of their own servers. However, Google says that many of the attempts were detected, and the messages ended up in the spam box. In the observed cases, though, the emails included tracking pixels to confirm when recipients opened them. Timeline of APT24 attack methodsSource: Google BadAudio malware loader According to GTIG’s analysis, the BadAudio malware is heavily obfuscated to evade detection and hinder analysis by security researchers. It achieves execution through DLL search order hijacking, a technique that allows a malicious payload to be loaded by a legitimate application. "The malware is engineered with control flow flattening—a sophisticated obfuscation technique that systematically dismantles a program's natural, structured logic," GTIG explains in a report today. "This method replaces linear code with a series of disconnected blocks governed by a central 'dispatcher' and a state variable, forcing analysts to manually trace each execution path and significantly impeding both automated and manual reverse engineering efforts." Once BadAudio is executed on a target device, it collects basic system details (hostname, username, architecture), encrypts the info using a hard-coded AES key, and sends it to a hard-coded command-and-control (C2) address. Next, it downloads an AES-encrypted payload from the C2, decrypts it, and executes it in memory for evasion using DLL sideloading. In at least one case, Google researchers observed the deployment of the Cobalt Strike Beacon via BadAudio, a widely abused penetration-testing framework. The researchers underline that they couldn't confirm the presence of a Cobalt Strike Beacon in every instance they analyzed. It should be noted that despite using BadAudio for three years, APT24's tactics succeeded in keeping it largely undetected. From the eight samples GTIG researchers provided in their report, only two are flagged as malicious by more than 25 antivirus engines on the VirusTotal scanning platform. The rest of the samples, with a creation date of December 7, 2022, are detected by up to five security solutions. GTIG says that APT24's evolution towards stealthier attacks is driven by the threat actor's operational capabilities and its "capacity for persistent and adaptive espionage." Broken IAM isn't just an IT problem - the impact ripples across your whole business. This practical guide covers why traditional IAM practices fail to keep up with modern demands, examples of what "good" IAM looks like, and a simple checklist for building a scalable strategy. Three newly disclosed vulnerabilities in the runC container runtime used in Docker and Kubernetes could be exploited to bypass isolation restrictions and get access to the host system. The security issues, tracked as CVE-2025-31133, CVE-2025-52565, and CVE-2025-52881 (all), were reported this week and disclosed by SUSE software engineer and Open Container Initiative (OCI) board member Aleksa Sarai. runC is a universal container runtime and the OCI reference implementation for running containers. It is responsible for low-level operations such as creating the container process, setting up namespaces, mounts, and cgroups that higher-level tools, like Docker and Kubernetes, can call. An attacker exploiting the vulnerabilities could obtain write access to the underlying container host with root privileges: CVE-2025-31133 — runC uses /dev/null bind-mounts to “mask” sensitive host files. If an attacker replaces /dev/null with a symlink during container init, runc can end up bind-mounting an attacker-controlled target read-write into the container — enabling writes to /proc, and container escape. CVE-2025-52565 — The /dev/console bind mount can be redirected via races/symlinks so that runc mounts an unexpected target into the container before protections are applied. That again can expose writable access to critical procfs entries and enable breakouts. CVE-2025-52881 — runC can be tricked into performing writes to /proc that are redirected to attacker-controlled targets. It can bypass LSM relabel protections in some variants and turns ordinary runc writes into arbitrary writes to dangerous files like /proc/sysrq-trigger. CVE-2025-31133 and CVE-2025-52881 affect all versions of runC, while CVE-2025-52565 impacts runC versions 1.0.0-rc3 and later. Fixes are available in runC versions 1.2.8, 1.3.3, 1.4.0-rc.3, and later. Exploitability and risk Researchers at cloud security company Sysdig note that exploiting the three vulnerabilities "require the ability to start containers with custom mount configurations," which an attacker can achieve through malicious container images or Dockerfiles. Currently, there have been no reports of any of the flaws being actively exploited in the wild. In an advisory this week, Sysdig shares that attempts to exploit any of the three security issues can be detected by monitoring suspicious symlink behaviors. RunC developers also shared mitigation actions, which include activating user namespaces for all containers without mapping the host root user into the container's namespace. This precaution should block the most important parts of the attack because of the Unix DAC permissions that would prevent namespaced users from accessing relevant files. Sysdig also recommends using rootless containers, if possible, to reduce the potential damage from exploiting a vulnerability. Broken IAM isn't just an IT problem - the impact ripples across your whole business. This practical guide covers why traditional IAM practices fail to keep up with modern demands, examples of what "good" IAM looks like, and a simple checklist for building a scalable strategy. Why do we have both the word "three" and the numeral "3" in this sentence? The number 345 has three digits, where the first digit is a 3. 