Security Rabbits

Your Security Rabbits report for February 18, 2022

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

28,695 vulnerabilities were disclosed in 2021 - the highest number on record

A total of 28,695 vulnerabilities were disclosed in 2021, according to a report from Risk Based Security. It puts the amount of risk that organizations and security teams face on full display.

The Hacker News

Another Critical RCE Discovered in Adobe Commerce and Magento Platforms

Adobe on Thursday updated its advisory for an actively exploited zero-day affecting Adobe Commerce and Magento Open Source to patch a newly discovered flaw that could be weaponized to achieve arbitrary code execution. Tracked as CVE-2022-24087, the issue - like CVE-2022-24086 - is rated 9.8 on the CVSS vulnerability scoring system and relates to an "Improper Input Validation" bug

Threatpost

Baby Golang-Based Botnet Already Pulling in $3K/Month for Operators

Newborn as it is, the Kraken botnet has already spread like wildfire, thanks to the malware's author tinkering away over the past few months, adding more infostealers and backdoors.

Security Affairs

CVE-2021-44731 Linux privilege escalation bug affects Canonical's Snap Package Manager

Qualys experts found a new Linux privilege escalation vulnerability, tracked as CVE-2021-44731, in Canonical's Snap Package Manager. Canonical's Snap software packaging and deployment system are affected by multiple vulnerabilities, including a privilege escalation flaw tracked as CVE-2021-44731 (CVSS score 7.8). Snap is a software packaging and deployment system developed by Canonical for operating systems that use the Linux [...] The post CVE-2021-44731 Linux privilege escalation bug affects Canonical's Snap Package Manager appeared first on Security Affairs.

CyberScoop

Deep dive into hack against Iranian state TV yields wiper malware, other custom tools

The Jan. 27 hack of Iranian state broadcaster IRIB -- which ran a message of support for opposition leaders and called for the assassination of Iran's supreme leader -- came with previously unidentified wiper malware, according to research that suggests the incident was more destructive than initially assumed. Researchers with Check Point, a Tel Aviv-based cybersecurity company, published the findings Friday based on what it said were files and other forensic evidence connected to the hack. Iranian officials acknowledged the attack at the time, saying that "disruptions" also occurred on another television channel and two radio stations, and called the hack "complex." The breach occurred the [...]

Security Affairs

European Data Protection Supervisor call for bans on surveillance spyware like Pegasus

The European Data Protection Supervisor authority called for a ban on the development and the use of Pegasus-like commercial spyware. The European Data Protection Supervisor (EDPS) authority this week called for a ban on the development and the use of surveillance software like the Pegasus spyware in the EU. Pegasus is a surveillance malware developed by [...] The post European Data Protection Supervisor call for bans on surveillance spyware like Pegasus appeared first on Security Affairs.

Cyware News - Latest Cyber News

FreeCryptoScam - A New Cryptocurrency Scam That Leads to Installation of Backdoors and Stealers

When the victim downloads the payload, it leads to the installation of multiple malware payloads on the victim's system, allowing the threat actor to establish backdoors and/or steal user information.

The Hacker News

Getting Your SOC 2 Compliance as a SaaS Company

If you haven't heard of the term, you will soon enough. SOC 2, meaning System and Organization Controls 2, is an auditing procedure developed by the American Institute of CPAs (AICPA). Having SOC 2 compliance means you have implemented organizational controls and practices that provide assurance for the safeguarding and security of client data. In other words, you have to show (e.g., document

Cyware

Intel Software and Firmware Updates Patch 18 High-Severity Vulnerabilities

Intel has released software and firmware updates to address many vulnerabilities found in the company's products. It released 22 security

The Hacker News

4 Cloud Data Security Best Practices All Businesses Should Follow Today

These days, businesses all around the world have come to depend on cloud platforms for a variety of mission-critical workflows. They keep their CRM data in the cloud. They process their payrolls in the cloud. They even manage their HR processes through the cloud. And all of that means they're trusting the bulk of their privileged business data to those cloud providers, too. And while most major

The Hacker News

Attackers Can Crash Cisco Email Security Appliances by Sending Malicious Emails

Cisco has released security updates to contain three vulnerabilities affecting its products, including one high-severity flaw in its Email Security Appliance (ESA) that could result in a denial-of-service (DoS) condition on an affected device. The weakness, assigned the identifier CVE-2022-20653 (CVSS score: 7.5), stems from a case of insufficient error handling in DNS name resolution that could

Cyware News - Latest Cyber News

Baltimore City Fell Prey to Cybercriminal Posing as Contractor to Siphon Funds

A new report by the Office of the Inspector General (OIG) has revealed that Baltimore city was tricked out of hundreds of thousands of dollars last year by a cyber-criminal posing as a vendor.

