



Your Security Rabbits report for March 24, 2022

Source: [Ransom Watch](#)











Ransomware attacks

























conti	Shapiro and Duncan	lockbit2	redgwick.com
alphv	Bradsby Group bradsbygroup.com	vicesociety	Establishment of the Agency for the Environmental Protection of the Marche Region
lockbit2	ignitarium.com	stormous	3S Standard Sharing Software
lockbit2	intouchgroup.ne...	alphv	LW Group
hiveleak	KONECTA SERVICIOS ADMINISTRATIVOS Y TECNOLOGICOS S.L SUCURSAL ARGENTINA	hiveleak	Instituto De Gesto EstratÁfica De Sade Do Distrito Federal
hiveleak	Wibag Bau Ag	cuba	powertech
midas	NetCompany	everest	Ministry of Economy and Finance of Peru
alphv	Maintainco Inc. maintainco.com starlift.com	alphv	KELLY,REMME&ZIMMERMAN first part
cuba	haltonhills	lockbit2	crich.it
lockbit2	credenceid.com	lockbit2	confindustriaca...
hiveleak	Banco Caribe	lockbit2	avidoc.fr
hiveleak	Asphalion		






Hot topics

Nothing today





News

 IT Security Guru	12,000 sensitive patient images leaked A medical Q&A service provider is facing criticism about its security processes after a cloud misconfiguration appeared to leak sensitive images of thousands of patients. A team at Safety Detectives reportedly discovered the Amazon S3 bucket, before tracing it to a Japanese firm called Doctors Me. There was reportedly no authentication controls in place, leaving [...] The post 12,000 sensitive patient images leaked appeared first on IT Security Guru.	 Krebs on Security	A Closer Look at the LAPSUS\$ Data Extortion Group Microsoft and identity management platform Okta both disclosed this week breaches involving LAPSUS\$, a relatively new cybercrime group that specializes in stealing data from big companies and threatening to publish the information unless a ransom demand is paid. Here's a closer look at LAPSUS\$, and some of the low-tech but high-impact methods the group uses to gain access to targeted organizations.
 Blog & Flashpoint	All About LAPSUS\$: What We Know About the Extortionist Group LAPSUS\$ is an extortionist threat group that became active on December 10, 2021. Unlike the majority of extortionist groups that typically rely on a combination of ransomware and data leaks, LAPSUS\$ is focused on monetizing their operations exclusively through data leaks advertised on Telegram without the use of ransomware. Initially, the group focused on data [...] The post All About LAPSUS\$: What We Know About the Extortionist Group appeared first on Flashpoint.	 Security Affairs	Anonymous claims to have hacked the Central Bank of Russia The Anonymous hacker collective claims to have hacked the Central Bank of Russia and stole accessed 35,000 documents. Anonymous continues to target Russian government organizations and private businesses, now it is claiming to have hacked the Central Bank of Russia. The popular hacker collective claims to have compromised the systems of the Central Bank of [...] The post Anonymous claims to have hacked the Central Bank of Russia appeared first on Security Affairs.
 IT Security Guru	Anonymous leaks 10GB of Nestle Data The hacktivist and activist group known as Anonymous has released Nestle's database. The move comes days after the Ukrainian President Zelensky called out the world's largest food company for its continued relationship with Russia. Anonymous announced the breach in a tweet on Tuesday: "Hacker group Anonymous has released 10 GB of data from Swiss company [...] The post Anonymous leaks 10GB of Nestle Data appeared first on IT Security Guru.	 Cyware News - Latest Cyber News	APT Group Targets Betting Companies Using MulCom Backdoor in Taiwan, the Philippines, and Hong Kong Due to the similarities between the MulCom backdoor used by this group and FFRat, researchers suspect that the FFRat codebase is being shared between several Chinese adversary groups.
 Cyware News - Latest Cyber News	Background Check Company Sued Over Data Breach Creative Services, Inc. (CSI), located in Mansfield, provides background screening, drug testing and security consulting services to employers, institutions and governments in the United States and overseas.	 Cyware News - Latest Cyber News	BitRAT Spreads as Windows Activator A new BitRAT malware campaign is leveraging illegal crack tools for Windows 10 license verification. The campaign targets users looking to activate pirated Windows OS versions on webhards for free. BitRAT supports generic keylogging, audio recording, clipboard monitoring, credential theft from web browsers, webcam access, XMRIg coin mining, and several additional features. Companies are urged to use reliable anti-malware solutions to stay protected from such threats.
 The Hacker News	Botnet of Thousands of MikroTik Routers Abused in Glupteba, TrickBot Campaigns Vulnerable routers from MikroTik have been misused to form what cybersecurity researchers have called one of the largest botnet-as-a-service cybercrime operations seen in recent years. According to a new piece of research published by Avast, a cryptocurrency mining campaign leveraging the new-disrupted Glupteba botnet as well as the infamous TrickBot malware were all distributed using the same	 Cyware News - Latest Cyber News	Browser-in-the-Browser - An (Almost) Invisible Attack Researchers devised a new phishing technique, dubbed Browser-in-the-Browser (BitB) attack that lets cybercriminals spoof a browser window within a browser by leveraging a mix of HTML and CSS code. The novel BitB attack bypasses both a URL with HTTPS encryption and a hover-over-it security check. Researchers suggest using secure proof of identity via a registered device or token.

