



## Your Security Rabbits report for February 23, 2022

### Hot topics

Nothing today

### News



#### 25 Malicious JavaScript Libraries Distributed via Official NPM Package Repository

Another batch of 25 malicious JavaScript libraries have made their way to the official NPM package registry with the goal of stealing Discord tokens and environment variables from compromised systems, more than two months after 17 similar packages were taken down. The libraries in question leveraged typosquatting techniques and masqueraded as other legitimate packages such as colors.js,



#### 91% of UK Organizations Compromised by an Email Phishing Attack in 2021

More than nine in ten (91%) UK organizations were successfully compromised by an email phishing attack last year, according to Proofpoint's 2022 State of the Phish report.



#### Carpet bombing DDoS attacks spiralled in 2021

Neustar Security Services has released a report which details the ongoing rise in cyberattacks in 2021, with an unprecedented number of carpet bombing distributed denial of service (DDoS) attacks.



#### Chinese Experts Uncover Details of Equation Group's Bvp47 Covert Hacking Tool

Researchers from China's Pangu Lab have disclosed details of a "top-tier" backdoor put to use by the Equation Group, an advanced persistent threat (APT) with alleged ties to the cyber-warfare intelligence-gathering unit of the U.S. National Security Agency (NSA). Dubbed "Bvp47" owing to numerous references to the string "Bvp" and the numerical value "0x47" used in the encryption algorithm, the



#### Cyberattackers Cook Up Employee Personal Data Heist for Meyer

The Conti gang breached the cookware giant's network, prepping thousands of employees' personal data for consumption by cybercrooks.



#### Documents shed light on ID.me's messaging to states about powerful facial recognition tech

Identity verification technology company ID.me quietly deployed a powerful form of facial recognition on unemployment benefits applicants while encouraging state partners to dispel the idea that the company used the technology, according to Oregon state records the American Civil Liberties Union shared with CyberScoop. The documents show that in the months following the introduction of facial recognition software that matched a photo across a wider database -- known as "1:many" -- into its fraud detection service, ID.me disseminated talking points to the Oregon Employment Department (OED) and other state partners to combat media reports that it used the more powerful form of facial recognit[...]



#### Gaming, Banking Trojans Dominate Mobile Malware Scene

The overall number of attacks on mobile users is down, but they're getting slicker, both in terms of malware functionality and vectors, researchers say.



#### Hackers focused on supply chains in 2021

Cybercriminals have put most of their time into breaking supply chains over the last year. The manufacturing sector has emerged as a top target. IBM's annual X-Force Threat Intelligence Index, a report based on threat data and security incidents over 2021, suggests that businesses are being "imprisoned" by criminals exploiting vulnerabilities and deploying ransomware. Researchers for [...] The post Hackers focused on supply chains in 2021 appeared first on IT Security Guru.



#### Hackers tried to shatter the spine of global supply chains in 2021

IBM researchers say supply chains were the focus of criminals last year and



#### 9-Year-Old Unpatched Email Hacking Bug Uncovered in Horde Webmail Software

Users of Horde Webmail are being urged to disable a feature to contain a nine-year-old unpatched security vulnerability in the software that could be abused to gain complete access to email accounts simply by previewing an attachment. "This gives the attacker access to all sensitive and perhaps secret information a victim has stored in their email account and could allow them to gain further



#### Asustor NAS owners hit by DeadBolt ransomware attack

The message displayed by the DeadBolt ransomware claims that victims were targeted simply because they were using Asustor NAS devices, and put the blame on the vendor's "inadequate security."



#### China-linked APT10 Target Taiwan's financial trading industry

China-linked APT group APT10 (aka Stone Panda, Bronze Riverside) targets Taiwan's financial trading sector with a supply chain attack. The campaign was launched by the APT10 group started in November 2021, but it hit a peak between 10 and 13 2022, Taiwanese cybersecurity firm CyCraft reported. The group (also known as Cicada, Stone Panda, MenuPass group, [...]) The post China-linked APT10 Target Taiwan's financial trading industry appeared first on Security Affairs.