Cyware News - Latest Cyber News

Deciphering Moses Staff APT's Persistent Attacks Against Israeli Organizations

As per a new update shared by Cybereason Nocturnus Team, the APT group has made improvements in tactics and techniques to target several organizations located across Italy, India, Germany, China, Turkey, the UAE, and the U.S.

CyberScoop

DOJ beefs up efforts to combat criminal use of cryptocurrencies

The U.S. government is intensifying efforts to combat the criminal use of cryptocurrencies as federal prosecutors continue to target the business models and logistics of cybercrimes such as ransomware, Deputy Attorney General Lisa Monaco said Thursday. Speaking at the Munich Cyber Security Conference to announce several key developments in the government's approach, Monaco said that the National Cryptocurrency Enforcement Team (NCET) -- unveiled in October as part of an overall U.S. government to focus its resources on combatting ransomware operators -- is getting its first director: Eun Young Choi. Choi is a seasoned federal cybersecurity prosecutor who most recently led the prosecution of [...]

Cyware News - Latest Cyber News

Extend Fertility Suffered Ransomware Attack Impacting Patients' Protected Health Information

Extend Fertility was hit with ransomware in the month of December 2021. The clinic hired third-party digital forensic specialists to determine the incident's nature and scope.

IT Security Guru

French Dad tries to block his kids internet, wipes out town WiFi

A French father attempting to use a signal jammer to prevent his children from accessing the internet accidentally knocked out an entire town's internet connection. A complaint was sent to the French Agence Nationale des Frequences, who are responsible for managing radio frequencies in the country received an unusual complaint (translated) from a mobile phone operator. [...] The post French Dad tries to block his kids internet, wipes out town WiFi appeared first on IT Security Guru.

The Hacker News

Google Bringing Privacy Sandbox to Android to Limit Sharing of User Data

Google on Wednesday announced plans to bring its Privacy Sandbox initiatives to Android in a bid to expand its privacy-focused, but also less disruptive, advertising technology beyond the desktop web. To that end, the internet giant said it will work towards building solutions that prevent cross-app tracking a la Apple's App Tracking Transparency (ATT) framework, effectively limiting sharing of

The Hacker News

Iranian Hackers Targeting VMware Horizon Log4j Flaws to Deploy Ransomware

A "potentially destructive actor" aligned with the government of Iran is actively exploiting the well-known Log4j vulnerability to infect unpatched VMware Horizon servers with ransomware. Cybersecurity firm SentinelOne dubbed the

News - Latest Cyber News

advisories, including seven with a severity rating of "high."

Threatpost

Kill Cloud Risk: Get Everybody to Stop Fighting Over App Security - Podcast

When it comes to ensuring safe cloud app rollouts, there's flat-out animosity between business shareholders. HackerOne's Alex Rice and GitLab's Johnathan Hunt share tips on quashing all the squabbling.

Threatpost

Microsoft Teams Targeted With Takeover Trojans

Threat actors are infiltrating the increasingly popular collaboration app to attach malicious files to chat threads that drop system-hijacking malware.

Cyware News - Latest Cyber News

Multiple vulnerabilities found in Snap-confine function on Linux systems

Security researchers with Qualys have discovered several vulnerabilities affecting Canonical's Snap software packaging and deployment system and urged users to apply patches.

Cyware News - Latest Cyber News

New quantum key distribution network resistant to quantum attacks

A QKD channel was multiplexed on the same fiber as ultra-high bandwidth 800 Gbps optical channels for the first time and used to provide keys for encryption of the data stream.

Cyware News - Latest Cyber News

Poisoned pipelines: Security researcher explores attack methods in CI environments

A security researcher has described how abusing permissions in source code management (SCM) repositories can lead to CI poisoning, also known as 'poisoned pipeline attacks'.

