Your Security Rabbits report for February 24, 2022

Hot topics

Nothing today

News

CISA Alerts

AA22-054A: New Sandworm Malware Cyclops Blink Replaces VPNFilter

The Sandworm actor, which the United Kingdom and the United States have previously attributed to the Russian GRU, has replaced the exposed VPNFilter malware with a new more advanced framework. The United Kingdom's (UK) National Cyber Security Centre (NCSC), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) in the U.S. have identified that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to here as Cyclops Blink. The NCSC, CISA, and the FBI have previously attributed the Sandworm actor to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Ce[...]

CyberScoop

Another round of 'wiper' malware appears in Ukrainian networks

Security researchers detected new destructive malware spreading in Ukraine on Wednesday, following evidence of distributed denial-of-service disruptions for government agencies -- both of which overlapped with the beginnings of a Russian invasion. ESET said the data-wiping malware it has dubbed "HermeticWiper" was "installed on hundreds of machines in the country," and there were signs that the attackers had been preparing for almost two months. Silas Cutler, principle reverse engineer and resident hacker at Stairwell, said that the wiper damages a system's master boot record, which tells a machine how to start up. That's similar to malware known as WhisperGate that was used in an attack in [...]

CyberScoop

As Russia invades, Ukrainian government networks suffer high-profile DDoS disruption

A series of Ukrainian government websites were inaccessible Wednesday after what a government official described as a "mass DDoS attack," marking the second apparent distributed denial-of-service disruption to hit government sites there in the last eight days. The websites for the country's Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, the Security Service of Ukraine and the Cabinet of Ministers suffered network disruptions in an incident that "appears consistent with recent DDOS attacks," according to NetBlocks, a London-based organization that tracks internet access. DDoS attacks knock sites offline by flooding them with phony traffic. Mykhailo Fedorov, Uk[...]

Naked Security

Apple AirTag anti-stalking protection bypassed by researchers

Problems with Apple's Tracker Detect system, which warns you of likely stalking attempts using hidden AirTags.

Cyware News - Latest Cyber News

Attackers Combing Internet to Target Exposed MS SQL Servers

Attackers have been found actively scanning ports for vulnerable MS-SQL servers in an attempt to deploy Cobalt Strike Beacon. These vulnerable servers are exploited through brute force and dictionary attacks. After gaining access to the admin account and logging into the server, the attackers drop coinminers such as Lemon Duck, KingMiner, and Vollgar. Stay updated with patches, it's the best defense!

Cyware News - Latest Cyber News

Banking Trojans Dominate the Mobile Malware Threat Landscape

While there was a downward trend in the overall mobile malware attack last year, Kaspersky researchers also discovered almost 100,000 new variants of mobile banking trojans in just a year.

CyberScoop

Chinese researchers accuse NSA of being behind a powerful exploit

A Chinese cybersecurity firm released a report Wednesday that revealed a decade-old exploit allegedly created by a covert hacking group associated with the U.S. National Security Agency. The report is the first time that a Chinese cybersecurity firm has both attributed a cyberattack to a U.S. hacking group and included technical indicators of compromise. "It's a completely different type of report here that that seems to mimic Western name-and-shame," said Winnona DeSombre, fellow at the Atlantic Council and Harvard's

Cyware News - Latest Cyber News

CISA Warns of Attacks Exploiting Recent Vulnerabilities in Zabbix Monitoring Tool

Tracked as CVE-2022-23131 and CVE-2022-23134, the two flaws could be exploited to bypass authentication and gain admin privileges, which could then allow an attacker to execute arbitrary commands.

Belfer Center. Pangu Lab researchers said they first discovered the backdoor in 2013 during an "in-depth forensic investigation of a host in a key domestic department." The res[...]

IT Security Guru

Construction companies receive cybersecurity guidance

The National Cyber Security Centre (NCSC) has provided the UK construction industry with a guidance document titled Cyber security for construction businesses. The document provided practical, tailored advice for construction firms on protecting their businesses and building projects from cyber-attackers. It provides practical, tailored advice for construction firms on how to defend against common attack [...] The post Construction companies receive cybersecurity guidance appeared first on IT Security Guru.