#### Cookware giant Meyer Corporation discloses cyberattack

US cookware distributor giant Meyer Corporation discloses a data breach that affected thousands of its employees. Meyer Corporation, the second-largest cookware distributor globally, has disclosed a data breach that affects thousands of its employees. The attack took place on October 25, 2021, as reported by the data breach notification letter shared with the U.S. Attorney [...] The post Cookware giant Meyer Corporation discloses cyberattack appeared first on Security Affairs.



#### Devious phishing method bypasses MFA using remote access software

A devious, new phishing technique allows adversaries to bypass MFA by secretly having victims log into their accounts directly on attacker-controlled servers using the VNC screen sharing system.



#### Employees are often using devices in seriously risky ways

According to a Mobile Mentor study, 36 percent of employees admit to finding ways to work around security policies, and 72 percent value their personal privacy over company security.



#### Guide to Cyber Threat Intelligence: Elements of an Effective Threat Intel and Cyber Risk Remediation Program

Threat intelligence serves as your organization's first line of defense against threat actors and security risks that may be targeting your data, infrastructure, assets, personnel, and stakeholders. Understanding the importance of this information--and working to improve the quality of your threat intel and risk remediation program--is crucial to maximizing your organization's defense capabilities and security [...] The post Guide to Cyber Threat Intelligence: Elements of an Effective Threat Intel and Cyber Risk Remediation Program appeared first on Flashpoint.

























#### Hackers Stole \$1.7 Million Worth of NFTs from Users of OpenSea Marketplace

Malicious actors took advantage of a smart contract upgrade process in the OpenSea NFT marketplace to carry out a phishing attack against 17 of its users that resulted in the theft of virtual assets worth about \$1.7 million. NFTs, short for non-fungible tokens, are digital tokens that act like certificates of authenticity for, and in some cases represent ownership of, assets that range from



#### Horde Webmail Software is affected by a dangerous bug since 2012

Experts found a nine-year-old unpatched flaw in the Horde Webmail software that could allow access to email accounts. A feature in the Horde Webmail is affected by a nine-year-old unpatched security vulnerability that could be abused to gain complete access to email accounts simply by previewing an