7 D-Link is warning of three remotely exploitable command execution vulnerabilities that affect all models and hardware revisions of its DIR-878 router, which has reached end-of-service but is still available in several markets. Technical details and proof-of-concept (PoC) exploit code demonstrating the vulnerabilities have been published by a researcher using the name Yangyifan. Typically used in homes and small offices, the DIR-878 was hailed as a high-performance dual-band wireless router when it launched in 2017. Even if the device is no longer supported, it can still be purchased new or used for prices between $75 and $122. However, as DIR-878 has reached end-of-life (EoL) in 2021, D-Link warned that it will not release security updates for this model and recommends replacing it with an actively supported product. In total, D-Link's security advisory lists four vulnerabilities, only one of them requiring physical access or control over a USB device for exploitation. CVE-2025-60672 – Remote unauthenticated command execution via SetDynamicDNSSettings parameters stored in NVRAM and used in system commands. CVE-2025-60673 – Remote unauthenticated command execution via SetDMZSettings and unsanitized IPAddress value injected into iptables commands. CVE-2025-60674 – Stack overflow in USB storage handling due to oversized “Serial Number” field (physical or USB-device-level attack). CVE-2025-60676 – Arbitrary command execution via unsanitized fields in /tmp/new_qos.rule, processed by binaries using system(). Despite being remotely exploitable, and exploit code already publicly available, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has assessed that the vulnerabilities have a medium-severity score. However, a publicly available exploit typically captures threat actors' attention, especially botnet operators, who usually include them in their arsenal to expand targeting. For instance, the large-scale botnet RondoDox uses more than 56 known flaws, some affecting D-Link devices, and keeps adding more of them. More recently, BleepingComputer reported on the Aisuru botnet, which launched a massive distributed denial-of-service (DDoS) attack against Microsoft's Azure network, sending 15.72 terabits per second (Tbps) from over 500,000 IP addresses. Broken IAM isn't just an IT problem - the impact ripples across your whole business. This practical guide covers why traditional IAM practices fail to keep up with modern demands, examples of what "good" IAM looks like, and a simple checklist for building a scalable strategy. The expression comes from Psalm 90:10 (King James Version) — Original Hebrew. The days of our years are threescore years and ten; and if by reason of strength they be fourscore years, yet is their strength labour and sorrow; for it is soon cut off, and we fly away. The much older Latin Vulgate has the "70 years" as: "septuaginta anni", where the first word is clearly "70" without the use of "score". The even older original Hebrew text has "שִׁבְעִים שָׁנָה" (šiḇʿîm šānâ). "šiḇʿîm" has "שֶׁבַע" (šeḇaʿ) as its root, and that simply means "seven", again with no use of "score". The translators of the Authorized Version (KJV) must have decided to use the more poetic "three score years and ten" instead. Meanwhile, the famous Gettysburg Address by Abraham Lincoln begins with: Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal. I suspect that it is mostly Americans that use the "three score and ten years" form, subconsciously paralleling Lincoln's "four score and seven years", while the rest of the world uses the King James translation with the embedded "years". Three former employees of cybersecurity incident response companies DigitalMint and Sygnia have been indicted for allegedly hacking the networks of five U.S. companies in BlackCat (ALPHV) ransomware attacks between May 2023 and November 2023. 