



## Your Security Rabbits report for February 16, 2022

### Hot topics

#### Ukraine under DDOS

Ukraine is under DDOS attack. The Ministry of Defence, the Armed Forces and major banks are/were unreachable.

If this is today limited to Ukraine, Cybersecurity specialists fears this attacks spreads to other countries, like the USA. Brace yourself.

--  
JL Dupont

### News



CyberScoop

#### 'Razzlekhan' released on bond, husband detained ahead of cryptocurrency laundering trial

A U.S. judge Monday determined that Ilya Dutch Lichtenstein, one-half of the couple accused of a massive cryptocurrency laundering scheme, will await trial in prison. His wife and alleged co-conspirator, Heather Morgan, was set free on a \$3 million bond package, with the conditions of strict electronic monitoring and limits on her virtual currency accounts. Federal law enforcement arrested the pair earlier this month for allegedly conspiring to launder \$4.5 billion worth of cryptocurrency stolen in a 2016 hack of virtual cryptocurrency exchange Bitfinex. Lichtenstein and Morgan employed sophisticated money-laundering techniques that included the use of a combination of fictitious identities[...]



Cyware  
News -  
Latest Cyber  
News

#### BlackByte Ransomware Spreads Far and Wide, Attacks Critical Infrastructure

The Super Bowl came by and the BlackByte ransomware group claimed its target. Not only that, but the group has also attacked at least three critical infrastructure organizations in the U.S.



Threatpost

#### Chrome Zero-Day Under Active Attack: Patch ASAP

The year's 1st Chrome zero-day can lead to all sorts of misery, ranging from data corruption to the execution of arbitrary code on vulnerable systems.



Cyware  
News -  
Latest Cyber  
News

#### Cyber security company Securonix raises \$1 billion in Vista-led round

Cloud-based security solutions provider Securonix has raised more than \$1 billion in a private fundraising round led by private equity firm Vista Equity Partners, the company said on Monday.



IT Security  
Guru

#### DDoS attack hits Ukraine Defence and Bank Networks

The attacks knocked out the Ukrainian defence ministry's website and two bank networks were knocked out. According to the internet monitoring organisation NetBlocks, the attack hit on Tuesday afternoon and lasted for several hours. In a statement yesterday, the organisation revealed that "NetBlocks metrics confirm the loss of service to multiple banking and online platforms [...]" The post DDoS attack hits Ukraine Defence and Bank Networks appeared first on IT Security Guru.



ZDNet |  
security RSS

#### F5 launches new SaaS app security cloud, edge computing platform

The solution aims to simplify the F5 security portfolio.



Naked  
Security

#### Google announces zero-day in Chrome browser - update now!

Zero-day buses: none for a while, then three at once. Here's Google joining Apple and Adobe in "zero-day week"



IT Security  
Guru

#### 3 out of 5 cyber-attacks in 2021 were malware-free

A new report from CrowdStrike has revealed that ransomware-related data leaks increased by 82% year-on-year in 2021, but three-fifths of cyber attacks involved no malware whatsoever. The security company's 2022 Global Threat Report was put together using an analysis of its own incident response engagements and security telemetry. The report revealed that 62% of attacks used legitimate [...] The post 3 out of 5 cyber-attacks in 2021 were malware-free appeared first on IT Security Guru.



Security  
Affairs

#### BlackCat gang claimed responsibility for Swissport ransomware attack

The BlackCat ransomware group (aka ALPHV), claimed responsibility for the attack on Swissport that interfered with its operations. The BlackCat ransomware group (aka ALPHV), has claimed responsibility for the cyberattack on Swissport that impacted its operations, causing flight delays. Swissport International Ltd. is an aviation services company providing airport ground, lounge hospitality and cargo handling services owned by an international group of investors. [...] The post BlackCat gang claimed responsibility for Swissport ransomware attack appeared first on Security Affairs.