 <div>Security Affairs</div>	<div>China-linked GIMMICK implant now targets macOS</div> <p>Gimmick is a newly discovered macOS implant developed by the China-linked APT Storm Cloud and used to target organizations across Asia. In late 2021, Volexity researchers investigated an intrusion in an environment they were monitoring and discovered a MacBook Pro running macOS 11.6 (Big Sur) that was compromised with a previously unknown macOS malware tracked [...] The post China-linked GIMMICK implant now targets macOS appeared first on Security Affairs.</p>	 <div>The Hacker News</div>	<div>Chinese 'Mustang Panda' Hackers Spotted Deploying New 'Hodur' Malware</div> <p>A China-based advanced persistent threat (APT) known as Mustang Panda has been linked to an ongoing cyber espionage campaign using a previously undocumented variant of the PlugX remote access trojan on infected machines. Slovak cybersecurity firm ESET dubbed the new version Hodur, owing to its resemblance to another PlugX (aka Korplug) variant called THOR that came to light in July 2021. "Most</p>
 <div>Cyware News - Latest Cyber News</div>	<div>Chinese Mustang Panda Hacker Group Spotted Deploying New Hodur Malware</div> <p>ESET researchers have discovered Hodur, a previously undocumented Korplug variant spread by Mustang Panda, that uses phishing lures referencing current events in Europe, including the invasion of Ukraine.</p>	 <div>Threatpost</div>	<div>DeadBolt Ransomware Resurfaces to Hit QNAP Again</div> <p>A new steady stream of attacks against network-attached storage devices from the Taiwan-based vendor is similar to a wave that occurred in January.</p>
 <div>Cyware News - Latest Cyber News</div>	<div>DirtyMoe Modules Introduce Worm-Like Features</div> <p>Avast researchers have observed three main ways in which the malware is being disseminated - PurpleFox EK, PurpleFox Worm, and injected Telegram installers. It is likely that the malware propagates through other methods too.</p>	 <div>Cyware News - Latest Cyber News</div>	<div>EDoS: The Next Big Threat to Your Cloud</div> <p>EDoS attacks exploit the elasticity of clouds, particularly auto-scaling capabilities, to inflate the billing of a cloud user until the account reaches bankruptcy or large-scale service withdrawal.</p>
 <div>Cyware News - Latest Cyber News</div>	<div>Fastest Ransomware Encrypts 100k Files in Four Minutes</div> <p>In order of fastest first, the ransomware variants analyzed by Splunk were: LockBit; Babuk; Avaddon; Ryuk; REvil; BlackMatter; DarkSide; Conti; Maze; and Mespinoza (Pysa).</p>	 <div>Security Affairs</div>	<div>FBI warns of growing risks of Russia-linked attacks on US energy firms</div> <p>The FBI is warning of risks related to cyber attacks aimed at energy companies of Russia-linked threat actors. The FBI is warning energy companies of the risks of cyber attacks carried out by Russia-linked threat actors, reported The Associated Press. The Associated Press has access to a security advisory issued by the FBI that reports [...] The post FBI warns of growing risks of Russia-linked attacks on US energy firms appeared first on Security Affairs.</p>
 <div>Cyware News - Latest Cyber News</div>	<div>FBI Warns of Growing Russian Hacking Activity Targeting US Energy Firms</div> <p>The FBI advisory shares 140 internet protocol, or IP, addresses that it says have been associated with the scanning of critical infrastructure in the U.S. since at least March 2021.</p>	 <div>CyberScoop</div>	<div>FBI: Cybercrime reports saw 'unprecedented' rise last year, costing nearly \$7B</div> <p>Business email compromise again proved costliest, at \$2.4 billion, according to the bureau's Internet Crime Complaint Center The post FBI: Cybercrime reports saw 'unprecedented' rise last year, costing nearly \$7B appeared first on CyberScoop.</p>
 <div>Security Affairs</div>	<div>It's official, Lapsus\$ gang compromised a Microsoft employee's account</div> <p>Microsoft confirmed that Lapsus\$ extortion group has hacked one of its employees to access and steal the source code of some projects. Microsoft confirmed that Lapsus\$ extortion group has hacked one of its employees to access and steal the source code of some projects. Yesterday the cybercrime gang leaked 37GB of source code stolen from [...] The post It's official, Lapsus\$ gang compromised a Microsoft employee's account appeared first on Security Affairs.</p>	 <div>ZDNet security RSS</div>	<div>Malicious npm packages target Azure developers to steal personal data</div> <p>Typosquatting and automatic tools are the weapons of choice.</p>
 <div>Threatpost</div>	<div>Microsoft: Lapsus\$ Used Employee Account to Steal Source Code</div> <p>The data-extortion gang got at Microsoft's Azure DevOps server. Meanwhile, fellow Lapsus\$ victim and authentication firm Okta said 2.5 percent of customers were affected in its own Lapsus\$ attack.</p>	 <div>WeLiveSecurity</div>	<div>Mustang Panda's Hodur: Old tricks, new Korplug variant</div> <p>ESET researchers have discovered Hodur, a previously undocumented Korplug variant spread by Mustang Panda, that uses phishing lures referencing current events in Europe, including the invasion of Ukraine The post Mustang Panda's Hodur: Old tricks, new Korplug variant appeared first on WeLiveSecurity</p>
