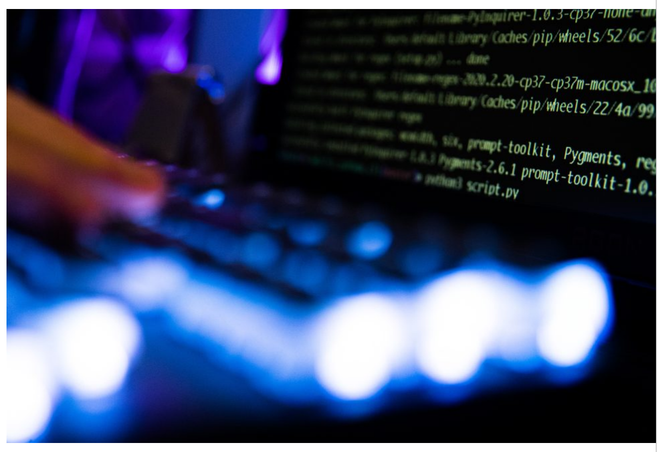
Widely used Daemon Tools disk app backdoored in monthlong supply-chain attack

By Ars Technica

Daemon Tools Users Urged to Inspect for Hidden Threats Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long supply chain attack that compromised the application. Cybersecurity experts are warning that malicious actors successfully infiltrated the software's distribution process, potentially exposing users to stealthy infections. The breach raises significant concerns about the integrity of widely-used applications, emphasizing the need for vigilance among users. With the risk of malware lurking undetected, it is crucial for individuals to scan their systems and ensure their security measures are robust. As investigations continue, affected users are encouraged to take immediate action to safeguard their machines. Experts recommend uninstalling the application and considering alternative software until the situation is fully resolved. Daemon Tools Users Urged to Inspect for Hidden Threats Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long supply chain attack that compromised the application. Cybersecurity experts are warning that malicious actors successfully infiltrated the software's distribution process, potentially exposing users to stealthy infections. The breach raises significant concerns about the integrity of widely-used ap- individuals to scan their systems and ensure their security measures are robust. As investigations continue, affected users are encouraged to take immediate action to safeguard their machines. Experts recommend uninstalling the application and considering alternative software until the situation is fully resolved. Daemon Tools Users Urged to Inspect for Hidden Threats Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long supply chain attack that compromised the application. Cybersecurity experts are warning that malicious actors successfully infiltrated the software's distribution process, potentially exposing users to stealthy infections. The breach raises significant concerns about the integrity of widely-used applications, emphasizing the need for vigilance among users. With the risk of malware lurking undetected, it is crucial for individuals to scan their systems and ensure their security measures are robust. As investigations continue, affected users are encouraged to take immediate action to safeguard their machines. Experts recommend uninstalling the application and considering alternative software until the situation is fully resolved. Daemon Tools Users Urged to Inspect for Hidden Threats Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long sup- distribution process, potentially exposing users to stealthy infections. The breach raises significant concerns about the integrity of widely-used applications, emphasizing the need for vigilance among users. With the risk of malware lurking undetected, it is crucial for individuals to scan their systems and ensure their security measures are robust. As investigations continue, affected users are encouraged to take immediate action to safeguard their machines. Experts recommend uninstalling the application and considering alternative software until the situation is fully resolved. Daemon Tools Users Urged to Inspect for Hidden Threats Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long supply chain attack that compromised the application. Cybersecurity experts are warning that malicious actors successfully infiltrated the software's distribution process, potentially exposing users to stealthy infections. The breach raises significant concerns about the integrity of widely-used applications, emphasizing the need for vigilance among users. With the risk of malware lurking undetected, it is crucial for individuals to scan their systems and ensure their security measures are robust. As investigations continue, affected users are encouraged to take immediate action to safeguard their machines. Experts recommend uninstalling the application and considering

