



Your Security Rabbits report for April 14, 2022

Hot topics

Nothing today

News



600k worth of crypto stolen by ethical hacker

Authorities in Pinellas Park, Florida have arrested 27-year old Aaron Daniel Motta after he allegedly stole a client's Trezor hardware wallet and its password while providing security assistance. Motta is a "certified ethical hacker", and has been charged with grand theft and other computer offenses. The accused is currently self employed and owns Motta Management [...] The post 600k worth of crypto stolen by ethical hacker appeared first on IT Security Guru.



AA22-103A: APT Cyber Tools Targeting ICS/SCADA Devices

Actions to Take Today to Protect ICS/SCADA Devices: * Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible. * Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks and to give defender monitoring systems opportunities to detect common attacks. * Leverage a properly installed continuous OT monitoring solution to log and alert on malicious indicators and behaviors. The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA[...])



Barracuda Networks changes hands with purchase by global investment firm KKR

KKR is taking over from Thoma Bravo.



CISA Warns Against Russian Hackers Exploiting a Critical Bug

The CISA issued an order urging federal civilian agencies and organizations to fix the actively exploited bug impacting WatchGuard Firebox and XTM appliances. Cyclops Blink, before getting disrupted, targeted nearly one percent WatchGuard Firebox firewall appliances with CVE-2022-23176 exploits. Infected users are suggested to follow shared instructions on recovering the infected Firebox appliances.



Citrix Patches Vulnerabilities in Several Products

Tracked as CVE-2022-27505, the newly resolved high-severity issue in SD-WAN is a reflected cross-site scripting (XSS) vulnerability that exists because input isn't properly neutralized during web page generation.



Critical VMware Workspace ONE Access Flow Under Active Exploitation in the Wild

A week after VMware released patches to remediate eight security vulnerabilities in VMware Workspace ONE Access, threat actors have begun to actively exploit one of the critical flaws in the wild. Tracked as CVE-2022-22954, the critical issue relates to a remote code execution vulnerability that stems from server-side template injection in VMware Workspace ONE Access and Identity Manager. The



CVE-2021-31805 RCE bug in Apache Struts was finally patched

Apache addressed a critical flaw in Apache Struts RCE that was linked to a previous issue that was not properly fixed. Apache Struts is an open-source web application framework for developing Java EE web applications. The Apache Software Foundation urges organizations to address a vulnerability, tracked as CVE-2021-31805, affecting Struts versions ranging 2.0.0 to 2.5.29. [...] The post CVE-2021-31805 RCE bug in Apache Struts was finally patched appeared first on Security Affairs.



Enemybot: a new Mirai, Gafgyt hybrid botnet joins the scene

The botnet borrows a few tricks from Mirai.



Fakecalls - An Unusual Twist to Banking Customer Support Frauds

A new banking trojan called Fakecalls hijacks phone conversations between a potential victim and its bank customer support to steal files stored on devices. The trojan can play a pre-recorded message that mimics the ones often used by banks to greet customers seeking support. Experts suggest downloading apps only from official stores and paying attention to the requested permissions of an app.



A practical reason why crypto might not work for large-scale sanctions evasion

According to crypto-tracking company Chainalysis, the markets probably couldn't handle it without prices tanking. The post A practical reason why crypto might not work for large-scale sanctions evasion appeared first on CyberScoop.



Apache says 2-year-old Struts bug wasn't fully fixed

Apache has taken another shot at fixing a critical remote code execution vulnerability in its Struts 2 framework for Java applications - because the first patch, issued in 2020, didn't fully do the trick.



China-linked Hafnium APT leverages Tarrask malware to gain persistence

China-linked Hafnium APT group started using a new piece of new malware to gain persistence on compromised Windows systems. The China-backed Hafnium cyberespionage group is likely behind a piece of a new malware, dubbed Tarrask, that's used to maintain persistence on compromised Windows systems, reported Microsoft Threat Intelligence Center (MSTIC) experts. HAFNIUM primarily targets entities [...] The post China-linked Hafnium APT leverages Tarrask malware to gain persistence appeared first on Security Affairs.