 <div>Cyware News - Latest Cyber News</div>	<div>New JSSLoader Trojan Delivered Through XLL Files</div> <p>Attackers are now using .XLL files to deliver a new, obfuscated version of JSSLoader. This new malware variant utilizes the Excel add-ins feature to load the malware and inspect the changes inside.</p>	 <div>Cyware News - Latest Cyber News</div>	<div>Nucleus Security raises \$20 million to boost product development and enhance customer experience</div> <p>This funding will be used to accelerate product development and enhance customer experience, scale engineering and support services, expand presence in APAC, as well as invest in the company's people and culture.</p>
 <div>ZDNet security RSS</div>	<div>Okta names Sitel in Lapsus\$ security incident impacting up to 366 customers</div> <p>The analogy "walking away from your computer at a coffee shop" has been used to describe the incident.</p>	 <div>CyberScoop</div>	<div>Okta says 366 customers potentially affected in data breach</div> <p>Customer data is safe, the company says. But an Okta official says it would have handled some things differently. The post Okta says 366 customers potentially affected in data breach appeared first on CyberScoop.</p>
 <div>Security Affairs</div>	<div>Okta says 375 customers impacted by the hack, but Lapsus\$ gang says it is lying</div> <p>The provider of access management systems Okta confirmed the data breach and revealed that 2.5% of its customers were impacted. This week Lapsus\$ extortion group claimed to have stolen sensitive data from the identity and access management giant Okta solutions. The gang announced the alleged hack through its Telegram channel and shared a series of screenshots [...] The post Okta says 375 customers impacted by the hack, but Lapsus\$ gang says it is lying appeared first on Security Affairs.</p>	 <div>The Hacker News</div>	<div>Over 200 Malicious NPM Packages Caught Targeting Azure Developers</div> <p>A new large scale supply chain attack has been observed targeting Azure developers with no less than 218 malicious NPM packages with the goal of stealing personal identifiable information. "After manually inspecting some of these packages, it became apparent that this was a targeted attack against the entire @azure NPM scope, by an attacker that employed an automatic script to create accounts</p>
 <div>The Hacker News</div>	<div>Researchers Trace LAPSUS\$ Cyber Attacks to 16-Year-Old Hacker from England</div> <p>Authentication services provider Okta on Wednesday named Sitel as the third-party linked to a security incident experienced by the company in late January that allowed the LAPSUS\$ extortion gang to remotely take over an internal account belonging to a customer support engineer. The company added that 366 corporate customers, or about 2.5% of its customer base, may have been impacted by the "</p>	 <div>CyberScoop</div>	<div>Russian indicted, added to 'Most Wanted' in cybercrime market case</div> <p>Igor Dekhtyarchuk allegedly ran the cybercrime forum Marketplace A, which specialized in stolen credit card data and website logins. The post Russian indicted, added to 'Most Wanted' in cybercrime market case appeared first on CyberScoop.</p>
 <div>CyberScoop</div>	<div>Senate ransomware investigation says FBI leaving victims in the lurch</div> <p>The report includes three case studies of ransomware attacks against U.S. companies within the past five years. The post Senate ransomware investigation says FBI leaving victims in the lurch appeared first on CyberScoop.</p>	 <div>Naked Security</div>	<div>Serious Security: DEADBOLT - the ransomware that goes straight for your backups</div> <p>Some tips on how to keep your network safe - even (or perhaps especially!) if you think you're safe already.</p>
 <div>Blog à€" Flashpoint</div>	<div>Shields Up: Understanding Guidance From the Biden Administration About Possible Russian Cyberattacks</div> <p>On Monday March 21, the Biden Administration released several statements stressing the importance of cybersecurity, warning the private sector of potential malicious cyber activity from Russia. Biden implored companies to "harden your cyber defenses immediately" and explicitly named CISA's Shields Up campaign as the best way to do so. This announcement, which comes smack in [...] The post Shields Up: Understanding Guidance From the Biden Administration About Possible Russian Cyberattacks appeared first on</p>	 <div>Cyware News - Latest Cyber News</div>	<div>Slithering Serpent - New Backdoor and a Unique Attack Chain</div> <p>An unknown and likely sophisticated threat actor is leveraging a unique amalgamation of open-source software, a detection bypass technique, and steganography to attack French entities.</p>