Security  
Affairs

#### CISA added 9 new flaws to the Known Exploited Vulnerabilities Catalog, including Magento e Chrome bugs

The U.S. CISA added to the Known Exploited Vulnerabilities Catalog another 9 security flaws actively exploited in the wild. US Cybersecurity and Infrastructure Security Agency (CISA) added nine new vulnerabilities to its Known Exploited Vulnerabilities Catalog, including two recently patched zero-day issues affecting Adobe Commerce/Magento Open Source and Google Chrome. CISA orders all Federal Civilian Executive [...] The post CISA added 9 new flaws to the Known Exploited Vulnerabilities Catalog, including Magento e Chrome bugs appeared first on Security Affairs.



Cyware  
News -  
Latest Cyber  
News

#### Cyberattackers Find New Interest in LOLBins to Spread a Variety of Malware

Living-off-the Land Binaries (LOLBins) are no joke; These system utility tools have become a new favorite attack channel for threat actors to hide their malicious activity from security solutions.



The Hacker  
News

#### EU Data Protection Watchdog Calls for Ban on Pegasus-like Commercial Spyware

The European Union's data protection authority on Tuesday called for a ban on the development and the use of Pegasus-like commercial spyware in the region, calling out the technology's "unprecedented level of intrusiveness" that could endanger users' right to privacy. "Pegasus constitutes a paradigm shift in terms of access to private communications and devices, which is able to affect the very



The Hacker  
News

#### Facebook Agrees to Pay \$90 Million to Settle Decade-Old Privacy Violation Case

Meta Platforms has agreed to pay \$90 million to settle a lawsuit over the company's use of cookies to allegedly track Facebook users' internet activity even after they had logged off from the platform. In addition, the social media company will be required to delete all of the data it illegally collected from those users. The development was first reported by Variety. The



CyberScoop

#### Google Cloud offers good news and bad news on Log4Shell, other issues

Google Cloud is seeing 400,000 scans per day for systems vulnerable to the Log4Shell bug, the company said Tuesday. The findings -- released as part of the company's semi-regular Threat Horizons report -- show that IT security professionals need to "keep paying attention to this, because the scans keep coming, and if you leave one vulnerable instance open, you're going to be found," Phil Venables, the chief information security officer at Google Cloud, told CyberScoop. That said, the companies interacting with Google Cloud have "been very much on top of this," according to Venables. The warning comes as a reminder, to security professionals to keep doing the work of finding the devi[...]

**Grafana web security vulnerability opened a plethora of attack possibilities**  
The CSRF flaw, tracked as CVE-2022-21703, opens the door for attackers to elevate privileges through cross-origin attacks against administrators on systems running vulnerable versions of Grafana.

**Netacea announces \$12Million Series A investment**  
The \$12 million Series A funding round will enable Netacea to expand its presence in the U.K. and the U.S., where the business sees significant opportunities for further growth.

**QNAP extends critical updates for some unsupported NAS devices**  
The company added that, while the support date has been moved until October, these EOL devices will only receive security updates addressing high severity and critical vulnerabilities.

**Questions linger after IRS's about-face on facial recognition**  
Why would a tax agency contractor's privacy policy mention collecting information about my Facebook friends? The post Questions linger after IRS's about-face on facial recognition appeared first on WeLiveSecurity

**SafeDNS: Cloud-based Internet Security and Web Filtering Solution for MSPs**  
Remote workplace trend is getting the upper hand in 2022. A recent survey by IWG (the International Workplace Group) determined that 70% of the world's professionals work remotely at least one day a week, with 53% based outside their workplace at least half of the week. Taking this into consideration, organizations have started looking for reliable partners that can deliver services and support

**SMS PVA Services' Use of Infected Android Phones Reveals Flaws in SMS Verification**  
The core security issue is that an enterprise has the ability to monitor and intercept SMSes from tons of devices globally, and then profit from it by offering the service to whoever can pay for it.

**Squirrelwaffle, Microsoft Exchange Server vulnerabilities exploited for financial fraud**  
Unpatched servers have been used to twist corporate email threads and conduct financial theft.