CISA warns orgs to patch actively exploited Windows LPE bug

The CISA has added ten new security bugs to its list of actively exploited vulnerabilities, including a high severity local privilege escalation bug in the Windows Common Log File System Driver.



CitySprint Discloses Security Breach Impacting Personal Data of Delivery Drivers

An email was sent on April 7th to thousands of drivers confirming that a security breach had occurred. CitySprint, which was recently acquired by parcel delivery giant DPD Group, uses self-employed drivers to deliver packages across the UK.



Critical vulnerabilities uncovered in hospital robots

The robots zip around hospitals delivering medicine and other supplies.



DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii

Nearly all of the world's internet data traverses such lines, which are prime targets for hackers of all stripes. The post DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii appeared first on CyberScoop.
























ESET takes part in global operation to disrupt Zloader botnets

ESET researchers provided technical analysis, statistical information, and known command and control server domain names and IP addresses The post ESET takes part in global operation to disrupt Zloader botnets appeared first on WeLiveSecurity




Feds Shut Down RaidForums Hacking Marketplace

The DoJ is charging its founder, 21-year-old Portuguese citizen Diogo Santos Coelho, on six criminal counts, including conspiracy, access device fraud and aggravated identity theft.

 CyberScoop	Feds warn about foreign government-connected hackers aiming to disrupt vital industrial systems Dragos says the group behind the tools has a "breadth of knowledge" that's "beyond" any previously witnessed. The post Feds warn about foreign government-connected hackers aiming to disrupt vital industrial systems appeared first on CyberScoop.	 Cyware News - Latest Cyber News	Flaws in ABB Network Interface Modules Expose Industrial Systems to DoS Attacks The vulnerabilities affect Symphony Plus SPIET800 and PNI800, which are network interface modules that enable communications between a control network and a host computer running an engineering tool or a human-machine interface (HMI).
 CyberScoop	Global advertising giant Omnicom suffers 'suspicious' IT incident The company said it is in the process of bringing systems back online. The post Global advertising giant Omnicom suffers 'suspicious' IT incident appeared first on CyberScoop.	 Cyware News - Latest Cyber News	Hackers exploit critical VMware CVE-2022-22954 bug, patch now A proof-of-concept exploit has been released online for the VMware CVE-2022-22954 remote code execution vulnerability, already being used in active attacks that infect servers with coin miners.
 Cyware News - Latest Cyber News	Hardware-assisted security will go big soon - study Hardware-assisted security (HAS) uses hardware extensions and components to support the security of higher-level machine layers, from the BIOS up through desktop applications.	 SOPHOS Naked Security	Hospital robot system gets five critical security holes patched Fortunately, we're not talking about a robot revolution, or about hospital AI run amuck. But these bugs could lead to ransomware, or worse...
 Cyware News - Latest Cyber News	Industroyer2 Found Targeting Energy Sector in Ukraine Sandworm APT has been associated with a new Industroyer-2 malware that was used to target electric power systems in Ukraine. Besides, the Sandworm group also uses other malware families such as CaddyWiper, AwfulShred, OrcShred, and SoloShred. Organizations are suggested to follow the recommendation provided by CERT-UA to stay protected.	 WeLiveSecurity	Innovation and the Roots of Progress If you look back at the long arc of history, it's clear that one of the most crucial drivers of real progress in society is innovation The post Innovation and the Roots of Progress appeared first on WeLiveSecurity
 Security Affairs	JekyllBot:5 flaws allow hacking TUG autonomous mobile robots in hospitals Researchers discovered five vulnerabilities that can be exploited to remotely hack hospital Aethon's TUG autonomous mobile robots. Researchers at healthcare IoT security firm Cynerio discovered a collection of five vulnerabilities impacting TUG autonomous mobile robots, collectively named JekyllBot:5, that could be exploited by remote attackers to hack the devices. According to a US CISA advisory, the [...] The post JekyllBot:5 flaws allow hacking TUG autonomous mobile robots in hospitals appeared first on Security Affairs.	 Cyware News - Latest Cyber News	MDR Provider Critical Start Lands \$215 Million Growth Investment Managed detection and response (MDR) solutions provider Critical Start on Tuesday announced that it has received more than \$215 million in strategic growth funding from private equity firm Vista Equity Partners.