	Flashpoint.		
	Theta Lake raises \$50 million to help organizations manage complex security and compliance issues Theta Lake announced a \$50 million Series B funding round led by Battery Ventures. The new investment brings the company's total funding raised to date to over \$70 million.		This is how much the average Conti hacking group member earns a month While ransom payments can reach millions of dollars, it isn't as much as you'd think.
	Ukrainian enterprises hit with the DoubleZero wiper Ukraine CERT-UA warns of cyberattack aimed at Ukrainian enterprises using the a wiper dubbed DoubleZero. Ukraine CERT-UA continues to observe malware based attacks aimed at Ukrainian organizations, in a recent alert it warned of attacks employing a wiper dubbed DoubleZero. The government CERT started observing this campaign on March 17, 2022, threat actors launched spear-phishing [...] The post Ukrainian enterprises hit with the DoubleZero wiper appeared first on Security Affairs.		VMware Issues Patches for Critical Flaws Affecting Carbon Black App Control VMware on Wednesday released software updates to plug two critical security vulnerabilities affecting its Carbon Black App Control platform that could be abused by a malicious actor to execute arbitrary code on affected installations in Windows systems. Tracked as CVE-2022-22951 and CVE-2022-22952, both the flaws are rated 9.1 out of a maximum of 10 on the CVSS vulnerability scoring system.
	Weeks after launch, Island hits \$1.3B valuation with \$115M round The round was led by previous lead investor Insight Partners, and comes just weeks after the New York-based venture capital firm raised over \$20 billion for its 12th flagship fund.		