**TrickBot developers continue to refine the malware's sneakiness and power**  
The versatile malware known as TrickBot continues to pose "great danger" to customers of financial and technology companies because its developers are trying to stay a step ahead of cybersecurity analysts, according to Check Point Research. The company says TrickBot's authors have equipped it with layers of "anti-analysis" and "anti-deobfuscation" capabilities, meaning that if an expert tries to pick apart the malware's code, it stops communicating with its command-and-control servers or stops working altogether. Those features "show the authors' highly technical background and explain why Trickbot remains a very prevalent malware family," Check Point says in research published Wednesday. Th[...]

**Ukrainian government says websites for banks, defense ministry hit with DDoS attacks**  
Websites for several banks and government agencies in Ukraine -- including the Ministry of Defense, Ministry of Internal Affairs and the Armed Forces of Ukraine -- were facing disruptions Tuesday, according to multiple sources. Ukraine's Center for Strategic Communications and Information Security posted a message to Facebook late morning U.S. time saying the banks and the government were hit by a "massive" distributed denial-of-service (DDoS) cyberattack. The Ministry of Defense tweeted that it had "probably" been targeted with DDoS, and that it was communicating via Facebook and Twitter. The Ukrainian State Service of Special Communication and Information Protection called it a "powerful D[...]"

**VMware fixes flaws demonstrated at Chinese Tianfu Cup hacking contest**  
VMware addressed several high-severity flaws that were disclosed during China's Tianfu Cup hacking contest. VMware addressed several high-severity vulnerabilities that were demonstrated by Kunlun Lab team during China's Tianfu Cup 2021 hacking contest. The vulnerabilities impact VMware ESXi, Workstation, and Fusion. Below is the list published by the virtualization giant: CVE-2021-22040 - VMware ESXi, Workstation, and [...] The post VMware fixes flaws demonstrated at Chinese Tianfu Cup hacking contest appeared first on Security Affairs.

**Watch Out! FritzFrog Botnet Has Gone Aggressively Wild**  
The operators of the FritzFrog botnet have returned with a new P2P campaign, registering a 10x growth in the infection rate within only a month. The new variant seems to possess additional capabilities to target WordPress servers. Researchers have spotted 24,000 attacks so far. However, the botnet has claimed only 1,500 victims. Be warned, the botnet is aggressively expanding its attack surface with new features.

**High-Severity RCE Security Bug Reported in Apache Cassandra Database Software**

Researchers have revealed details of a now-patched high-severity security vulnerability in Apache Cassandra that, if left unaddressed, could be abused to gain remote code execution (RCE) on affected installations. "This Apache security vulnerability is easy to exploit and has the potential to wreak havoc on systems, but luckily only manifests in non-default configurations of Cassandra," Omer

**New tool can uncover redacted, pixelated text to reveal sensitive data**

Researchers have demonstrated how a new tool named Unredacter can help uncover redacted text from documents, potentially exposing sensitive information to nefarious actors.

**QNAP extends security Updates for some EOL devices**

Taiwanese vendor QNAP extended the security update window for some devices that have reached end-of-life (EOL). Taiwanese vendor QNAP extended the security update for some devices that have reached end-of-life (EOL) years ago. The company decided to extend until October this year the security updates for some models that have reached EOL, the decision aims [...] The post QNAP extends security Updates for some EOL devices appeared first on Security Affairs.

**Researchers Link ShadowPad Malware Attacks to Chinese Ministry and PLA**  
Cybersecurity researchers have detailed the inner workings of ShadowPad, a sophisticated and modular backdoor that has been adopted by a growing number of Chinese threat groups in recent years, while also linking it to the country's civilian and military intelligence agencies. "ShadowPad is decrypted in memory using a custom decryption algorithm," researchers from Secureworks said in a report

**Small businesses facing upwards of 11 cyberthreats per day per device**

BlackBerry Limited has released the 2022 BlackBerry Annual Threat Report, highlighting a cybercriminal underground which it says has been optimised to better target local small businesses. Small businesses will continue to be an epicentre for cybercriminal focus as SMBs facing upward of 11 cyberthreats per device per day, which only stands to accelerate as cybercriminals [...] The post Small businesses facing upwards of 11 cyberthreats per day per device appeared first on IT Security Guru.