Security Affairs

Researchers created a PoC exploit for recently disclosed critical Magento CVE-2022-24086 bug

Researchers developed an exploit code for CVE-2022-24086 vulnerability affecting Adobe Commerce and Magento Open Source. Positive Technologies researchers have created a working PoC exploit for the recently patched CVE-2022-24086 vulnerability affecting its Commerce and Magento Open Source products. An attacker could use the exploit to achieve remote code execution from an unauthenticated user. This week, Adobe rolled […] The post Researchers created a PoC exploit for recently disclosed critical Magento CVE-2022-24086 bug appeared first on Security Affairs.

Naked Security

S3 Ep70: Bitcoin, billing blunders, and 0-day after 0-day after 0-day [Podcast + Transcript]

Latest episode - listen and learn!

Security Affairs

Specially crafted emails could crash Cisco ESA devices

Cisco warns of a DoS issue affecting its Email Security Appliance (ESA) product that could be exploited using specially crafted emails. Cisco ESA products are affected by a DoS vulnerability, tracked as CVE-2022-20653, that resides in the DNS-based Authentication of Named Entities (DANE) email verification component of Cisco AsyncOS Software for ESA. A remote, unauthenticated attacker […] The post Specially crafted emails could crash Cisco ESA devices appeared first on Security Affairs.

ZDNet | security RSS

Thanks, dad: jammer used to stop kids going online, wipes out a town's internet by mistake

The -interesting- control method could lead to a hefty fine and jail time.

Cyware News - Latest Cyber News

UK Cyber Sector Generates Record Investment and Revenue

The DCMS Annual Cyber Sector Report 2022 revealed more than PS1 billion (~$1.36 billion) was raised in external investment over 84 deals during this period by the UK's cybersecurity industry.

IT Security Guru

Vulnerability found in major WordPress plugin

UpdraftPlus, a WordPress plugin with over 3 million installations, has been patched following the discovery of a vulnerability by security researcher Marc Montpas. The Wordfence Threat Intelligence team explained in a blog post that the vulnerability enables any logged in user, including subscriber-level users, to download backups made with the plugin. The WordPress security company […] The post Vulnerability found in major WordPress plugin appeared first on IT Security Guru.

group "TunnelVision" owing to their heavy reliance on tunneling tools, with overlaps in tactics observed to that of a broader group tracked under the moniker Phosphorus

IT Security Guru

Major vape vendor hacked

According to BleepingComputer, Element Vape, a major online vendor of e-cigarettes and vaping kits is serving a credit card skimmer on its live site, presumably after being hacked. The company sells e-cigarettes, vaping equipment, e-liquids and CBD products and has significant presence across the US and Canada. Element Vape's website is hosting a malicious JavaScript […] The post Major vape vendor hacked appeared first on IT Security Guru.

ZDNet | security RSS

Microsoft warns of emerging 'ice phishing' threat on blockchain, DeFi networks

The firm says that the introduction of Web3 may also bring with it unique forms of phishing.

The Hacker News

New Linux Privilege Escalation Flaw Uncovered in Snap Package Manager

Multiple security vulnerabilities have been disclosed in Canonical's Snap software packaging and deployment system, the most critical of which can be exploited to escalate privilege to gain root privileges. Snaps are self-contained application packages that are designed to work on operating systems that use the Linux kernel and can be installed using a tool called snapd. Tracked

ZDNet | security RSS

New RCE flaw added to Adobe Commerce, Magento security advisory

Researchers have also been able to replicate the original security flaw.

Cyware News - Latest Cyber News

Ransomware's savage reign continues as attacks increase 105%

Researchers diligently tracked the dramatic rise in ransomware, recording an astounding 318.6 million more ransomware attacks than 2020, a 105% increase. Ransomware volume has risen 232% since 2019.

Cyware News - Latest Cyber News

Researchers Thwart Largest Ever Bot Attack Leveraging 400,000 Compromised IP Addresses

Imperva researchers said that the large-scale botnet generated 400 million requests from the IP addresses over four days, comprising around 10 requests per IP per hour on average.

Cyware News - Latest Cyber News

Snyk Buys Cloud Security Vendor Fugue To Protect Developers

Snyk has purchased Cloud Security Posture Management (CSPM) vendor Fugue to help organizations manage compliance and security throughout the software development lifecycle.

Cyware News - Latest Cyber News

TA2541: A Tale of New Mysterious Hackers

Proofpoint discovered a new threat group, dubbed TA2541, targeting entities in the aviation, aerospace, transportation, defense, and manufacturing sectors, since at least 2017. The most delivered RAT in TA2541 campaigns include AsyncRAT, followed by Parallax, NetWire, and WSH RAT. The campaigns are still active and spreading phishing emails to target victims around the world.