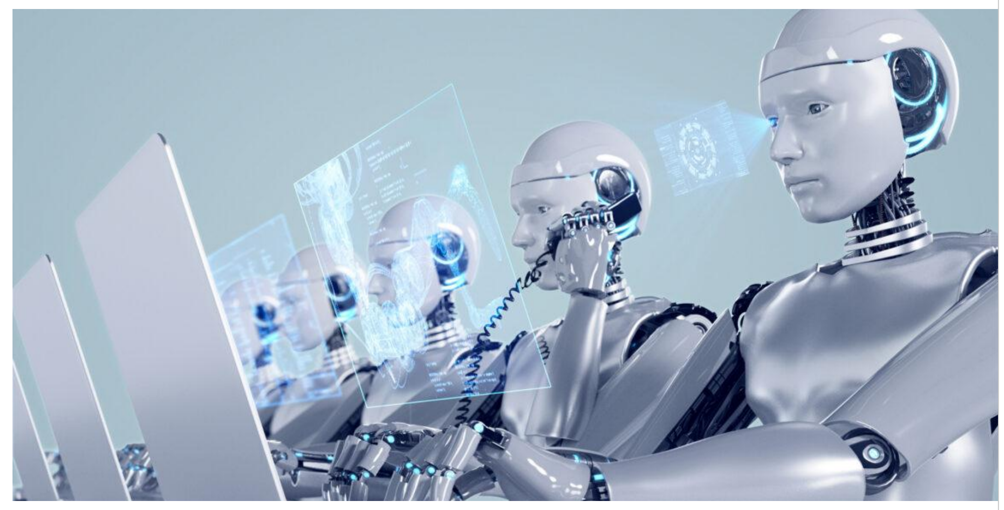


Daemon Tools Users Urged to Inspect for Hidden Threats Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long

Inspect for Hidden Threats Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long supply chain attack that compromised the application. Cybersecurity experts are warning that malicious actors successfully infiltrated the software's distribution process, potentially exposing users to stealthy infections. The breach raises significant concerns about the integrity of widely-used applications, emphasizing the need for vigilance among users. With the risk of malware lurking undetected, it is crucial for individuals to scan their systems and ensure their security measures are robust. As investigations continue, affected users are encouraged to take immediate action to safeguard their machines. Experts recommend uninstalling the application and considering alternative software until the situation is fully resolved. Daemon Tools Users of the popular Daemon Tools disk management software are on high alert following revelations of a month-long supply chain attack that compromised the application. Cybersecurity experts are warning that malicious actors successfully infiltrated the software's distribution process, potentially exposing users to stealthy infections. The breach raises significant concerns about the integrity of widely-used applications, emphasizing the need for vigilance among users. With the risk of malware lurking undetected, it is crucial for individuals to scan their systems and ensure their security measures are robust. As investigations continue, affected users are encouraged to take immediate action to safeguard their machines. Experts recommend uninstalling the application and considering alternative software until the situation is fully resolved. Daemon Tools Users Urged to Inspect for Hidden

Mozilla says 271 vulnerabilities found by Mythos have "almost no false positives"