 The Hacker News	Microsoft Disrupts ZLoader Cybercrime Botnet in Global Operation Microsoft and a consortium of cybersecurity companies took legal and technical steps to disrupt the ZLoader botnet, seizing control of 65 domains that were used to control and communicate with the infected hosts. "ZLoader is made up of computing devices in businesses, hospitals, schools, and homes around the world and is run by a global internet-based organized crime gang operating malware as a	 The Hacker News	Microsoft Exposes Evasive Chinese Tarrask Malware Attacking Windows Computers The Chinese-backed Hafnium hacking group has been linked to a piece of a new malware that's used to maintain persistence on compromised Windows environments. The threat actor is said to have targeted entities in the telecommunication, internet service provider and data services sectors from August 2021 to February 2022, expanding from the initial victimology patterns observed during its attacks
 Security Affairs	Microsoft has taken legal and technical action to dismantle the Zloader botnet Microsoft's Digital Crimes Unit (DCU) announced to have shut down dozens C2 servers used by the infamous ZLoader botnet. Microsoft dismantled the C2 infrastructure used by the ZLoader trojan with the help of telecommunications providers around the world and cybersecurity firms. The IT giant obtained a court order that allowed it to sinkhole 65 domains used by [...] The post Microsoft has taken legal and technical action to dismantle the Zloader botnet appeared first on Security Affairs.	 Krebs on Security	Microsoft Patch Tuesday, April 2022 Edition Microsoft on Tuesday released updates to fix roughly 120 security vulnerabilities in its Windows operating systems and other software. Two of the flaws have been publicly detailed prior to this week, and one is already seeing active exploitation, according to a report from the U.S. National Security Agency (NSA).
 The Hacker News	New EnemyBot DDoS Botnet Borrows Exploit Code from Mirai and Gafgyt A threat group that pursues crypto mining and distributed denial-of-service (DDoS) attacks has been linked to a new botnet called Enemybot, which has been discovered enslaving routers and Internet of Things (IoT) devices since last month. "This botnet is mainly derived from Gafgyt's source code but has been observed to borrow several modules from Mirai's original source code," Fortinet	 Cyware News - Latest Cyber News	SMS group spam promises free gifts in return for bill payment Most of these messages promise free gifts and/or offers after having paid bills. Nobody has asked for these texts, and they're not being sent by providers of any services.
 The Hacker News	U.S. Warns of APT Hackers Targeting ICS/SCADA Systems with Specialized Malware The U.S. government on Wednesday warned of nation-state actors deploying specialized malware to maintain access to industrial control systems (ICS) and supervisory control and data acquisition (SCADA) devices. "The APT actors have developed custom-made tools for targeting ICS/SCADA devices," multiple U.S. agencies said in an alert. "The tools enable them to scan for, compromise, and control	 Cyware News - Latest Cyber News	Update: T-Mobile Secretly Bought Its Customer Data from Hackers to Stop Leak. It Failed. According to court documents unsealed today and reviewed by Motherboard, a third-party hired by T-Mobile tried to pay the hackers for exclusive access to that data and limit it from leaking more widely.
 SOPHOS Naked Security	US cryptocurrency coder gets 5 years for North Korea sanctions busting Cryptocurrency expert didn't take "No" for an answer when the US authorities said he couldn't pursue bitcoin opps in North Korea.	 Blog &" Flashpoint	What Does a Cyber Threat Intel Analyst Do? A Look at the Intelligence Professionals Who Bring Threat Intel Programs to Life What is a threat intelligence analyst? A strong cyber threat intelligence program is your organization's most valuable line of defense against attacks that harm your customer, users, data, assets, infrastructure, and personnel. Although high-quality intel is important, even the best threat intel can be useless without professionals to help your security team understand where to [...] The post What Does a Cyber Threat Intel Analyst Do? A Look at the Intelligence Professionals Who Bring Threat Intel Programs to Life appeared first on Flashpoint.
 IT Security Guru	Wind turbine giant hacked Nordex Group, a major German wind turbine manufacturer, suffered a cyberattack on the 31 March 2022. According to Nordex, the attack was discovered early by IT security teams, who reacted quickly. The company has announced that IT systems across multiple locations and business units were shut down as part of their response protocols. The company [...] The post Wind turbine giant hacked appeared first on IT Security Guru.		