Twitter

 <div>Rep. Val Demings</div>	Last night we passed the federal budget to keep us SAFE. I voted to strengthen Americas military and provide strong resources for: - Securing our border - Homeland security grants that protect communities & houses of worship - Cybersecurity - Coast Guard and port security	 <div>Dave Rubin</div>	This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[...]
 <div>Gary Gensler</div>	Join us in now at our Investor Advisory Committee Meeting. Todays agenda includes a panel on artificial intelligence and robo-advising and a discussion on cybersecurity disclosures.	 <div>Spiros Margaris</div>	The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam

Source: *NIST*

NIST CVE: Critical

CVE-2021-23632	All versions of package git are vulnerable to Remote Code Execution (RCE) due to missing sanitization in the Git.git method, which allows execution of OS commands rather than just git commands. Steps to Reproduce 1. Create a file named exploit.js with the following content: <pre>js var Git = require("git").Git; var repo = new Git("repo-test"); var user_input = "version; date"; repo.git(user_input, function(err, result) { console.log(result); }) 2. In the same directory as exploit.js, run npm install git. 3. Run exploit.js: node exploit.js. You should see the outputs of both the git version and date command-lines. Note that the repo-test Git repository does not need to be present to make this PoC work.</pre> <div>CRITICAL Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>	CVE-2020-15591	fexsrv in F*EX (aka Fram's Fast File EXchange) before fex-20160919_2 allows eval injection (for unauthenticated remote code execution). <div>CRITICAL Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>
CVE-2021-44908	SailsJS Sails.js <=1.4.0 is vulnerable to Prototype Pollution via controller/load-action-modules.js, function loadActionModules(). <div>CRITICAL Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>	CVE-2022-25352	The package libnested before 1.5.2 are vulnerable to Prototype Pollution via the set function in index.js. Note: This vulnerability derives from an incomplete fix for [CVE-2020-28283] (https://security.snyk.io/vuln/SNYK-JS-LIBNESTED-1054930) <div>CRITICAL Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>
CVE-2022-0748	The package post-loader from 0.0.0 are vulnerable to Arbitrary Code Execution which uses a markdown parser in an unsafe way so that any javascript code inside the markdown input files gets evaluated and executed. <div>CRITICAL Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>	CVE-2022-25354	The package set-in before 2.0.3 are vulnerable to Prototype Pollution via the setIn method, as it allows an attacker to merge object prototypes into it. Note: This vulnerability derives from an incomplete fix of [CVE-2020-28273](https://security.snyk.io/vuln/SNYK-JS-SETIN-1048049) <div>CRITICAL Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>
CVE-2022-0749	This affects all versions of package SinGooCMS.Utility. The socket client in the package can pass in the payload via the user-controllable input after it has been established, because this socket client transmission does not have the appropriate restrictions or type bindings for the BinaryFormatter. <div>CRITICAL Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>		

Source: *NIST*

NIST CVE: High

CVE-2021-45794	Slims9 Bulian 9.4.2 is affected by SQL injection in /admin/modules/system/backup.php. User data can be obtained. <div>HIGH Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>	CVE-2021-45793	Slims9 Bulian 9.4.2 is affected by SQL injection in lib/comment.inc.php. User data can be obtained. <div>HIGH Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>
CVE-2022-25296	The package bodymen from 0.0.0 are vulnerable to Prototype Pollution via the handler function which could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload. Note: This vulnerability derives from an incomplete fix to [CVE-2019-10792] (https://security.snyk.io/vuln/SNYK-JS-BODYMEN-548897) <div>HIGH Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>	CVE-2022-21221	The package github .com/valyala/fasthttp before 1.34.0 are vulnerable to Directory Traversal via the ServeFile function, due to improper sanitization. It is possible to be exploited by using a backslash %5c character in the path. Note: This security issue impacts Windows users only. <div>HIGH Vector: network Created: 2022-03-17 Updated: 2022-03-24</div>

NIST CVE: Medium

CVE-2021-23771

This affects all versions of package notevil; all versions of package argencoders-notevil. It is vulnerable to Sandbox Escape leading to Prototype pollution. The package fails to restrict access to the main context, allowing an attacker to add or modify an object's prototype.
Note: This vulnerability derives from an incomplete fix in [SNYK-JS-NOTEVIL-608878](https://security.snyk.io/vuln/SNYK-JS-NOTEVIL-608878).