Security Affairs

Threat actors leverage Microsoft Teams to spread malware

Attackers compromise Microsoft Teams accounts to attach malicious executables to chat and spread them to participants in the conversation. While the popularity of Microsoft Teams continues to grow, with roughly 270 million monthly active users, threat actors started using it as an attack vector. Starting in January 2022, security researchers from Avanan observed attackers compromising […] The post Threat actors leverage Microsoft Teams to spread malware appeared first on Security Affairs.

Threatpost

Ukrainian DDoS Attacks Should Put US on Notice-Researchers

On Tuesday, institutions central to Ukraine's military and economy were hit with denial-of-service (DoS) attacks. Impact was limited, but the ramifications are not.

Twitter

RedPacket Security

HUAWEI EMUI/Magic UI code execution | CVE-2021-39994 -

CVE-2021-39994 There is an arbitrary address access vulnerability with the

RedPacket Security

HUAWEI EMUI/Magic UI code execution | CVE-2021-39997 -

CVE

product line test code.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.

Wolfgang Sesin

New post from (CVE-2021-39997) has been published on

www.sesin.at

New post from (Huawei EMUI Audio out-of-bounds read [CVE-2021-39997]) has been published on

Threat Intel Center

NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL

Remotely Alerts

Severity: | There is a vulnerability of unstrict inp... | CVE-2021-39997 | Link for more:

CVE

CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access.

www.sesin.at

New post from (CVE-2021-39997) has been published on

Wolfgang Sesin

New post from (Huawei EMUI Audio out-of-bounds read [CVE-2021-39997]) has been published on

Threat Intel Center

NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL

Threat Intel Center

NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL

Source: NIST

NIST CVE: Critical

CVE-2021-42940

A Cross Site Scripting (XSS) vulnerability exists in **Projeqtor** 9.3.1 via /projeqtor/tool/saveAttachment.php, which allows an attacker to upload a SVG file containing malicious JavaScript code.

CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-18

CVE-2020-36062

Dairy Farm Shop Management System v1.0 was discovered to contain hardcoded credentials in the source code which allows attackers access to the **control panel** if compromised.

CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-18

CVE-2021-44521

When running **Apache Cassandra** with the following configuration: enable_user_defined_functions: true enable_scripted_user_defined_functions: true enable_user_defined_functions_threads: false it is possible for an attacker to execute arbitrary code on the host. The attacker would need to have enough permissions to create user defined functions in the cluster to be able to exploit this. Note that this configuration is documented as unsafe, and will continue to be considered unsafe after this CVE.

CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-18

CVE-2022-24112

An attacker can abuse the batch-requests plugin to send requests to bypass the IP restriction of Admin API. A default configuration of **Apache APISIX** (with default API key) is vulnerable to remote code execution. When the admin key was changed or the port of Admin API was changed to a port different from the data panel, the impact is lower. But there is still a risk to bypass the IP restriction of Apache APISIX's data panel. There is a check in the batch-requests plugin which overrides the client IP with its real remote IP. But due to a bug in the code, this check can be bypassed.

CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-18

CVE-2020-13675

Drupal's JSON:API and REST/File modules allow file uploads through their HTTP APIs. The modules do not correctly run all file validation, which causes an access bypass vulnerability. An attacker might be able to **upload files** that bypass the file validation process implemented by modules on the site.

CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-18

Source: NIST

NIST CVE: High

CVE-2022-24289

Hessian serialization is a network protocol that supports object-based **transmission**. **Apache** Cayenne's optional Remote Object Persistence (ROP) feature is a web services-based technology that provides object persistence and query functionality to 'remote' applications. In Apache Cayenne 4.1 and earlier, running on non-current patch versions of Java, an attacker with **client access** to Cayenne ROP can transmit a malicious payload to any vulnerable third-party dependency on the server. This can result in arbitrary code execution.

HIGH Vector: network Created: 2022-02-11 Updated: 2022-02-18

CVE-2020-13677

Under some circumstances, the **Drupal** core JSON:API module does not properly restrict access to certain content, which may result in unintended access bypass. Sites that do not have the JSON:API module enabled are not affected.

HIGH Vector: network Created: 2022-02-11 Updated: 2022-02-18

CVE-2021-23597

This affects the package **fastify-multipart** before 5.3.1. By providing a name=constructor property it is still possible to crash the application. **Note:** This is a bypass of CVE-2020-8136 (https://security.snyk.io/vuln/SNYK-JS-FASTIFYMULTIPART-1290382).