Twitter

 Mariana Betsa	April 13, 2022 will come into history as the day when flag of Ukraine was raised next to those of @NATO member states to welcome Ukraine as a future @ccdcoc member. We are confident that Ukraine will be a valuable contributor to the cyber security #StandWithUkraine	 FBI	Certain advanced persistent threat (APT) #cyber actors have shown the ability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices. Learn more via our joint Cybersecurity Advisory.
---	---	--	---



Cyber security remains a top priority for our government. Today I met with stakeholders at the Ontario Tech University to discuss how to keep Canadians safe from cyber crimes

Source: *NIST*

NIST CVE: Critical

Nothing today

Source: *NIST*

NIST CVE: High

CVE-2022-20774

A vulnerability in the web-based management interface of **Cisco IP Phone** 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform configuration changes on the affected device, resulting in a denial of service (DoS) condition.

HIGH

Vector: network

Created: 2022-04-06

Updated: 2022-04-14

Source: *NIST*

NIST CVE: Medium

CVE-2022-20781

A vulnerability in the web-based management interface of **Cisco AsyncOS** Software for Cisco **Web Security Appliance** (WSA) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface.

MEDIUM

Vector: network

Created: 2022-04-06

Updated: 2022-04-14

CVE-2022-20782

A vulnerability in the web-based management interface of **Cisco Identity Services Engine** (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to improper enforcement of administrative privilege levels for high-value sensitive data. An attacker with read-only Administrator privileges to the web-based management interface on an affected device could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system.

MEDIUM

Vector: network

Created: 2022-04-06

Updated: 2022-04-14

Source: *NIST*

NIST CVE: Unrated

CVE-2022-1350

A vulnerability classified as problematic was found in **Ghostscript** 9.55.0. This vulnerability affects the function chunk_free object of the file gsmchunk.c. The manipulation with a malicious file leads to a memory corruption. The attack can be initiated remotely but requires user interaction. The exploit has been disclosed to the public as a POC and may be used. It is recommended to apply the patches to fix this issue.

UNRATED

Vector: unknown

Created: 2022-04-14

Updated: 2022-04-14

CVE-2022-1279

A vulnerability in the encryption implementation of EBICS messages in the open source library ebics-java/ebics-java-client allows an attacker sniffing network traffic to decrypt EBICS payloads. This issue affects: ebics-java/ebics-java-client versions prior to 1.2.

UNRATED

Vector: unknown

Created: 2022-04-14

Updated: 2022-04-14

CVE-2022-0023

An improper handling of exceptional conditions vulnerability exists in the DNS proxy feature of Palo Alto Networks **PAN-OS** software that enables a meddler-in-the-middle (MITM) to send specifically crafted traffic to the firewall that causes the service to restart unexpectedly. Repeated attempts to send this request result in denial-of-service to all PAN-OS services by restarting the device in maintenance mode. This issue does not impact **Panorama** appliances and **Prisma** Access customers. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.22; PAN-OS 9.0 versions earlier than PAN-OS 9.0.16; PAN-OS 9.1 versions earlier than PAN-OS 9.1.13; PAN-OS 10.0 versions earlier than PAN-OS 10.0.10; PAN-OS 10.1 versions earlier than PAN-OS 10.1.5. This issue does not impact PAN-OS 10.2.