	<p>manufacturers bore the brunt of attacks.</p>	<p>attachment. Horde Webmail is a free, enterprise-ready, and [...] The post Horde Webmail Software is affected by a dangerous bug since 2012 appeared first on Security Affairs.</p>
	<p><b>Iranian Broadcaster IRIB hit by wiper malware</b> Iranian national media corporation, Islamic Republic of Iran Broadcasting (IRIB), was hit by a wiper malware in late January 2022. An investigation into the attack that hit the Islamic Republic of Iran Broadcasting (IRIB) in late January, revealed the involvement of a disruptive wiper malware along with other custom-made backdoors, and scripts and configuration files [...] The post Iranian Broadcaster IRIB hit by wiper malware appeared first on Security Affairs.</p>	 <p><b>IRS offers live interview to replace facial recognition</b> US taxpayers signing up for an online account now have the option of a live interview to verify their identity instead of using ID.me facial recognition. Following discomfort surrounding their collection of biometric data, the IRS has offered the interviews as a short term solution for this year's filing system. The agency previously required taxpayers [...] The post IRS offers live interview to replace facial recognition appeared first on IT Security Guru.</p>
	<p><b>IRS: Selfies Now Optional, Biometric Data to Be Deleted</b> The U.S. Internal Revenue Service (IRS) said Monday that taxpayers are no longer required to provide facial scans to create an account online at irs.gov. In lieu of providing biometric data, taxpayers can now opt for a live video interview with ID.me, the privately-held Virginia company that runs the agency's identity proofing system. The IRS also said any biometric data already shared with ID.me would be permanently deleted over the next few weeks, and any biometric data provided for new signups will be destroyed after an account is created.</p>	 <p><b>Kids Luxury Clothing Store Melijoe Exposed 2 Million Files Due to Cloud Misconfiguration</b> An Amazon S3 bucket owned by the company was left accessible without authentication controls in place, exposing sensitive and personal data for potentially hundreds of thousands of customers.</p>
	<p><b>Malicious JS Libraries Distributed via Official NPM Package Repository to Steal Discord Tokens</b> Another batch of malicious JavaScript libraries have made their way to the official NPM package registry with the goal of stealing Discord tokens and environment variables from compromised systems.</p>	 <p><b>Malware authors target rivals with malicious npm packages</b> Trojan packages reveal what could be internal rivalry between cybercriminals.</p>
	<p><b>National Cyber Director Chris Inglis calls for 'new social contract' to redistribute risk</b> Cyberspace needs a "new social contract" where "isolated individuals, small businesses and local governments" no longer shoulder "absurd levels of risk," says a top U.S. cyber official. National Cyber Director Chris Inglis, writing in Foreign Affairs over the weekend with a senior adviser, said that the tech sector should make deeper investments in hardware and software security and the U.S. government should take a greater role in fostering digital defenses. "Those more capable of carrying the load -- such as governments and large firms -- must take on some of the burden, and collective, collaborative defense needs to replace atomized and divided efforts," write Inglis and Harry Krejsa, the[...]</p>	 <p><b>Payment card skimming reemerges with an online twist</b> Card skimming has been around for a long time and is undergoing a renaissance as financial fraudsters are recognizing new opportunities to combine physical world data theft with online intrusions.</p>
	<p><b>Phishing Group Used 40 Fake Mobile Service Top-up Sites to Steal Credit Cards</b> The Ukrainian Cyberpolice has arrested a group of phishing actors who managed to steal payment card data from at least 70,000 people after luring them to fake mobile service top-up sites.</p>	 <p><b>Police dismantled a gang that used phishing sites to steal credit cards</b> The Ukrainian police arrested a gang specialized in the sale of stolen payment card data through phishing attacks. The cybercrime unit of the Ukrainian police has arrested a group of cybercriminals who managed to steal payment card data from at least 70,000 people by setting up mobile fake top-up services. The police arrested five that created and [...] The post Police dismantled a gang that used phishing sites to steal credit cards appeared first on Security Affairs.</p>
	<p><b>Report: Missouri Governor's Office Responsible for Teacher Data Leak</b> Missouri Governor Mike Parson made headlines last year when he vowed to criminally prosecute a journalist for reporting a security flaw in a state website that exposed personal information of more than 100,000 teachers. But Missouri prosecutors now say they... Read More &gt;&gt;</p>	 <p><b>These new hacking groups are striking industrial, operational tech targets</b> Two of the new groups are sophisticated enough to reach ICS/OT networks directly.</p>
	<p><b>Threat actors target poorly protected Microsoft SQL Servers</b> Threat actors install Cobalt Strike beacons on vulnerable Microsoft SQL Servers to achieve a foothold in the target network. Researchers from Ahn Lab's ASEC spotted a new wave of attacks deploying Cobalt Strike beacons on vulnerable Microsoft SQL Servers to achieve initial access to target networks and deploy malicious payloads. The threat actors behind the [...] The post Threat actors target poorly protected Microsoft SQL Servers appeared first on Security Affairs.</p>	 <p><b>UK Defence Secretary warns Russia of cyber-retaliation</b> The UK's Secretary of State for Defence has reportedly warned Russia that they will retaliate with cyber attacks if the Kremlin targets British networks. The House of Commons statement from Ben Wallace follows President Putin's order to Russian troops to invade the separatist Donetsk and Luhansk regions of Ukraine. "I'm a soldier - I was always [...] The post UK Defence Secretary warns Russia of cyber-retaliation appeared first on IT Security Guru.</p>
	<p><b>Ukraine police arrest phishing group</b> The Ukrainian cyberpolice have arrested five individuals who stole credit card data from at least 70,000 people. The group of phishing actors lured people to fake mobile top up service sites. According to law enforcement, the actors used the stolen information to empty their victims' bank accounts. The phishing operation relied on marketing and advertising [...] The post Ukraine police arrest phishing group appeared first on IT Security Guru.</p>	 <p><b>USA to attack bad cyber actors if it protects victims</b> The DoJ has revealed new policies that may see it undertake pre-emptive action against cyber threats. Such actions will be undertaken if the DoJ feels that action can reduce risks for victims.</p>
	<p><b>Virsec Appoint Greg Kelton as Senior Regional Director for EMEA</b> Following on from their recent announcement of their Deterministic Protection Platform (DPP), California based software security firm Virsec have todayannounced the appointment of Greg Kelton as the new Senior Regional Director for EMEA, an appointment which will help to drive growth and expansion for Virsec in a key region. Greg is a hugely experienced software [...] The post Virsec Appoint Greg Kelton as Senior Regional Director for EMEA appeared first on IT Security Guru.</p>	 <p><b>Why DevOps pipelines are under attack and how to fight back</b> Software developers often have high permission levels and access privileges. If the software being produced is designed for external consumption, the impact of breaches can be dramatically greater.</p>
	<p><b>WordPress backup plugin maker Updraft says "You should update"...</b> A straight-talking bug report written in plain English by an actual expert - there's a teachable moment in this cybersecurity story!</p>	 <p><b>Xenomorph Malware Burrows into Google Play Users, No Facehugger Required</b> Researchers discovered a new, modular banking trojan with ties to Cerberus and Alien that has the capability to become a much larger threat than it is now.</p>
	<p><b>Zero-day RCE flaw among multiple bugs found in Extensis Portfolio - research</b> A group of cybersecurity researchers examined the source code of Extensis Portfolio version 3.6.3 and found a total of five vulnerabilities that required immediate attention.</p>	