Threatpost

Creaky Old WannaCry, GandCrab Top the Ransomware Scene

Nothing like zombie campaigns: WannaCry's old as dirt, and GandCrab threw in the towel years ago. They're on auto-pilot at this point, researchers say.

Cyware News - Latest Cyber News

Cybersecurity is the Biggest Obstacle to Cloud Adoption

As organizations tackle their migrations to the cloud, IT professionals believe that cyber threats aimed at the cloud represent the biggest obstacle to continued adoption.

Cyware News - Latest Cyber News

Darktrace To Buy Attack Insights Vendor Cybersprint For $53.7M

Darktrace has agreed to purchase attack surface management vendor Cybersprint for $53.7 million to give customers insights that help eliminate blind spots and detect risks.

CyberScoop

DOJ drops Trump-era 'China Initiative' but remains focused on nation-state threats

The U.S. Department of Justice is closing down its controversial "China Initiative," instead launching a broader strategy toward countering multiple threats from several countries, a senior department official said Wednesday. The new "Strategy for Countering Nation-State Threats" will focus the department's resources on multiple concurrent threats from China, Russia, Iran and North Korea, such as transnational repression, foreign malign influence and cyberthreats, said Assistant Attorney General Matthew Olsen in remarks at George Mason University. "We see nations such as China, Russia, Iran and North Korea becoming more aggressive and more capable in their activity than ever before," Olsen s[...]

The Hacker News

Dridex Malware Deploying Entropy Ransomware on Hacked Computers

Similarities have been unearthed between the Dridex general-purpose malware and a little-known ransomware strain called Entropy, suggesting that the operators are continuing to rebrand their extortion operations under a different name. "The similarities are in the software packer used to conceal the ransomware code, in the malware subroutines designed to find and obfuscate commands (API calls),

Cyware News - Latest Cyber News

EU countries offer cyber-defense assistance to Ukraine

The support is apparently being provided via the EU's Cyber Rapid Response Teams (CRRTs) - a project supported by the governments of Croatia, Estonia, Lithuania, the Netherlands, Poland, and Romania.

IT Security Guru

EU cyber-response team deployed

The European Union's newly formed Cyber Rapid-Response Team (CRRT) has been deployed to Ukraine to aid in combat against Russian threat actors. In a tweet yesterday, the Lithuanian Ministry of Defence confirmed the CRRT is to be deployed at the request of the Ukrainian government. Lithuania will sit at the head of a coalition of [...] The post EU cyber-response team deployed appeared first on IT Security Guru.

IT Security Guru

Expert opinion: NHS reveals data leak

This week, the NHS reported a data leak incident to the Information Commissioner's Office, which puts third-party contractor cybersecurity risks in the spotlight. What happened? A former employee of PSL Print Management, a consultancy used by the NHS, requested all emails and text messages regarding his employment at the company. PSL obliged, but sent [...] The post Expert opinion: NHS reveals data leak appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Inside the Lab Where Intel Tries to Hack Its Own Chips

Five years ago, Intel launched a dedicated hardware hacking group known as Intel Security Threat Analysis and Reverse Engineering (iSTARE) to analyze and attack Intel's future generations of chips.

Cyware News - Latest Cyber News

Kostovite, Petrovite, and Erythrite Hacking Groups are Striking Industrial, Operational Technology Systems

Three new threat groups targeting firms in the industrial sector have appeared but over half of all attacks are the work of only two known cybercriminal outfits, researchers say.

IT Security Guru

LockBit, Conti ransomware targets industrial sector

A new report from Dragos suggests that the industrial sector has become a common target for both financially motivated and state sponsored attacks. Ransomware groups known as LockBit and Conti have been most active in targeting organisations with and Industrial Control System (ICS)/Operational Technology (OT) environment in 2021. Researchers noted that the manufacturing vertical was [...] The post LockBit, Conti ransomware targets industrial sector appeared first on IT Security Guru.

New Phishing Technique Uses Remote Access Software

Security researchers discovered a new phishing technique wherein adversaries bypass MFA using the

The Hacker

New Wiper Malware Targeting Ukraine Amid Russia's Military Operation

Cybersecurity firms ESET and Broadcom's Symantec said they discovered a new data wiper malware used in

Cyware News - Latest Cyber News

VNC screen sharing system without victims logging into their accounts. The demonstrated phishing technique has not been used in real-world attacks yet. However, the researcher suspects that it could be used in the future.