UNRATED

Vector: unknown

Created: 2022-04-13

Updated: 2022-04-14

CVE-2022-27479

Apache Superset before 1.4.2 is vulnerable to SQL injection in chart data requests. Users should update to 1.4.2 or higher which addresses this issue.

UNRATED

Vector: unknown

Created: 2022-04-13

Updated: 2022-04-14

CVE-2022-24828

Composer is a dependency manager for the PHP programming language. Integrators using Composer code to call ``VcsDriver::getFileContent`` can have a code injection vulnerability if the user can control the ``$file`` or ``$identifier`` argument. This leads to a vulnerability on packagist.org for example where the composer.json's ``readme`` field can be used as a vector for injecting parameters into hg/Mercurial via the ``$file`` argument, or git via the ``$identifier`` argument if you allow arbitrary data there (Packagist does not, but maybe other integrators do). Composer itself should not be affected by the vulnerability as it does not call ``getFileContent`` with arbitrary data into ``$file`/`$identifier``. To the best of our knowledge this was not abused, and the vulnerability has been patched on packagist.org and Private Packagist within a day of the vulnerability report.

UNRATED

Vector: unknown

Created: 2022-04-13

Updated: 2022-04-14

CVE-2021-43154

Cross Site Scripting (XSS) vulnerability exists in **CMS Made Simple** 2.2.15 via the Name field in an Add Category **action** in moduleinterface.php.

UNRATED

Vector: unknown

Created: 2022-04-13

Updated: 2022-04-14

CVE-2022-24847

GeoServer is an open source software server written in **Java** that allows users to share and edit geospatial data. The GeoServer security mechanism can perform an unchecked JNDI lookup, which in turn can be used to perform class deserialization and result in arbitrary code execution. The same can happen while configuring data stores with data sources located in JNDI, or while setting up the disk **quota** mechanism. In order to perform any of the above changes, the attack needs to have obtained admin rights and use either the GeoServer GUI, or its REST API. The lookups are going to be restricted in GeoServer 2.21.0, 2.20.4, 1.19.6. Users unable to upgrade should restrict access to the ``geoserver/web`` and ``geoserver/rest`` via a firewall and ensure that the GeoWebCache is not remotely accessible.

UNRATED

Vector: unknown

Created: 2022-04-13

Updated: 2022-04-14

CVE-2022-24818

GeoTools is an open source **Java** library that provides tools for geospatial data. The GeoTools library has a number of data sources that can perform unchecked JNDI lookups, which in turn can be used to perform class deserialization and result in arbitrary code execution. Similar to the **Log4j** case, the vulnerability can be triggered if the JNDI names are user-provided, but requires admin-level login to be triggered. The lookups are now restricted in GeoTools 26.4, GeoTools 25.6, and GeoTools 24.6. Users unable to upgrade should ensure that any downstream application should not allow usage of remotely provided JNDI strings.

UNRATED

Vector: unknown

Created: 2022-04-13

Updated: 2022-04-14

	<div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
CVE-2022-24843	<div>Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. Gin-vue-admin 2.50 has arbitrary file read vulnerability due to a lack of parameter validation. This has been resolved in version 2.5.1. There are no known workarounds for this issue.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
CVE-2022-24816	<div>JAI-EXT is an open-source project which aims to extend the Java Advanced Imaging (JAI) API. Programs allowing Jiffle script to be provided via network request can lead to a Remote Code Execution as the Jiffle script is compiled into Java code via Janino, and executed. In particular, this affects the downstream GeoServer project. Version 1.2.22 will contain a patch that disables the ability to inject malicious code into the resulting script. Users unable to upgrade may negate the ability to compile Jiffle scripts from the final application, by removing janino-x.y.z.jar from the classpath.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>