Kathy  
Hochul

protection. That's why today we're announcing the first-in-the-nation, statewide Joint Security Operations Center, serving as the nerve center for joint local, state & federal cyber efforts.



Mayor  
Eric  
Adams

Cyber attacks can bring our entire city to a halt. The new Joint Security Operations Center will take our cybersecurity defenses to the next level. We're proud to stand shoulder to shoulder with @GovKathyHochul and my fellow New York Mayors in this critical fight.



Mayor  
Eric  
Adams

Brooklyn for a major announcement.



New York  
Post

Hochul details new cybersecurity plans as US braces for possible Russian hacks

Source: *NIST*

NIST CVE: Critical

*Nothing today*

Source: *NIST*

NIST CVE: High

*Nothing today*

Source: *NIST*

NIST CVE: Medium

*Nothing today*

Source: *NIST*

NIST CVE: Low

*Nothing today*

Source: *NIST*

NIST CVE: Unrated

CVE-2022-0654	Exposure of Sensitive Information to an Unauthorized Actor in <b>GitHub</b> repository fgribreau/node-request-retry prior to 7.0.0. <div>UNRATED</div> Vector: unknown Created: 2022-02-23 Updated: 2022-02-23	CVE-2022-0736	Insecure Temporary File in <b>GitHub</b> repository mlflow/mlflow prior to 1.23.1. <div>UNRATED</div> Vector: unknown Created: 2022-02-23 Updated: 2022-02-23
CVE-2022-0717	Out-of-bounds Read in <b>GitHub</b> repository mruby/mruby prior to 3.2. <div>UNRATED</div> Vector: unknown Created: 2022-02-23 Updated: 2022-02-23		