**SquirrelWaffle Adds a Twist of Fraud to Exchange Server Malspamming**

Researchers have never before seen SquirrelWaffle attackers use typosquatting to keep sending spam once a targeted Exchange server has been patched for ProxyLogon/ProxyShell.

**TA2541: APT Has Been Shooting RATs at Aviation for Years**

Since 2017, the attacker has flung simple off-the-shelf malware in malicious email campaigns aimed at aviation, aerospace, transportation and defense.

**Ukraine: Military defense agencies and banks hit by cyberattacks**

Ukraine 's defense agencies and two state-owned banks were hit by Distributed Denial-of-Service (DDoS) attacks. The Ministry of Defense and the Armed Forces of Ukraine and state-owned banks, Privatbank (Ukraine's largest bank) and Oschadbank were hit by Distributed Denial-of-Service (DDoS) attacks. The website of the Ukrainian Ministry of Defense has been taken down by the wave of [...] The post Ukraine: Military defense agencies and banks hit by cyberattacks appeared first on Security Affairs.

**Ukrainian Military Agencies, State-Owned Banks Suffer Disruptive Cyberattacks**

Ukraine's Cyberpolice also reported that bank customers received SMS messages claiming that bank ATMs were down, adding that they were "part of an information attack and do not correspond to reality."

**VMware Patches Vulnerabilities Reported by Researchers to Chinese Government**

The security vulnerabilities impact VMware ESXi, Workstation, and Fusion, and they were used at the 2021 Tianfu Cup hacking contest by Kunlun Lab, the team that won the event.

**Years of hacks against aviation, transportation industries tied to one group, researchers say**

Analysts have noticed various attempts in recent years by hackers trying to breach entities in the aviation and aerospace industries, as well as related transportation fields. The operators typically use of off-the-shelf malware and deploy digital lures that refer to industry-specific topics like airline cargo conferences or machine parts. It now appears that most of those incidents were by the same group, according to cybersecurity firm Proofpoint. Dubbing the group "TA2541," Proofpoint said Tuesday that the trail of evidence goes back to at least 2017, and the hackers remain a "consistent, active cybercrime threat." Hundreds of different organizations have been targeted globally, with an e[...]

NIST CVE: Critical			
CVE-2021-39997	There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access.		
	CRITICAL	Vector: network	Created: 2022-02-09   Updated: 2022-02-16

CVE-2021-39994	There is an arbitrary address access vulnerability with the product line test code.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.		
	CRITICAL	Vector: network	Created: 2022-02-09   Updated: 2022-02-16

NIST CVE: High			
CVE-2022-24315	A CWE-125: Out-of-bounds Read vulnerability exists that could cause denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)		
	HIGH	Vector: network	Created: 2022-02-09   Updated: 2022-02-16

CVE-2022-24316	A CWE-665: Improper Initialization vulnerability exists that could cause information exposure when an attacker sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)		
	HIGH	Vector: network	Created: 2022-02-09   Updated: 2022-02-16

CVE-2021-39992	There is an improper security permission configuration vulnerability on ACPU.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.		
	HIGH	Vector: local	Created: 2022-02-09   Updated: 2022-02-16

CVE-2022-24314	A CWE-125: Out-of-bounds Read vulnerability exists that could cause memory leaks potentially resulting in denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: <b>Interactive Graphical SCADA System</b> Data Server (V15.0.0.22020 and prior)		
	HIGH	Vector: network	Created: 2022-02-09   Updated: 2022-02-16

CVE-2021-40044	There is a permission verification vulnerability in the <b>Bluetooth</b> module.Successful exploitation of this vulnerability may cause unauthorized operations.		
	HIGH	Vector: adjacent_network	Created: 2022-02-09   Updated: 2022-02-16