CVE-2022-1345	<div>Stored XSS viva .svg file upload in GitHub repository causefx/organizr prior to 2.1.1810. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
---------------	--

CVE-2022-24788	<div>Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. Versions of vyper prior to 0.3.2 suffer from a potential buffer overrun. Importing a function from a JSON interface which returns `bytes` generates bytecode which does not clamp bytes length, potentially resulting in a buffer overrun. Users are advised to upgrade. There are no known workarounds for this issue.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
----------------	---

CVE-2022-24844	<div>Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. The problem occurs in the following code in server/service/system/sys_auto_code_pgsql.go, which means that PostgreSQL must be used as the database for this vulnerability to occur. Users must: Require JWT login? and be using PostgreSQL to be affected. This issue has been resolved in version 2.5.1. There are no known workarounds.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
----------------	--

CVE-2022-1347	<div>Stored XSS in the "Username" & "Email" input fields leads to account takeover of Admin & Co-admin users in GitHub repository causefx/organizr prior to 2.1.1810. Account takeover and privilege escalation</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
---------------	--

CVE-2022-24845	<div>Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. In affected versions, the return of `returns_int128()` is not validated to fall within the bounds of `int128`. This issue can result in a misinterpretation of the integer value and lead to incorrect behavior. As of v0.3.0, `returns_int128()` is validated in simple expressions, but not complex expressions. Users are advised to upgrade. There is no known workaround for this issue.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
----------------	---

CVE-2021-41119	<div>Wire-server is the system server for the wire back-end services. Releases prior to v2022-03-01 are subject to a denial of service attack via a crafted object causing a hash collision. This collision causes the server to spend at least quadratic time parsing it which can lead to a denial of service for a heavily used server. The issue has been fixed in wire-server 2022-03-01 and is already deployed on all Wire managed services. On premise instances of wire-server need to be updated to 2022-03-01, so that their backends are no longer affected. There are no known workarounds for this issue.</div> <div>UNRATED</div> <div>Vector: unknown Created: 2022-04-13 Updated: 2022-04-14</div>
----------------	---

Source: Hybrid Analysis

Top malicious files			
100% Threat score	cda37b13d1fdee1b4262b5a6146a35d8fc88fa572e55437a47a950037cc65d40	100% Threat score	W-975792762.xlsb
100% Threat score	FinHek.exe	100% Threat score	bd2906e0fd4d4ba5bbe954b50c8f056a8524868599a7257c9eae6cb6626f0170d
100% Threat score	clouidx-latest (1).exe	100% Threat score	62611275c4ae4a11bb2ad6a4d3a2890c80e023fd6e31c5b7b3dee43f08fe229d
100% Threat score	SETx64.dll	100% Threat score	tmpvjqo_m_
100% Threat score	Driver.exe	100% Threat score	USIGLOBAL - PO NO. 220330100837503 - H18G015 - 01.exe
100% Threat score	Service_21.exe	98% Threat score	AddPlug.exe
87% Threat score	7641ae596b53c5de724101bd6df35c999c9616d93503bce0ffd30b1c0d041e3b	85% Threat score	Wlniornez_Dablvtrq_converted.dll.bin
84% Threat score	avast_update_converted.dll.bin	83% Threat score	Invoice 13966396.html
83% Threat score	Invoice FW76857484.html	80% Threat score	LocalServiceComponents.exe
79% Threat score	W-623267633.xlsb	78% Threat score	48f7277ea1e7a782822db155c61709d44e363c29f77de41a67b9ca2a48e0d442
75% Threat score	MHPicViewer.exe		




Source: Hybrid Analysis

Top malicious URL			
98% Threat score	http://84.213.77.235:59871/Mozi.m	93% Threat score	http://27.220.83.47:46660/Mozi.a
93% Threat score	http://42.231.223.123:51511/Mozi.m	90% Threat score	http://www.101-bg.com/s16r/
80% Threat score	http://infoholix.net/redirect.php?mId=4263&mWeb=https%3A%2F%2Fstinagramaleenhancement.com	80% Threat score	http://infoholix.net/redirect.php?mId=4263&mWeb=https%3A%2F%2Fstinagramaleenhancement.com