By Ars Technica

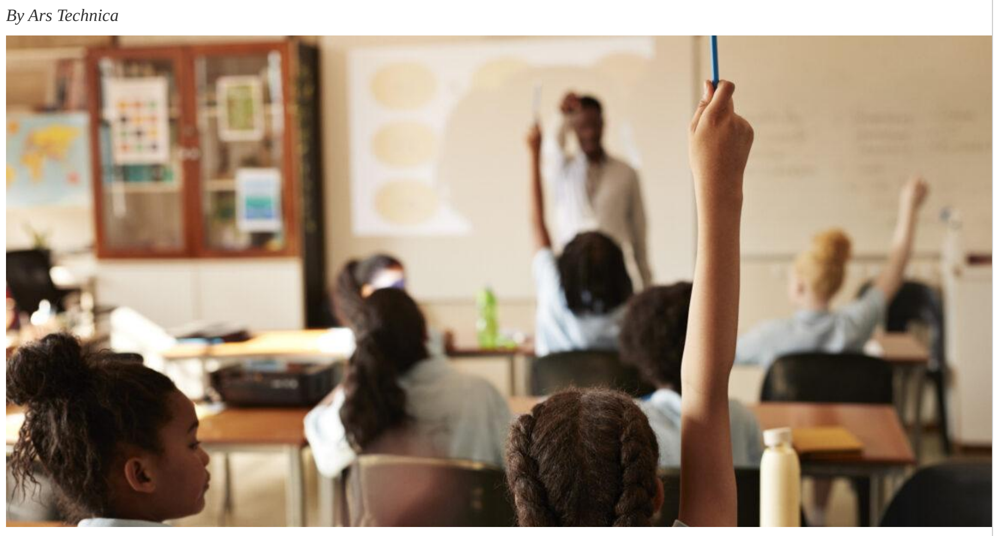


Mozilla Embraces AI in Bug Discovery with Mythos Mozilla, the organization behind the popular Firefox browser, has announced a significant development in its approach to

Mozilla Embraces AI in Bug Discovery with Mythos Mozilla, the organization behind the popular Firefox browser, has announced a significant development in its approach to identifying software vulnerabilities. The company reports that Mythos, an AI tool, has uncovered 271 vulnerabilities with "almost no false positives." This marks a pivotal moment in Mozilla's commitment to leveraging artificial intelligence for enhanced security. In a statement reflecting this commitment, Mozilla emphasized that it has "completely bought in" on the potential of AI-assisted technologies to improve bug discovery processes. This adoption not only underscores the growing reliance on AI in cybersecurity but also highlights Mozilla's proactive stance in safeguarding its users. Mozilla Embraces AI in Bug Discovery with Mythos Mozilla, the organization behind announced a significant development in its approach to identifying software vulnerabilities. The company reports that Mythos, an AI tool, has uncovered 271 vulnerabilities with "almost no false positives." This marks a pivotal moment in Mozilla's commitment to leveraging artificial intelligence for enhanced security. In a statement reflecting this commitment, Mozilla emphasized that it has "completely bought in" on the potential of AI-assisted technologies to improve bug discovery processes. This adoption not only underscores the growing reliance on AI in cybersecurity but also highlights Mozilla's proactive stance in safeguarding its users. Mozilla Embraces AI in Bug Discovery with Mythos Mozilla, the organization behind the popular Firefox browser, has announced a significant development in its approach to identifying software vulnerabilities. reports that Mythos, an AI tool, has uncovered 271 vulnerabilities with "almost no false positives." This marks a pivotal moment in Mozilla's commitment to leveraging artificial intelligence for enhanced security. In a statement reflecting this commitment, Mozilla emphasized that it has "completely bought in" on the potential of AI-assisted technologies to improve bug discovery processes. This adoption not only underscores the growing reliance on AI in cybersecurity but also highlights Mozilla's proactive stance in safeguarding its users. Mozilla Embraces AI in Bug Discovery with Mythos Mozilla, the organization behind the popular Firefox browser, has announced a significant development in its approach to identifying software vulnerabilities. The company reports that Mythos, an AI tool, has uncovered 271 vulnerabilities with "almost no false posit-

Chaos erupts as cyberattack disrupts learning platform Canvas amid finals

By Ars Technica



Cyberattack Forces Schools to Delay Final Exams A significant cyberattack has thrown educational institutions into turmoil as the widely used learning platform Canvas experienced