Cyware News - Latest Cyber News

Operation Cache Panda - Chinese APT10 Targets Taiwan

Taiwanese cybersecurity firm CyCraft attributed months-long attacks against Taiwan's financial sector to the APT10 group (aka Stone Panda or Bronze Riverside), which is affiliated with the Chinese government.

CyberScoop

Russia-linked Sandworm reportedly has retooled with 'Cyclops Blink'

A long-running hacking group associated with Russian intelligence has developed a new set of tools to replace malware that was disrupted in 2018, according to an alert Wednesday from the U.S. and U.K. cybersecurity and law enforcement agencies. The advanced persistent threat group, known primarily as Sandworm, is now using a "large-scale modular malware framework" that the agencies call Cyclops Blink. Western governments have blamed Sandworm for major incidents such as the disruption of Ukraine's electricity grid in 2015, the the NotPetya attacks in 2017 and breaches of the Winter Olympics in 2018. Cyclops Blink has largely replaced the VPNFilter malware in Sandworm's activities since at lea[...]

Threatpost

Sextortion Rears Its Ugly Head Again

Attackers are sending email blasts with malware links in embedded PDFs as a way to evade email filters, lying about having fictional "video evidence."

Security Affairs

Sophos linked Entropy ransomware to Dridex malware. Are both linked to Evil Corp?

The code of the recently-emerged Entropy ransomware has similarities with the one of the infamous Dridex malware. The recently-emerged Entropy ransomware has code similarities with the popular Dridex malware. Experts from Sophos analyzed the code of Entropy ransomware employed in two distinct attacks. "A pair of incidents at different organizations in which attackers deployed a [...] The post Sophos linked Entropy ransomware to Dridex malware. Are both linked to Evil Corp? appeared first on Security Affairs.

IT Security Guru

The Inside Man Season 4: The Future of Cybersecurity Awareness Training

Corporate training videos. The words alone make you feel bored. They summon dreary memories of wasted hours, terrible acting and worse storytelling. If I told you that it doesn't have to be that way, that training videos can be informative, engaging and even exciting, would you believe me? You'd be forgiven if you didn't. But [...] The post The Inside Man Season 4: The Future of Cybersecurity Awareness Training appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Ukrainian Government Agencies and Largest Banks Once Again Hit by DDoS Attacks

The sites of Ukrainian agencies (including the Ministries of Foreign Affairs, Defense, and Internal Affairs, the Security Service, and the Cabinet of Ministers), and two banks are again targeted.

Cyware News - Latest Cyber News

fresh attacks against hundreds of machines in Ukraine, as Russian forces formally launched a full-scale military operation against the country. The Slovak company dubbed the wiper "HermeticWiper" (aka KillDisk.NCV), with one of the malware samples compiled on December 28, 2021, implying that

Security Affairs

Researchers shared technical details of NSA Equation Group's Bvp47 backdoor

Pangu Lab researchers disclosed details of the Bvp47 backdoor that was used by the US NSA Equation Group. Researchers from The China's Pangu Lab have disclosed details of a Linux top-tier APT backdoor, tracked as Bvp47, which is associated with the U.S. National Security Agency (NSA) Equation Group. The name "Bvp47" comes form numerous references to [...] The post Researchers shared technical details of NSA Equation Group's Bvp47 backdoor appeared first on Security Affairs.

Threatpost

Samsung Shattered Encryption on 100M Phones

One cryptography expert said that 'serious flaws' in the way Samsung phones encrypt sensitive material, as revealed by academics, are 'embarrassingly bad.'

Cyware News - Latest Cyber News

Social Media Attacks Double, Financial Sector Suffers Most - Report

As per the Quarterly Threat Trends & Intelligence Report by PhishLabs, social media threats increased by 103% from January to December 2021. In December, organizations witnessed an average of 68 attacks per month.