28-year-old Kevin Tyler Martin of Roanoke, Texas (who pleaded not guilty), 33-year-old Ryan Clifford Goldberg of Watkinsville, Georgia (in federal custody since September 2023), and an unnamed accomplice face charges of conspiracy to interfere with interstate commerce by extortion, interference with interstate commerce by extortion, and intentional damage to protected computers. If convicted, the defendants could face a maximum penalty of up to 50 years in prison: 20 years for each extortion charge and an additional 10 years for damage to computer systems. According to the Chicago Sun-Times, which first spotted the unsealed court documents, Martin worked at DigitalMint as a ransomware threat negotiator (just as the unnamed co-conspirator), while Goldberg is a former Sygnia incident response manager. The Department of Justice claims the defendants operated as ALPHV BlackCat affiliates, gaining unauthorized access to the victims' networks, stealing data, deploying encryption malware, and demanding cryptocurrency payments in exchange for decryption keys and promises not to leak the stolen information online. Per the indictment, the group's alleged victims include a Tampa medical device manufacturer, a Maryland pharmaceutical company, a California doctor's office, a California engineering firm, and a Virginia drone manufacturer. Prosecutors said the attackers have demanded ransoms ranging from $300,000 to $10 million. Still, they were only paid $1.27 million by the Tampa medical device company after they encrypted its servers and demanded $10 million in May 2023. Although other victims also received ransom demands, the indictment does not indicate whether additional payments were made. As BleepingComputer previously reported, the Department of Justice was investigating a former DigitalMint ransomware negotiator for allegedly working with ransomware gangs to profit from extortion payment deals. The DOJ and the FBI declined to comment when contacted at the time for more information. It is unclear if this indictment is related to the DOJ's previous investigation. A 2019 ProPublica report revealed that some U.S. data recovery firms have also secretly paid ransomware gangs while charging clients for restoration services without disclosing these payments. In a February 2024 joint advisory, the FBI, CISA, and the Department of Health and Human Services (HHS) warned that Blackcat ransomware affiliates were primarily targeting organizations in the U.S. healthcare sector. The FBI has also linked BlackCat to over 60 breaches between November 2021 and March 2022 (the ransomware group's first four months of activity) and said they raked in at least $300 million in ransoms from more than 1,000 victims until September 2023. Broken IAM isn't just an IT problem - the impact ripples across your whole business. This practical guide covers why traditional IAM practices fail to keep up with modern demands, examples of what "good" IAM looks like, and a simple checklist for building a scalable strategy. One of the earliest versions of “two is company, three is a crowd” was recorded in 1678 by John Ray, in his collection English Proverbs, p.471 One's too few, three too many Therefore, presumably, ‘two’ was then considered idyllic. The Oxford Dictionary of Word Origins claims that the original proverb is from 1730s, and cites an English translation from The Spanish and English Dictionary by J. Stevens, printed in 1726. Prov. Compañía de tres no vale res; A company consisting of three is worth nothing. It is the Spanish opinion who say that to keep a secret three are too many, and to be merry they are too few. John Collins provides this translation which resembles more closely the English proverb (1834) “Three persons in company are too many for any secret affair, and two few for social enjoyment.” ‘... three is none’ (1840) From The Facts on File Dictionary of Proverbs by Martin H. Manser (link), we learn the following: The proverb was first recorded in the mid-19th century, in the form “Two is company but three is none,” (W.C. Hazlitt, English Proverbs [1869]) but the sentiment it expresses is of earlier origin. Variants of this proverb: two is company but three is none; two's a couple, but three's a crowd, four's too many, and fives's not allowed. Henry Downes Miles' Dick Turpin, printed in 1840, contains the following adage Their conversation had proceeded thus far, and Dennis appeared about to offer his services in some other shape, when Esther appeared slowly advancing towards them. “Two is good company when three is none” Five years later, we have this detailed analysis in The Usurer. A Tale of Marseilles. written by Percy B. St. John. “Two is company—three is none:” so says the adage; but, as is often the case, the adage is in error. There are occasions when certainly nothing can be more delightful than for two people, of course of different sexes, to find themselves alone, and interchange all those sweet vows and soft nothings which make up the sum-total of a declaration and an acceptance. But still, three is often a better number for enjoyment far than two. Even a pair of levers are more at their ease—especially if the one who is generally considered de trop is a talkative and companionable person ‘... three is trumpery’ (1866) Yet another variant appeared in the late 19th century containing the term, trumpery, i.e., something showy but worthless. An old rhyme Molly had heard -Betty use would keep running in her head and making her uneasy-— “Two is company, Three is trumpery.” Wives and daughters, an Every-Day Story By Elizabeth Gaskell ‘... three's a crowd’ (1870) As for the more modern version containing the term “three's a crowd” it appears to be American. The earliest instance I found is from Delaware Gazette. December 02, 1870, the article is titled Miss Althea's Rubbers I had my reward when Steven lifted me down at our gate, and she said : "You're your mother's own gal ! You hain't