MEDIUM Vector: network Created: 2022-03-17 Updated: 2022-03-24

NIST CVE: Low

Nothing today

NIST CVE: Unrated

CVE-2021-31326

D-Link DIR-816 A2 1.10 B05 allows unauthenticated attackers to arbitrarily reset the device via a crafted tokenid parameter to /goform/form2Reboot.cgi.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27811

GNOME OCRFeeder before 0.8.4 allows OS command injection via shell metacharacters in a PDF or image filename.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-0315

Insecure Temporary File in GitHub repository horovod/horovod prior to 0.24.0.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27820

OWASP Zed Attack Proxy (ZAP) through w2022-03-21 does not verify the TLS certificate chain of an HTTPS server.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27083

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadAccessCodePic.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27077

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadWeiXinPic.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27076

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/delAd.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-26289

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/exeCommand.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27078

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setAdInfoDetail.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-26536

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setFixTools.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27082

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetInternetLanInfo.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27081

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetLanInfo.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27079

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setPicListItem.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-27080

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setWorkmode.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

CVE-2022-26290

Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/WriteFacMac.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-24

Top malicious files

100% Threat score	PurchaseOrder.exe	100% Threat score	a3conversorSii_1_33.exe
100% Threat score	tmptkensrs7	100% Threat score	ActiveMINSoftware.exe
100% Threat score	fps.exe	100% Threat score	app3.apk
100% Threat score	UnbodSetup.exe	100% Threat score	PMT402200318_PDF.exe
100% Threat score	DuplicateCleaner_setup.exe	100% Threat score	paym_details-60112944.xlsb
100% Threat score	qzeakdebxl.apk	98% Threat score	GoogleCal.exe
95% Threat score	belegtransfer514.exe	95% Threat score	WeAreDevsMainDLL.dll
87% Threat score	ntfc.php2393903	87% Threat score	aftral.com invoice.html
85%	UniPC_setup_3_4.exe	80%	OPSWAT_GEARs_Client_3445-7c867995737c1853977386e89a5560c5-0.msi