WeLiveSecurity

Technology, Progress, and Climate

The climate solutions we need to transform every sector are here. The question is: what role will you play in this transformation? You, your community, your business, your government? The post Technology, Progress, and Climate appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

Ukraine organizations hit by new wiper malware

According to ESET, the victim pool in Ukraine numbers at least in the hundreds. Symantec saw the wiper in Ukraine, Lithuania, and Latvia, with attacks on financial firms and government contractors.

Security Affairs

US and UK link new Cyclops Blink malware to Russian state hackers

UK and US cybersecurity agencies linked Cyclops Blink malware to Russia's Sandworm APT US and UK cybersecurity and law enforcement agencies published a joint security advisory about a new malware, dubbed Cyclops Blink, that has been linked to the Russian-backed Sandworm APT group. Sandworm (aka BlackEnergy and TeleBots) has been active since 2000,

it operates under the [...] The post US and UK link new Cyclops Blink malware to Russian state hackers appeared first on Security Affairs.

Cyware News - Latest Cyber News

US, UK link new Cyclops Blink malware to Russian state hackers
New malware dubbed Cyclops Blink has been linked to the Russian-backed Sandworm hacking group in a joint security advisory published today by US and UK cybersecurity and law enforcement agencies.

Cyware News - Latest Cyber News

Vulnerability Spotlight: Buffer overflow vulnerabilities in Accusoft ImageGear could lead to code execution
Cisco Talos recently discovered multiple vulnerabilities in Accusoft ImageGear. It is a document-imaging developer toolkit that allows users to create, edit, annotate, and convert various images.

Twitter

CVE

CVE-2021-35689 A potential vulnerability in the Oracle Talent Acquisition Cloud - Taleo Enterprise Edition. This high severity potential vulnerability allows attackers to perform remote code execution on Taleo Enterprise Edition system. Successful...

Vulmon Vulnerability Feed

CVE-2021-35689 A potential vulnerability in the Oracle Talent Acquisition Cloud - Taleo... Vulnerability Notification:

Debra M. Fezza Reed #SecRiskRptSME #QSC2022

New/Modified vulnerability published February 23, 2022 at 07:15PM on the NVD: CVE-2021-35689 A potential vulnerability in the Oracle Talent Acquisition Cloud - Taleo Enterprise Edition. This high severity potential vulnerability allows attackers to perfo[...]

Xanadu GNU/Linux

CVE-2021-35689

Brandon Workentin

New vulnerability on the NVD: CVE-2021-35689

Wolfgang Sesin

New post from (Oracle Talent Acquisition Cloud Remote Code Execution [CVE-2021-35689]) has been published on

www.sesin.at

New post from (Oracle Talent Acquisition Cloud Remote Code Execution [CVE-2021-35689]) has been published on

Wes

New vulnerability on the NVD: CVE-2021-35689

Threat Intel Center

NEW: CVE-2021-35689 A potential vulnerability in the Oracle Talent Acquisition Cloud - Taleo Enterprise Edition. This high severity potential vulnerability allows attackers to perform remote code execution on T... (click for more)
Severity: CRITICAL

delapena.esteban

New vulnerability on the NVD: CVE-2021-35689

Wolfgang Sesin

New post from (CVE-2021-35689) has been published on

Threat Intel Center

NEW: CVE-2021-35689 A potential vulnerability in the Oracle Talent Acquisition Cloud - Taleo Enterprise Edition. This high severity potential vulnerability allows attackers to perform remote code execution on T... (click for more)
Severity: CRITICAL

Joe Walsh

Trump had to be forced into signing new Russian sanctions. Trump pushed for a joint cyber security unit with Russia. Trump thanked Putin for expelling US diplomats from Russia. Trump eased sanctions on Putins top oligarchs. Trump congratulated Putin on his sham election. 4/

Source: NIST

NIST CVE: Critical

CVE-2021-35689

A potential vulnerability in the **Oracle** Talent Acquisition Cloud - Taleo Enterprise Edition. This high severity potential vulnerability allows attackers to perform remote code execution on Taleo Enterprise Edition system. Successful attacks of this vulnerability can result in unauthorized remote code execution within Taleo Enterprise Edition and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Talent Acquisition Cloud - Taleo Enterprise Edition. All affected customers were notified of CVE-2021-35689 by Oracle.