Top malicious files			
100% Threat score	Thunderbird20Setup2091 (.) 6 (.) 3 (.) exe		
100% Threat score	tmpunh9menx		
100% Threat score	tmpb8jrwpf5		
100% Threat score	tmpfn_trl0g		
100% Threat score	winexesvc (.) exe_		
100% Threat score	P402 (.) Hermes (.) LC (.) 632_SecureBootOff (.) LC (.) exe		
100% Threat score	v_MULTI_MIX_HEAVY_413ebd37620cfcb229322a0f3217ae8a6a61163eb73b14a30e3d8d5a68847f1b_0 (.) exe		
100% Threat score	Thunderbird20Setup2091 (.) 6 (.) 0 (.) exe		
100% Threat score	LM-1399530119 (.) txt		
100% Threat score	nanocore (.) dot		
100% Threat score	LuminarAISetup_144033_5 (.) exe		
100% Threat score	8ba2ac3bda200bade5d7f2a643587df7e44410883a22e56646a257e778d99c28		
100% Threat score	AnyDesk_144032_5 (.) exe		
100% Threat score	tmp7yq0yq7d		
100% Threat score	tmpkrjmw_i_9		
97% Threat score	tmppra2fxh3h		
85% Threat score	MH Thump Installer (.) exe		
77%	tmpqmqm2ezi2k		
100% Threat score	Online Banking Payment Advice (.) exe		
100% Threat score	tmpo3glrt8g		
100% Threat score	tmp9ithdgni		
100% Threat score	csrss (.) exe		
100% Threat score	tmp3ocnqjka		
100% Threat score	v_MULTI_MIX_HEAVY_5e244bf3a2fe36942e9e001bbb6677f6cf (.) exe		
100% Threat score	QWBTS421267 (.) VBS		
100% Threat score	N̂%ĐĐ@N̂`â••N̂...Đ«â•N̂...Đ%ĐN̂`â•jĐ`N̂„â•ĐN̂...ĐŸĐN̂`â•—Đ` (.) exe		
100% Threat score	tmprt8eb4j9		
100% Threat score	Thunderbird20Setup2091 (.) 6 (.) 2 (.) exe		
100% Threat score	825pdf (.) vbs		
100% Threat score	tmpjkmgyutk		
100% Threat score	tmpgeggwyoh		
100% Threat score	tmp60tpphq		
97% Threat score	tmp5s350hnc		
91% Threat score	tmpsf23c5ob		
80% Threat score	LocalServiceComponents (.) exe		
75%	OopsRelease (.) exe		

Threat score		Threat score	
75% Threat score	WindowexeAllkiller (.) exe		










Source: Hybrid Analysis

Top malicious URL			
100% Threat score	http://124 (.) 131 (.) 197 (.) 133:44392/bin (.) sh	100% Threat score	https://estudiombm (.) com/pos/canadapost (.) reschedule (.) portal (.) services (.) parcel (.) html
100% Threat score	https://safeproperjavadocs (.) ti02222 (.) repl (.) co/	88% Threat score	http://115 (.) 50 (.) 127 (.) 248:53511/bin (.) sh
88% Threat score	http://1 (.) 196 (.) 250 (.) 145:39460/i	88% Threat score	http://117 (.) 241 (.) 182 (.) 69:39305/i
77% Threat score	http://avidclever424 (.) weebly (.) com/	77% Threat score	http://myah (.) azurewebsites (.) net/frontoffice/#%2Fauth%2Flogin
75% Threat score	https://fortunezipperbd (.) com/cgi-sys/suspendedpage (.) cgi	74% Threat score	https://www (.) facebook (.) com/pages/category/Clothing-store/Splash-Fashions-1597412503888133/
74% Threat score	https://fortunezipperbd (.) com/facture/weds/office/	72% Threat score	http://a1-1111asa00a0a0a1s2a1s2as121sa2a1s2as12a (.) bolpeoak (.) xyz/
72% Threat score	https://m4gbp7os4r (.) efigur (.) com/82		

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 Iran (Islamic Republic of)		#10 Pakistan

Source: [SpamHaus](#)

Top phishing countries			
	#1 United States		#2 Germany
	#3 Netherlands		#4 Russia
	#5 Hong Kong		#6 Singapore
	#7 France		#8 Ireland
	#9 Australia		#10 India