Threat score		Threat score	
75% Threat score	webplugin(2).exe		



Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://ablink.info.axahealth.co.uk/ls/click?upn=0-2BGjS-2BbuiQX4SOVdle8lNRlKzm3WmI-2BHRdw-2BZ-2FO-2BEiVjPvJlxxvf6Rxs-2F6HYuwHsoQ2cYwWlvgHVbAd9zSUVa03ZfbHEp8aTnHsHFzV2r3D1A8Efg54n97QKXHR12l6s-2FOXFHIELsJ08jJGMjpSDMuZt8-2BFlyZt26oQZhe-2BRbSHE3y8prTZsp8zndJpBj-2BguwogajpzrdtEmfG8yD18gCuy7eYldeSHPLKa8aonl9mWAuSuvOrwELDnu6qSpODjR-xB_bQiQ5-2BGmXnymGnBlujf8oUCkC3RzCQ-2FTlouozl8kECwDkyKPLp4XKTUvVmKKrÜZjWBwSlYjh7oi2r2lrH-2FtejH-2BwcGWeXiFFXpXjLmHYF7S6x3ErqUpp-2Biyb6udBs5bcobB3MrtlRdz1RX9JBrmEA-2F2Nj2kQl6F62NE0KvsIe7jsQ63dQlAmqCvlHmz9iDzbXEcQA-2FPUqejzSfglO21lolbA0YmNZTzPDKLcl81rGRkkGvDSWEeZ6pzuaVBxdJ0OkychGqhbflJr-2FidNvjDg8FD9AJiF1gkDrqYrZi22aiQ78IcMlaj5-2BN-2BtuSdGITZ3rZl3eUvTPHRjziXHqEVfRkOkBNQx2AW3BW5wn3sr-2FvFzbOzpVM6P3xjHQ68ldRyJMSpcR7LgFAFXbB83VznljBd0z7-2FIB2-2BGT3W2Ml8N0klUhcNpkjOGPa800EbihHUuPSj-2Ft0IJUapNiA1m0qXOVYi3irQcDymC0w4prHkevx57IPDmUvfSCNBuFVf-2BB3xrdkemubQ7QTRib6pTtIAV95fTCqBykBzTemqRrgbdqujG7CIYAZBXjuKilJb9TRvltSLSEI-2FepCDcg2pDEdN0us8QezaJDtRZdOp0XCKcaVYpbi21ZPu1UcdLvCYD98ny8HZ7E6r-2BvkXHIjqnh417HrKEJ3iEfryei6MQyU6-2BzxzkDOWA3m0NRYqtidd-2BFI-2BQHyzEaWveMVuVrA0M6oxX8SYDDh1FM-2BFvZQjdZ-2F175Ycd-2F4o2xz-2BODj2-2BJ4q0va	100% Threat score	https://sessionprotocol.com/pars
100% Threat score	http://42.235.90.137:33282/Mozi.m	100% Threat score	http://61.52.39.87:47700/Mozi.m
100% Threat score	https://bluemooseroofing.com/www.lbpiaaccess.com/landbank/	100% Threat score	http://117.208.137.119:47359/Mozi.m
100% Threat score	http://42.224.47.57:46933/Mozi.m	95% Threat score	http://amiciforzearmate.com/?hi
95% Threat score	http://muchdubious.top/	95% Threat score	https://osf.io/mvdcf/
95% Threat score	https://ipfs.io/ipfs/QmbQw5JLa55xPy7RyNqKco8fDVfFqEqFrrSZkVJJkRspN/#test%40test.com	95% Threat score	http://choobingroup.ir/
95% Threat score	https://t.nylas.com/t1/261/6cbe8v4imih3bw9gf8ioresjc/0/3c7cce77cbac8079dc26fe3f4c568d022c2c22692db729bf1901a98255e5e50	95% Threat score	https://juliaray.ca/wp-includes/IT
95% Threat score	https://test.scoutingwestvoorne.nl/	95% Threat score	http://choobingroup.ir/
94% Threat score	https://osf.io/e2c9d/	91% Threat score	https://test.scoutingwestvoorne.nl/ytf=laurent.perinet%40rte-franc
89% Threat score	https://osf.io/ymd9h/	89% Threat score	https://finmonitoring.in.ua/onlajn
89% Threat score	https://ipfs.io/ipfs/QmY6XgyLWVyUys7UVteWw7jaHimocjVq4pZ4eq9yJF4mMY?filename=cbk_index.htm#ZG9uYWwub2Zhb2xhaW5AbmNzZS5pZQ%3D%3D	89% Threat score	https://www.virustotal.com/gui/ur
89% Threat score	http://softlibre.unizar.es/videolan/vlc/2.2.6/win32/vlc-2.2.6-win32.exe;	86% Threat score	https://app.pizzarotticpsa.com/sa
84% Threat score	https://osf.io/mnhrj/	82% Threat score	https://vuemc.io/#introduction




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 Brazil
 #9 Uruguay	 #10 Japan











Source: SpamHaus

Top spammers

 #1 Canadian Pharmacy 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.	 #2 PredictLabs / Sphere Digital 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.
 #3 Hosting Response / Michael Boehm 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.		#4 Michael Persaud Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
	#5 RetroCubes 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.		#6 Cyber World Internet Services/ e-Insites 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.
	#7 RR Media A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.		#8 Kobeni Solutions 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.
	#9 Richpro Trade Inc. / Richvestor GmbH Uses botnets or hires botnet spammers to send spam linking back to suspect investment, "quack-health-cures" and other sites that he owns or is an affiliate of. Botnet spamming and hosting sites on hacked servers is fully criminal in much of the world. Managed or owned by a Timo Richert.		

Source: [SpamHaus](#)

Top countries with botnet			
	#1 China		#2 United States of America
	#3 India		#4 Indonesia
	#5 Thailand		#6 Algeria
	#7 Viet Nam		#8 Brazil
	#9 Pakistan		#10 Venezuela (Bolivarian Republic of)

Source: [SpamHaus](#)

Top phishing countries			
	#1 United States		#2 Germany
	#3 Russia		#4 Netherlands
	#5 Singapore		#6 India
	#7 United Kingdom		#8 Indonesia
	#9 France		#10 Vietnam

Source: [Have I been pwned?](#)

Have I been pwned

Nothing today

Source: [Imperva DDOS Map](#)

Top DDOS attackers

Source: [Imperva DDOS Map](#)

Top DDOS country targets

Source: [Imperva DDOS Map](#)

Top DDOS techniques

Source: [Imperva DDOS Map](#)

Top DDOS industry targets