Source: *Hybrid Analysis*

Top malicious files

100% Threat score	KcsSetup (.) exe	100% Threat score	9008 fix (.) exe
100% Threat score	sti (.) dll	100% Threat score	LockDownBrowserOEMSetup (.) exe
100% Threat score	20220223_729296_005 (.) xls	100% Threat score	DATA SHEET (.) pdf (.) exe
100% Threat score	WGXMAN (.) DLL	100% Threat score	swntmpatcher (.) exe
100% Threat score	SARS Letter Of Summon (.) html	100% Threat score	PO 045647 (.) exe
100% Threat score	RunGame (.) exe	100% Threat score	pdfshaper_free_11 (.) 5 (.) exe
100% Threat score	LedBasic_15 (.) 3 (.) 1 (.) exe	100% Threat score	vlc-setup-win64 (.) exe
85% Threat score	Setup (.) exe	83% Threat score	lnv_1100 (.) html
80% Threat score	Ferdi-5 (.) 7 (.) 0 (.) msi	79% Threat score	Ecoromsrl 0222-001022 (.) exe
75% Threat score	Un_A (.) exe	75% Threat score	PentaCraft (.) exe
75% Threat score	Au_ (.) exe	75% Threat score	Hash_Suite_64 (.) exe

Source: *Hybrid Analysis*










Top malicious URL

100%	https://fabfloors (.) com/wp-main (.) php
------	---

Threat score	
89% Threat score	<a href="https://u24999073(.)ct(.)sendgrid(.)net/ls/click?upn=0Cj5LO2LyNYAe3Mk6sgJMmnjQBROixIDMYNpKjpa23pZcl16OpKLJbRWTY8WUgu-2FGjJRZoPybYp0wveYuwCT68vYWtAMZ-3DQQqB_5JEHDCGYhEXIHn36vdziKoQXdGkCwGAlhPDm4oG6TTynFAq2aB4ZrIGj4SFJFjkjUvjFXOjEI6ksVPVMW1bFmOOh0tjhFBRV5WXUVTIT0SuSiWx0NWRP9dVflvt9PhjXjkIVNO2FIAFYHiQCACnREZeG5i6amqNne1q4cMMAcxnPnn5yzGjPjYLw9hp1i58UA8k-3D">https://u24999073(.)ct(.)sendgrid(.)net/ls/click?upn=0Cj5LO2LyNYAe3Mk6sgJMmnjQBROixIDMYNpKjpa23pZcl16OpKLJbRWTY8WUgu-2FGjJRZoPybYp0wveYuwCT68vYWtAMZ-3DQQqB_5JEHDCGYhEXIHn36vdziKoQXdGkCwGAlhPDm4oG6TTynFAq2aB4ZrIGj4SFJFjkjUvjFXOjEI6ksVPVMW1bFmOOh0tjhFBRV5WXUVTIT0SuSiWx0NWRP9dVflvt9PhjXjkIVNO2FIAFYHiQCACnREZeG5i6amqNne1q4cMMAcxnPnn5yzGjPjYLw9hp1i58UA8k-3D</a>
81% Threat score	<a href="https://kalam(.)website/mikoeoeoeoe">https://kalam(.)website/mikoeoeoeoe</a>
77% Threat score	<a href="http://url6973(.)whatnextglobal(.)net(.)in/ls/click?upn=dnJqr9-2B-2FHiiTKXk1JYeDBuwtjZpraMXXRhN8nLqLdRS4BEv1P5SwPak3-2BX0-2BG0E-2B0dyup7Qpcqh6Re2Bwob0msMB69TcxnpYFaKO9rnHw9Fjl3tbyNoM0kqefuSngjR-2FOjFbr7X0r3Wv680ieqD9zdJc0p9-2FkeTjVSG-2B4K3iqfj2zIMXc1mHj99NBOBVMFQUxg-2BMdoGN3a72BHWYCCQyoVW0DU8rtZ-2BbqxpII0KzEn3U1oIoJNl6fmBFdZHSiGVUimgDGNMd-2FTIukj6nQA8iILvDY2SXfM0ZLKYSt2sDippxHaqSqO-2F6oayuSaGiGyRklTfQk1p2wgxk_azrjFSBAq7DzoEF6V41aeGjYVEN5L7GMgecdjbh3pSzynZLbggk2S2kxy6YIH9EXx2xEpo4DMV25tvVJjdWnUWP1jDc-2F9SKwS6EEWfb-2BOW8BS1qFYLtoJwLb7LG2BHkK6Pj6EAD3vOU07W2AHvPa15HZrOD8qdINPaE72-2B9T3RYD7FS85X-2BJjh0Et0GWLnW0H65a5G834aYrzt-2Fgkiq0Lc-3D">http://url6973(.)whatnextglobal(.)net(.)in/ls/click?upn=dnJqr9-2B-2FHiiTKXk1JYeDBuwtjZpraMXXRhN8nLqLdRS4BEv1P5SwPak3-2BX0-2BG0E-2B0dyup7Qpcqh6Re2Bwob0msMB69TcxnpYFaKO9rnHw9Fjl3tbyNoM0kqefuSngjR-2FOjFbr7X0r3Wv680ieqD9zdJc0p9-2FkeTjVSG-2B4K3iqfj2zIMXc1mHj99NBOBVMFQUxg-2BMdoGN3a72BHWYCCQyoVW0DU8rtZ-2BbqxpII0KzEn3U1oIoJNl6fmBFdZHSiGVUimgDGNMd-2FTIukj6nQA8iILvDY2SXfM0ZLKYSt2sDippxHaqSqO-2F6oayuSaGiGyRklTfQk1p2wgxk_azrjFSBAq7DzoEF6V41aeGjYVEN5L7GMgecdjbh3pSzynZLbggk2S2kxy6YIH9EXx2xEpo4DMV25tvVJjdWnUWP1jDc-2F9SKwS6EEWfb-2BOW8BS1qFYLtoJwLb7LG2BHkK6Pj6EAD3vOU07W2AHvPa15HZrOD8qdINPaE72-2B9T3RYD7FS85X-2BJjh0Et0GWLnW0H65a5G834aYrzt-2Fgkiq0Lc-3D</a>
77% Threat score	<a href="http://tracking(.)findaprospect(.)com/tracking/click?d=glfQYopWZjfpBEo6LpBN3Ocbark2kHi1e1K4jQzA4XBhrlMdcnI4dBTYzQS4c0DjpY6capf05hkPcVC_jzf9VEta3ivh7HF1q3AUCCpn1bt_savsAx6P_id8b8aO5Pk6hZ6RIZ-">http://tracking(.)findaprospect(.)com/tracking/click?d=glfQYopWZjfpBEo6LpBN3Ocbark2kHi1e1K4jQzA4XBhrlMdcnI4dBTYzQS4c0DjpY6capf05hkPcVC_jzf9VEta3ivh7HF1q3AUCCpn1bt_savsAx6P_id8b8aO5Pk6hZ6RIZ-</a>