HIGH Vector: network Created: 2022-02-11 Updated: 2022-02-18

Source: NIST

NIST CVE: Medium

CVE-2021-45387

tcpreplay 4.3.4 has a Reachable Assertion in add_tree_ipv4() at tree.c.

MEDIUM Vector: local Created: 2022-02-11 Updated: 2022-02-18

CVE-2020-13676

The QuickEdit module does not properly check access to fields in some circumstances, which can lead to unintended disclosure of field data. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed.

MEDIUM Vector: network Created: 2022-02-11 Updated: 2022-02-18

CVE-2021-45386

tcpreplay 4.3.4 has a Reachable Assertion in add_tree_ipv6() at tree.c

MEDIUM Vector: local Created: 2022-02-11 Updated: 2022-02-18

CVE-2020-13674

The QuickEdit module does not properly validate access to routes, which could allow cross-site request forgery under some circumstances and lead to possible data integrity issues. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed. Removing the "access in-place editing" permission from untrusted users will not fully mitigate the vulnerability.

MEDIUM Vector: network Created: 2022-02-11 Updated: 2022-02-18

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2020-8107

A Process Control vulnerability in ProductAgentUI.exe as used in **Bitdefender Antivirus Plus** allows an attacker to tamper with product settings via a specially crafted DLL file. This issue affects: Bitdefender **Antivirus Plus** versions prior to 24.0.26.136. Bitdefender **Internet** Security versions prior to 24.0.26.136. Bitdefender **Total Security** versions prior to 24.0.26.136.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2021-41599

A remote code execution vulnerability was identified in **GitHub Enterprise Server** that could be exploited when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.0.21, 3.1.13, 3.2.5. This vulnerability was reported via the GitHub Bug Bounty program.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2022-25319

An issue was discovered in Cerebrate through 1.4. Endpoints could be open even when not enabled.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2022-25320

An issue was discovered in Cerebrate through 1.4. Username enumeration could occur.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2021-46108

D-Link DSL-2730E CT-20131125 devices allow XSS via the username parameter to the password page in the maintenance configuration.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2022-25314

In **Expat** (aka libexpat) before 2.4.5, there is an integer overflow in copyString.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2021-44730

snapd 2.54.2 did not properly validate the location of the snap-confine binary. A local attacker who can **hardlink** this binary to another location to cause snap-confine to execute other arbitrary binaries and hence gain privilege escalation. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-18

CVE-2022-22922

TP-Link TL-WA850RE Wi-Fi Range Extender before v6_200923 was discovered to use highly predictable and easily detectable session keys, allowing attackers to gain administrative privileges.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2021-44731

A race condition existed in the **snapd** 2.54.2 snap-confine binary when preparing a private mount namespace for a snap. This could allow a local attacker to gain root privileges by bind-mounting their own contents inside the snap's private mount namespace and causing snap-confine to execute arbitrary code and hence gain privilege escalation. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-18

CVE-2022-25318

An issue was discovered in Cerebrate through 1.4. An incorrect sharing group ACL allowed an unprivileged user to edit and modify sharing groups.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2022-25317

An issue was discovered in Cerebrate through 1.4. genericForm allows reflected XSS in form descriptions via a user-controlled description.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2022-25321

An issue was discovered in Cerebrate through 1.4. XSS could occur in the bookmarks component.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2022-25313

In **Expat** (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2022-25315

In **Expat** (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-18

CVE-2021-4120

snapd 2.54.2 fails to perform sufficient validation of snap content interface and layout paths, resulting in the ability for snaps to inject arbitrary **AppArmor** policy rules via malformed content interface and layout declarations and hence escape strict snap confinement. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-18

Source: Hybrid Analysis

Top malicious files

100% Threat score — CallApp v1 (.) 916 (.) apk

100% Threat score — PacketClient (.) exe

100% Threat score — stclientid109 (.) js

96% Threat score — reserva (.) exe

92% Threat score — 3eed5f9a1d57b6ae71a5d434ea38814d

87% Threat score — wsc (.) dll

80% Threat score — ConfigMgrWebService 1 (.) 8 (.) 0 (.) msi

75% Threat score — IRULE v0 (.) 1 (.) 6 (.) exe

73% Threat score — Setup_Power_BI_Helperv12 (.) 2 (.) msi

100% Threat score — 2e85ca515acbfd4b03f93218764e3166af04eb6f75de14ce4dfd97d6ef259579