CRITICAL | Vector: network | Created: 2022-02-24 | Updated: 2022-02-24

CVE-2021-23682

This affects the package litespeed.js before 0.3.12; the package appwrite/server-ce from 0.12.0 and before 0.12.2, before 0.11.1. When parsing the query string in the getJsonFromUrl function, the key that is set in the result object is not properly sanitized leading to a Prototype Pollution vulnerability.

CRITICAL | Vector: network | Created: 2022-02-16 | Updated: 2022-02-24

Source: NIST

NIST CVE: High

CVE-2021-21958

A heap-based buffer overflow vulnerability exists in the Hword HwordApp.dll functionality of **Hancom Office** 2020 11.0.0.2353. A specially-crafted malformed file can lead to memory corruption and potential arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.

HIGH | Vector: local | Created: 2022-02-16 | Updated: 2022-02-24

CVE-2022-23188

Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a buffer overflow vulnerability due to insecure handling of a crafted malicious file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted malicious file in Illustrator.

HIGH | Vector: local | Created: 2022-02-16 | Updated: 2022-02-24

CVE-2022-23186

Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

HIGH | Vector: local | Created: 2022-02-16 | Updated: 2022-02-24

CVE-2022-22792

MobiSoft - MobiPlus User Take Over and Improper Handling of url Parameters Attacker can navigate to specific url which will expose all the users and password in clear text. http://IP/MobiPlusWeb/Handlers/MainHandler.ashx?MethodName=GridData&GridName=Users

HIGH | Vector: network | Created: 2022-02-16 | Updated: 2022-02-24

Source: NIST

NIST CVE: Medium

CVE-2022-23189

Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

MEDIUM | Vector: local | Created: 2022-02-16 | Updated: 2022-02-24

CVE-2022-23197

Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

MEDIUM | Vector: local | Created: 2022-02-16 | Updated: 2022-02-24

CVE-2021-4134

The Fancy Product **Designer WordPress** plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the ID parameter found in the ~/inc/api/class-view.php file which allows attackers with administrative level permissions to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 4.7.4.

MEDIUM | Vector: network | Created: 2022-02-16 | Updated: 2022-02-24

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-24671

A link following privilege escalation vulnerability in Trend Micro **Antivirus** for Max 11.0.2150 and below could allow a local attacker to modify a file during the update process and escalate their privileges. Please note: an attacker must **first** obtain the ability to execute low-privileged code on the target system in order to exploit this

CVE-2022-24680

A security link following local privilege escalation vulnerability in Trend Micro **Apex** One, Trend Micro **Apex One** as a Service, Trend Micro Worry-Free **Business Security** 10.0 SP1 and Trend Micro **Worry-Free Business Security** Services agents could allow a local attacker to create a mount point and leverage this for arbitrary folder deletion, leading to escalated privileges on affected installations. Please note: an attacker must **first**

vulnerability.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2022-24679

A security link following local privilege escalation vulnerability in Trend Micro **Apex** One, Trend Micro **Apex One** as a Service, Trend Micro Worry-Free **Business Security** 10.0 SP1 and Trend Micro **Worry-Free Business Security** Services agents could allow a local attacker to create an writable folder in an arbitrary location and escalate privileges affected installations. Please note: an attacker must **first** obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2022-24678

An **security agent** resource exhaustion denial-of-service vulnerability in Trend Micro **Apex** One, Trend Micro **Apex One** as a Service, Trend Micro Worry-Free **Business Security** 10.0 SP1 and Trend Micro **Worry-Free Business Security** Services agents could allow an attacker to flood a temporary log location and consume all disk **space** on affected installations.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2022-25330

Integer overflow conditions that **exist** in Trend Micro **ServerProtect** 6.0/5.8 **Information Server** could allow a remote attacker to crash the process or achieve remote code execution.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2022-25329

Trend Micro **ServerProtect** 6.0/5.8 **Information Server** uses a static credential to perform authentication when a specific command is typed in the console. An unauthenticated remote attacker with access to the Information Server could exploit this to register to the server and perform authenticated actions.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2021-43943

Affected versions of **Atlassian Jira** Service **Management Server** and **Data Center** allow attackers with administrator privileges to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the "Object Schema" field of /secure/admin/InsightDefaultCustomFieldConfig.jspa. The affected versions are before version 4.21.0.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2021-26092