Source: [SpamHaus](#)

Top spamming countries

	#1 United States of America		#2 China
	#3 Russian Federation		#4 Mexico
	#5 Dominican Republic		#6 Saudi Arabia
	#7 India		#8 Japan
	#9 Brazil		#10 Korea, Republic of








Source: [SpamHaus](#)

Top spammers

	<b>#1 Canadian Pharmacy</b> A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.		<b>#2 PredictLabs / Sphere Digital</b> This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.
	<b>#3 Hosting Response / Michael Boehm</b> Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.		<b>#4 Mint Global Marketing / Adgenics / Cabo Networks</b> Florida affiliate spammers and bulletproof spam hosters
	<b>#5 RetroCubes</b> Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.		<b>#6 Michael Persaud</b> Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
	<b>#7 Cyber World Internet Services/ e-Insites</b> Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.		<b>#8 RR Media</b> A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.
	<b>#9 Kobeni Solutions</b> High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.		

Source: [SpamHaus](#)

Top countries with botnet

	#1 China		#2 India
	#3 United States of America		#4 Thailand
	#5 Indonesia		#6 Algeria
	#7 Viet Nam		#8 Brazil

	#9 Pakistan		#10 Iran (Islamic Republic of)
---	-------------	---	--------------------------------

Source: [SpamHaus](#)

**Top phishing countries**

	#1 United States		#2 Russia
	#3 Germany		#4 Hong Kong
	#5 Netherlands		#6 India
	#7 France		#8 Thailand
	#9 United Kingdom		#10 Australia