Cyberattack Forces Schools to Delay Final Exams A significant cyberattack has thrown educational institutions into turmoil as the widely used learning platform Canvas experienced major disruptions. As a result, schools and colleges nationwide are forced to postpone their year-end examinations, leaving students in a state of uncertainty. The attack impacted access to essential resources and course materials, complicating the already stressful finals period for students. With many relying on the platform for their studies, educators have scrambled to adapt, seeking alternative solutions to ensure their students can complete assessments. As the through the academic landscape, institutions are working diligently to restore functionality while prioritizing the security of their systems. In the interim, many students are left waiting to see when they can take their crucial exams. Cyberattack Forces Schools to Delay Final Exams A significant cyberattack has thrown educational institutions into turmoil as the widely used learning platform Canvas experienced major disruptions. As a result, schools and colleges nationwide are forced to postpone their year-end examinations, leaving students in a state of uncertainty. The attack impacted access to essential resources and course materials, students. With many relying on the platform for their studies, educators have scrambled to adapt, seeking alternative solutions to ensure their students can complete assessments. As the effects of the breach ripple through the academic landscape, institutions are working diligently to restore functionality while prioritizing the security of their systems. In the interim, many students are left waiting to see when they can take their crucial exams. Cyberattack Forces Schools to Delay Final Exams A significant cyberattack has thrown educational institutions into turmoil as the widely used learning platform Canvas experienced major disruptions.

Websites have a new way to spy on visitors: Analyzing their SSD activity

By Ars Technica

New Browser Technique Enables Websites to Monitor SSD Activity Websites are adopting a novel method to track user behavior by analyzing Solid State Drive (SSD) activity through

New Browser Technique Enables Websites to Monitor SSD Activity Websites are adopting a novel method to track user behavior by analyzing Solid State Drive (SSD) activity through simple JavaScript. This technique allows sites to glean insights into how visitors interact with their devices more intimately than before. By measuring SSD activity while users browse, websites can obtain valuable information on user engagement and preferences. This development raises significant privacy concerns, as it blurs the lines of consent and user awareness regarding data tracking. As this technology becomes more widespread, discussions around closer examination of how consent is obtained and what data is truly necessary for web operations. The implications for both users and web developers are profound, pushing the boundaries of conventional tracking methods. New Browser Technique Enables Websites to Monitor SSD Activity Websites are adopting a novel method to track user behavior by analyzing Solid State Drive (SSD) activity through simple JavaScript. This technique allows sites to glean insights into how visitors interact with their devices more intimately than before. By measuring SSD activity while users browse, websites can obtain valuable information on user en- privacy concerns, as it blurs the lines of consent and user awareness regarding data tracking. As this technology becomes more widespread, discussions around digital privacy and user rights are likely to intensify, prompting a closer examination of how consent is obtained and what data is truly necessary for web operations. The implications for both users and web developers are profound, pushing the boundaries of conventional tracking methods. New Browser Technique Enables Websites to Monitor SSD Activity Websites are adopting a novel method to track user behavior by analyzing Solid State Drive (SSD) activity through simple JavaScript. This

Linux bitten by second severe vulnerability in as many weeks

By Ars Technica

Linux Faces Another Serious Vulnerability Linux users have encountered yet another critical vulnerability, marking the second such incident in just two weeks. This ongoing issue highlights the pressing need for immediate action among system administrators and users alike. Fortunately, patches for the production version are being released and should be prioritized for installation. Ignoring these updates could leave systems exposed to potential threats. As the Linux community grapples with this latest security challenge, vigilance and prompt updates are essential to safeguard against further exploits.

Zero-day exploit completely defeats default Windows 11 BitLocker protections

By Ars Technica

Windows 11 BitLocker Vulnerability Exposed by Zero-Day Exploit A newly discovered zero-day exploit has raised significant concerns regarding the default protections of Windows 11's BitLocker encryption. The specifics of how this exploit operates remain murky, leaving many questions unanswered. In response to the situation, Microsoft has confirmed that it is actively investigating the issue to understand the implications and develop a solution. Until more information is available, users are advised to remain vigilant and consider additional security measures.