Failure to sanitize input in the **SSL VPN** web portal of **FortiOS** 5.2.10 through 5.2.15, 5.4.0 through 5.4.13, 5.6.0 through 5.6.14, 6.0.0 through 6.0.12, 6.2.0 through 6.2.7, 6.4.0 through 6.4.4; and **FortiProxy** 1.2.0 through 1.2.9, 2.0.0 through 2.0.1 may allow a remote unauthenticated attacker to perform a reflected Cross-site Scripting (XSS) attack by sending a request to the error page with malicious GET parameters.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2022-23655

Octobercms is a self-hosted CMS platform based on the **Laravel** PHP Framework. Affected versions of OctoberCMS did not validate gateway server signatures. As a result non-authoritative gateway servers may be used to exfiltrate user private keys. Users are advised to upgrade their installations to build 474 or v1.1.10. The only known workaround is to manually apply the patch (e3b455ad587282f0fbcb7763c6d9c3d000ca1e6a) which adds server signature validation.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

CVE-2022-25331

Uncaught exceptions that can be generated in Trend Micro ServerProtection 6.0/5.8 **Information Server** could allow a remote attacker to crash the process.

UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-02-24

Source: Hybrid Analysis

Top malicious files

100% Threat score	DATOS 2302 (.) xls	100% Threat score	Invoice (.) xlsm
100% Threat score	VLCInstaller (.) exe	100% Threat score	ICNEditClient (.) exe
100% Threat score	VLC (.) exe	100% Threat score	SysTools MailXaminer 4 (.) 7 (.) exe
100% Threat score	Setup (.) exe	100% Threat score	j (.) exe

100% Threat score	BABBLEv1 (.) apk
97% Threat score	pdf (.) dll
90% Threat score	report 02 24 2022 (.) xlsm
80% Threat score	SetupIQVIAMarketV_LVA_SO (.) exe
80% Threat score	OCCT (.) exe
75% Threat score	offsetexplorer (.) exe
75% Threat score	offsetexplorer_64bit (.) exe

97% Threat score	pdf (.) dll
95% Threat score	0B995FE0C4384D7DEF2F8D6C7BBE4550C82C8C09DCD674D1F41C27434EDDEF1E
85% Threat score	vlc-back (.) exe
80% Threat score	RVTools4 (.) 3 (.) 1 (.) msi
80% Threat score	ApexSQLSetup-ApexSQLPlan (.) exe
75% Threat score	setup (.) exe

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://www (.) fcos-uae (.) com/
97% Threat score	http://42 (.) 226 (.) 222 (.) 134:59915/Mozi (.) m
92% Threat score	https://656115 (.) selcdn (.) ru/mex/jacksjoe (.) html
83% Threat score	https://chrissieperry (.) com/
77% Threat score	http://www (.) 1830ndaytona (.) info/wp-includes/js/comment-reply (.) min (.) js?ver=4 (.) 7 (.) 6
77% Threat score	http://www (.) greydynamics (.) com:443/
77% Threat score	http://poweradblocker (.) com/
74% Threat score	http://www (.) tapdance-claquettes (.) org/manouche
72% Threat score	http://e8f485 (.) phxxqmwnxjbtq (.) com/

100% Threat score	http://a (.) wvwvwv (.) cf/
93% Threat score	http://59 (.) 95 (.) 67 (.) 19:43202/bin (.) sh
83% Threat score	http://42 (.) 225 (.) 237 (.) 125:49955/Mozi (.) m
79% Threat score	https://clck (.) ru/bnN32?
77% Threat score	https://www (.) architecturalfiberglass (.) org/glass-fiber-reinforced-gypsum/
77% Threat score	http://www (.) imss-sa (.) com/
77% Threat score	http://www (.) www (.) www (.) hermes (.) effizienz-holding (.) de/
74% Threat score	http://bupdate (.) d3u2ngn8pr5nbt (.) amplifyapp (.) com/

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 Japan

#10 Korea, Republic of

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 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#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 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#7 **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.

#8 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#9 **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.

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 Germany

#3 Russia	#4 Japan
#5 Netherlands	#6 Hong Kong
#7 Singapore	#8 India
#9 France	#10 Australia