80% Threat score	http://bit.ly/36wLZpK	80% Threat score	http://bit.ly/36wLZpK
80% Threat score	http://url9545.getontop.com/ls/click?upn=fVyQqGYzDdbAAki0FbwK6nwO1JKODu7K3kw2dTtBFm1EpXOTaDkjgK5z-2FSFaYQq9yB7R_uVmyxOCvQZpADzpg-2Br32WOpYr8mRYXz-2FI-2BSEL5GQhzWkCRxxQgLphT-2BG6Vkl-2BzKaz5mWcFoB0tF9KGJqwrx-2BPKLX4QmsGG3hsRQSPFE88mbYGA3xaK0WBgxdfemawa1xJfgWPIFjDfhGIWFFbXUibVzloza5rxIJVtqtKYaL-2BkM0mTcEJA6ul2CDFueOSjmceUB1xRG89Zaubd-2FriXj00vEZnFZAZq1iLlIo0n9TGZ0NHQmqBlwmrwygyM6UgUWVdlM12FYi9zKuPY2zF4y4PJKUY1oBSzQS-2BA60HoFIPy-2B-2B3p4H1HlCWtIS-2BbcepSjhfoaX5agsSOCXePs9PVBk8xK00HH1arQeMf8ii1SCvpwMA-2F-2B2EKGggLkTetc2ExxDSAwkfPqrKKbxm4-2Fz0yeobj3xp2KI9evrAFrmyusfi-2Bss4-3D	75% Threat score	http://www.defendx.it/
75% Threat score	http://www.101-bg.com/	73% Threat score	http://fghfghfdghdfg.tk/
73% Threat score	https://qokoro.cloud/yunohost/sso/?r=aHR0cHM6Ly9xb2tvcmluY2xvdWQv	73% Threat score	http://www.ministerodellasalute.pro.it/
73% Threat score	https://logosymetris.com/operators2/index.php?data=ZS5hbW1lbmRvbGFAaW5haWwuaXQ%3D		










Source: *SpamHaus*

Top spamming countries

 #1 United States of America	 #2 China
 #3 Russian Federation	 #4 Mexico
 #5 Dominican Republic	 #6 Saudi Arabia
 #7 Uruguay	 #8 India
 #9 Brazil	 #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 India
 #3 United States of America	 #4 Indonesia
 #5 Thailand	 #6 Viet Nam
 #7 Algeria	 #8 Brazil

			
	#9 Pakistan		#10 Japan

Source: [SpamHaus](#)

Top phishing countries

	#1 United States		#2 Japan
	#3 Netherlands		#4 Germany
	#5 Russia		#6 Canada
	#7 Singapore		#8 United Kingdom
	#9 Hong Kong		#10 China




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

Have I been pwnd

Nothing today




Source: [Imperva DDOS Map](#)

Top DDOS attackers

	United States (36%)
	Germany (14%)
	Netherlands (7%)

Source: [Imperva DDOS Map](#)

Top DDOS country targets

	Russia (31%)
	United States (27%)
	Ukraine (17%)

Source: [Imperva DDOS Map](#)

Top DDOS techniques

47%	DDoS
38%	Automated Threat
15%	OWASP

Source: [Imperva DDOS Map](#)

Top DDOS industry targets

34%	Financial Services
26%	Business
11%	Computing & IT

Source: [Ransom Watch](#)

Ransomware attacks

suncrypt	Atlas Copco	conti	Elevate Services
lockbit2	polyplastics.co...	lockbit2	tpdrug.com
lockbit2	www.cassinobuil...	lockbit2	www.mpm.fr

lockbit2	www.verifiedlab...	lockbit2	applya.com
lockbit2	get-greenenergy...	lockbit2	heartlandhealth...
lorenz	Simply Placed	everest	Standard Building Supplies Ltd