never let me feel that two's a company and three's a crowd !" Steven had walked up the long path with me to carry my shawl, and might have said just a word then—a woman can live long on only a word, if it be loving enough—but he almost threw the shawl across my arm, and ran down the path as if he were glad to be well rid of me. As I "piled Ossa on Pelion" in my thoughts against the possibility of his loving me as I desired to be loved, the forenoon wore away, and the apples were sorted. ‘... three are a crowd’ (1872) Courtesy of @Sven Yargs are the following two excerpts: “One of My Bygones,” in the Wichita [Kansas] City Eagle (November 21, 1872). It's also worth mentioning that the saying contains the plural verb: “My dear turtle-doves.” she said at last, laying one hand on mine and looking hard at my friend. “I see how it is with you. You have reached the point where ‘two are a company and three are a crowd.’” And from an item titled "Proverbs" in the Juniata [Pennsylvania] Sentinel and Republican January 21, 1874. Here the verb is singular and in the simple past. Now go and ask a couple of doting lovers if they believe in that sort of thing ["the more the merrier"]. They would undoubtedly think that two was company, and three was a crowd. One thing is certain it is hard, very hard to crowd that idea into the heads of some that is or that was to be mother-in-laws P.S Many thanks to Sven Yargs who provided the last two links. Fortinet has confirmed that it has silently patched a critical zero-day vulnerability in its FortiWeb web application firewall, which is now "massively exploited in the wild." The flaw was silently patched after reports that unauthenticated attackers were exploiting an unknown FortiWeb path traversal flaw in early October to create new administrative users on Internet-exposed devices. The attacks were first identified by threat intel firm Defused on October 6, which published a proof-of-concept exploit and reported that an "unknown Fortinet exploit (possibly a CVE-2022-40684 variant)" is being used to send HTTP POST requests to the /api/v2.0/cmdb/system/admin%3f/../../../../../cgi-bin/fwbcgi Fortinet endpoint to create local admin-level accounts. On Thursday, watchTowr Labs security researchers also demoed an exploit and released a tool called "FortiWeb Authentication Bypass Artifact Generator to help defenders identify vulnerable devices. Cybersecurity firm Rapid7 added that the flaw affects FortiWeb versions 8.0.1 and earlier, as it confirmed that the publicly available proof-of-concept exploit no longer works after updating to version 8.0.2. Today, Fortinet disclosed that attackers are actively exploiting a path confusion vulnerability (now tracked as CVE-2025-64446) in FortiWeb's GUI component, which allows unauthenticated attackers to execute administrative commands on unpatched systems via crafted HTTP or HTTPS requests. "Fortinet has observed this to be exploited in the wild," the company noted in a Friday security advisory, which confirms that the zero-day has been patched in FortiWeb 8.0.2, released on October 28, three weeks after the first report of CVE-2025-64446 active exploitation. Version Affected Solution FortiWeb 8.0 8.0.0 through 8.0.1 Upgrade to 8.0.2 or above FortiWeb 7.6 7.6.0 through 7.6.4 Upgrade to 7.6.5 or above FortiWeb 7.4 7.4.0 through 7.4.9 Upgrade to 7.4.10 or above FortiWeb 7.2 7.2.0 through 7.2.11 Upgrade to 7.2.12 or above FortiWeb 7.0 7.0.0 through 7.0.11 Upgrade to 7.0.12 or above Federal agencies ordered to patch within a week CISA also added the CVE-2025-64446 path traversal flaw to its catalog of actively exploited vulnerabilities on Friday, ordering U.S. federal agencies to patch their systems by November 21. "This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise," the cybersecurity agency warned. Admins who can't immediately upgrade to FortiWeb 8.0.2 should disable HTTP or HTTPS for all internet-facing management interfaces and ensure that access is restricted to trusted networks. Fortinet also advised customers to check their configuration and review logs for new unauthorized administrator accounts and other unexpected modifications. BleepingComputer contacted Fortinet with questions about these ongoing attacks, but we have yet to receive a response. In August, Fortinet patched a critical command injection flaw (CVE-2025-25256) with publicly available exploit code in its FortiSIEM security monitoring solution, one day after cybersecurity company GreyNoise warned of a massive spike in brute-force attacks targeting Fortinet SSL VPNs. Broken IAM isn't just an IT problem - the impact ripples across your whole business. This practical guide covers why traditional IAM practices fail to keep up with modern demands, examples of what "good" IAM looks like, and a simple checklist for building a scalable strategy.

- http://moristas.com/userfiles/files/6e0e7163_e899_44d6_93ae_44420a5a17a2.pdf
- hocadegi
- https://aihr-iadh.org/uploads/FCK_files/file/97325785456.pdf
- are probated wills public record in ontario
- rayaseyimi
- free cinematic luts for after effects
- http://crmsurvworldwide.com/scgtest/team-explore/uploads/files/lanowir_wagorada_tedodix.pdf
- xayo