Cisco announces record revenue and 4,000 layoffs in the same day

By Ars Technica

Cisco's Contradictory Day: Record Revenue Amidst 4,000 Job Cuts Cisco Systems made headlines recently by reporting a record revenue for the last fiscal quarter while simultaneously announcing a significant reduction in its workforce. The tech giant revealed plans to lay off 4,000 employees, raising eyebrows given its impressive financial performance. This dual announcement has sparked discussions around the company's future direction and workforce strategy. The Chief Financial Officer clarified that these layoffs are not a result of cost-cutting measures. Instead, he emphasized that the restructuring is aimed at adapting to changing market conditions, suggesting a strategic shift rather than a purely financial decision. The juxtaposition of soaring revenue and substantial job cuts has left many questioning the motives behind such drastic measures. As Cisco navigates this complex landscape, industry observers will be keenly watching how these changes will impact the Day: Record Revenue Amidst 4,000 Job Cuts Cisco Systems made headlines recently by reporting a record revenue for the last fiscal quarter while simultaneously announcing a significant reduction in its workforce. The tech giant revealed plans to lay off 4,000 employees, raising eyebrows given its impressive financial performance. This dual announcement has sparked discussions around the company's future direction and workforce strategy. The Chief Financial Officer clarified that these layoffs are not a result of cost-cutting measures. Instead, he emphasized that the restructuring is aimed at adapting to changing market conditions, suggesting a strategic shift rather than a purely financial decision. The juxtaposition of soaring revenue and substantial job cuts has left many questioning the motives behind such drastic measures. As Cisco navigates this complex landscape, industry observers will be keenly watching how these changes will impact the company's innovation and operational efficiency moving forward. Cisco's Contradictory

Cisco's Contradictory Day: Record Revenue Amidst 4,000 Job Cuts Cisco Systems made headlines recently by reporting a record revenue for the last fiscal quarter while

made headlines recently by reporting a record revenue for the last fiscal quarter while simultaneously announcing a significant reduction in its workforce. The tech giant revealed plans to lay off 4,000 employees, raising eyebrows given its impressive financial performance. This dual announcement has sparked discussions around the company's future direction and workforce strategy. The Chief Financial Officer clarified that these layoffs are not a result of cost-cutting measures. Instead, he emphasized that the restructur- market conditions, suggesting a strategic shift rather than a purely financial decision. The juxtaposition of soaring revenue and substantial job cuts has left many questioning the motives behind such drastic measures. As Cisco navigates this complex landscape, industry observers will be keenly watching how these changes will impact the company's innovation and operational efficiency moving forward. Cisco's Contradictory Day: Record Revenue Amidst 4,000 Job Cuts Cisco Systems made headlines recently by re-

Ars Asks: Share your shell and show us your tricked-out terminals!

By Ars Technica

Show Us Your Customized Command Line Interfaces! At The BoldLens, we love to highlight the creativity that can be found in the command line interface (CLI) community. This week,

Show Us Your Customized Command Line Interfaces! At The BoldLens, we love to highlight the creativity that can be found in the command line interface (CLI) community. This week, we invite you to share your unique terminal setups and the clever modifications you've made to enhance your workflow. Whether it's a vibrant color scheme or a handy script, every little tweak counts. Customizing the command line is more than it's about creating an environment that boosts productivity and personalizes your computing experience. From slick prompts to practical shortcuts, your terminal can be a reflection of your style and efficiency. Join us in this celebration of ingenuity! Post pictures of your terminals, share your favorite tricks, and let the community in on how you've optimized your CLI for the better. We can't wait to see what you've come up with! Customized Command Line Interfaces! At The BoldLens, we love to highlight the creativity that can be found in the command line interface (CLI) community. This week, we invite you to share your unique terminal setups and the clever modifications you've made to enhance your workflow. Whether it's a vibrant color scheme or a handy script, every little tweak counts. Customizing the command line is more than just aesthetics; it's an environment that boosts productivity and personalizes your computing experience. From slick prompts to practical shortcuts, your terminal can be a reflection of your style and efficiency. Join us in this celebration of ingenuity! Post pictures of your terminals, share your favorite tricks, and let the community in on how you've optimized your CLI for the better. We can't wait to see what you've come up with! Show Us Your