100% Threat score — delfino-g3 (.) exe

98% Threat score — eed2ab9f2c09e47c7689204ad7f91e5aef3cb25a41ea524004a48bb7dc59f969

94% Threat score — Setup (1) (.) exe

91% Threat score — 8296df9afa5aa40b9fc1f5e015a15f57dd5e0c8f26b1630feebea6961a0f43e4

80% Threat score — full (.) exe

78% Threat score — e-Fax (.) html

75% Threat score — UltimateS2Installer-2 (.) 1 (.) 1 (.) exe

Source: Hybrid Analysis

Top malicious URL

Threat score	URL
88%	http://59 (.) 94 (.) 206 (.) 17:38675/bin (.) sh
87%	http://mail (.) gms (.) pwc (.) com/ls/click?upn=w2i3qkzj-2BZr7plnkJ5K3BdhHelFEBn83qG9SGC9-2Fmt3-2BLCvwmkEqCC40Q0HCOdNjZaHG0o-2FkucXBW6OPpu9uChp5KSNwosyAyAkGws1RjGAVgUs4UboRvsRZxQNf9LqjYt51j-2BdClTh3pRo-2BLz7ldpIZcMNxTC2FhO5hUFYGSV4-3DrOLR_t-2BDoMIxxm4FGLFhQ6N7LXBizr9CblzSk6fkj7YhfHtIs3-2BQEJAgfQwjIQMYiTvxlD8u2lKMjtLbZc-2BMJbCKBCtskJ7Zk6c5Jfd59eQzQleu-2B3YgzHEtoIvjzqjxQvNDA9YlHh7AqSFP6cqADy3wTyXEsJWOyC-2F-2BUSb-2FhbWMuxuckMUj7DiWq9R7hkjUs-2FnTj2qNzvGo9vrKFMmVvGGQCkvqhT5tIb60edb39zs-2FMTCkab2nL1GnAbiXR7l-2B6CcjZnUzaVsk0h06jk19YlaTskI7xspBhgbAw5-2FOEgpKmtoXMZIx4UeHcFnJqirdfy5fxTsOr5p9tqACOrUQiAyy4YKiWCW1-2BoV14mzqrArcpJ2oGgFbDeL3LUyAjF-2FoQeWTQGZoNkhWCYOCSp9-2FpilY4Ryg0Etl9-2FIp-2B4xV8lm6EFyeN8A2W5a6V2tkC5osWnO-2FZHYhPc3qNYqXmjboIYiQnQJ5vJLdnOhXqSrNUkyi-2Bc-2B75HHlrRAcbW2y8UtxmfiCrhrxT680BkTEMGvKqUqjoQpfCHP3SBWwLvpHa5RN9EoiT8uadSG6dZ7jdI4lg18R4zCHp8pv5NPQYsVdvdiSlWakg35nj7PP1E4kKWZXRAfk4LwS8yjE8Tty 2BHU2gBy0m
82%	http://aboveredirect (.) top/
79%	https://edhcceb (.) r (.) bh (.) d (.) sendibt3 (.) com/tr/cl/ts7WR0VpA5UK4VuRmSaaGkoQ8am9j-fyi2xYz_mU7Nf8hZt-kLjqfwJGBVihjrZ9mqwQ7-ZbXpqBXn4YhVdYZxCrqKi_LMGuGYUdEwujQULeqhEgXHRVue6Gl8_M9OA5wsquWFXQrj8b8on0p3Kn4-UL_4NzA0asQi3fCLARYoL_jke8XhqQLz3-AqJuCZSzWA121_wA1ABBVYFrulEpqn990BJ_0qgunWRfnP4yantEqmVBxPzwl_AzfO_OXko#avisos (.) exercito%40defesa (.) pt
77%	http://uplod (.) net/o3pbwm0myu2pahd8
74%	http://mwqsj2 (.) 2ywuw (.) mikeakintayo (.) com/
74%	http://wlmr35 (.) eqkmz (.) mikeakintayo (.) 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 Japan
#9 Brazil	#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 Indonesia
- #5 Thailand
- #6 Algeria
- #7 Viet Nam
- #8 Brazil
- #9 Iran (Islamic Republic of)
- #10 Pakistan

Source: SpamHaus

Top phishing countries

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