Your Security Rabbits report for February 11, 2022

Hot topics

Nothing today

News

ZDNet | security RSS

$1.3 billion lost to romance scams in the past five years: FTC

Romance scams are reaching record-highs, regulators warn.

The Hacker News

Apple Releases iOS, iPadOS, macOS Updates to Patch Actively Exploited Zero-Day Flaw

Apple on Thursday released security updates for iOS, iPadOS, macOS, and Safari to address a new WebKit flaw that it said may have been actively exploited in the wild, making it the company's third zero-day patch since the start of the year. Tracked as CVE-2022-22620, the issue concerns a use-after-free vulnerability in the WebKit component that powers the Safari web browser and

Cyware News - Latest Cyber News

Californian College Attacked with Ransomware

The online student portal was down for 17 days, and Ohlone College's phone and email systems were knocked offline for 10 days. A separate student information system was also impacted.

The Hacker News

COVID Does Not Spread to Computers

"...well, of course!" is what you might think. It's a biological threat, so how could it affect digital assets? But hang on. Among other effects, this pandemic has brought about a massive shift in several technological areas. Not only did it force numerous organizations - that up to now were reluctant - to gear up in cyber to go digital, all at once, oftentimes with hastily pieced together

IT Security Guru

DDoS attacks hit historic peak

Cybersecurity company Kaspersky found that distributed denial of service (DDoS) attacks recorded quarterly peaked towards the end of 2021. The company's DDoS attacks in Q4 2021 Report found the total number of DDoS attacks that occurred in Q4 2021 was 4.65 times higher compared with Q4 the previous year, then showing an increase of 52% […] The post DDoS attacks hit historic peak appeared first on IT Security Guru.

CyberScoop

EARN IT Act gets no changes to encryption language in Senate committee

The Senate Judiciary Committee approved legislation Thursday that is designed to crack down on child sexual abuse materials online, despite warnings from privacy advocates that the bill could pose a major threat to encrypted technologies. The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act), introduced for the first time in 2020 by Sens. Lindsey Graham, R-S.C., and Richard Blumenthal, D-Conn., would remove legal liability immunity from tech platforms found in violation of federal or state laws regarding child sexual abuse materials (CSAM). In 2020 the EARN IT Act sailed out of committee but failed to see a floor vote before the end of the 116th Congress. […]

Cyware News - Latest Cyber News

FritzFrog Botnet Grows 10x, Hits Healthcare, Education, and Government Systems

Discovered in August 2020, the malware is written in Golang and is considered to be a sophisticated threat that relies on custom code, runs in memory, and is a decentralized peer-to-peer (P2P) botnet.

The Hacker News

FritzFrog P2P Botnet Attacking Healthcare, Education and Government Sectors

A peer-to-peer Golang botnet has resurfaced after more than a year to compromise servers belonging to entities in the healthcare, education, and government sectors within a span of a month, infecting a total of 1,500 hosts. Dubbed FritzFrog, "the decentralized botnet targets any device that exposes an SSH server -- cloud instances, data center servers, routers, etc. -- and is capable of running

WeLiveSecurity

Hidden in plain sight: How the dark web is spilling onto social media

A trip into the dark corners of Telegram, which has become a magnet for criminals peddling everything from illegal drugs to fake money and COVID-19 vaccine passes The post Hidden in plain sight: How the dark web is spilling onto social media appeared first on WeLiveSecurity

IT Security Guru

API Security in the spotlight as Salt Security becomes next Black Unicorn

In December 2021, Gartner(r) reviewed its earlier predictions about API attacks, commenting, "On Target: 2017 Prediction -- By 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise web applications.... As 2022 approaches, this prediction could arguably be counted as "missed" -- but only because we underestimated the steep rise in […] The post API Security in the spotlight as Salt Security becomes next Black Unicorn appeared first on IT Security Guru.

Security Affairs

Attackers Increasingly Adopting Regsvr32 Utility Execution Via Office Documents

The Uptycs threat research team has been observing an increase in utilization of regsvr32.exe heavily via various types of Microsoft Office documents. The full report that includes Indicators of Compromise (IOCs) is available here: https://www.uptycs.com/blog/attackers-increasingly-adopting-regsvr32-utility-execution-via-office-documents During our analysis of these malware samples, we have identified that some of the malware samples belonged to Qbot and […] The post Attackers Increasingly Adopting Regsvr32 Utility Execution Via Office Documents appeared first on Security Affairs.

Cyware News - Latest Cyber News

Charity Site for Ottawa Truckers' 'Freedom Convoy' Protest Exposes Donors' Passports and Driver Licenses

The donation site used by truckers in Ottawa who are currently protesting against national vaccine mandates has fixed a security lapse that exposed the passports and driver licenses of donors.

IT Security Guru

Cybersecurity Association of Maryland to set up Centres of Excellence

The Cybersecurity of Maryland, Inc (CAMI) announced today plans to expand its membership program alongside setting up Centres of Excellence. CAMI aims to develop cybersecurity in the Old Line State through collaboration and advocacy. The organisation hopes to foster cooperation in cybersecurity through opportunities for companies across all industries. The organisation announced today that it […] The post Cybersecurity Association of Maryland to set up Centres of Excellence appeared first on IT Security Guru.

Threatpost

Decryptor Keys Published for Maze, Egregor, Sekhmet Ransomwares

The Maze gang are purportedly never going back to ransomware and have destroyed all of their ransomware source code, said somebody claiming to be the developer.

The Hacker News

France Rules That Using Google Analytics Violates GDPR Data Protection Law

French data protection regulators on Thursday found the use of Google Analytics a breach of the European Union's General Data Protection Regulation (GDPR) laws in the country, almost a month after a similar decision was reached in Austria. To that end, the National Commission on Informatics and Liberty (CNIL) ruled that the transatlantic movement of Google Analytics data to the U.S. is not "

ZDNet | security RSS

FritzFrog botnet returns to attack healthcare, education, government sectors

The botnet managed to strike at least 500 government and enterprise SSH servers in eight months.

Cyware News - Latest Cyber News

Georgia Voter Information Leaked Online After EasyVote Solutions Security Breach

Public information about voters was posted to an online forum, but the breach didn't involve Social Security numbers or driver's license numbers, said Charles Davis, CFO for EasyVote.

Security Affairs

How Does An IPv6 Proxy Work & How Enterprises Can Get Benefit?

IPv6 became imperative after developers discovered that IPv4 had a finite number and addresses. How does an IPv6 Proxy work? Technological advancements have come a long way - from when internet utility was very limited to when internet connection was achieved only through internet protocol (IP) version 4 (IPv4) addresses to this modern age where […] The post How Does An IPv6 Proxy Work & How Enterprises Can Get Benefit? appeared first on

Cyware News - Latest Cyber News

Information for over 6,000 Memorial Hermann patients accessed in security breach

One of its contracted vendors, Advent Health Partners, announced a cybersecurity issue Tuesday. According to the health system, the protected health information of 6,260 patients has been breached.

Cyware News - Latest Cyber News

Microsoft fixes Defender flaw letting hackers bypass antivirus scans

Microsoft addressed a weakness in the Microsoft Defender Antivirus on Windows that allowed attackers to plant and execute malicious payloads without triggering Defender's malware detection engine.

Cyware News - Latest Cyber News

Moxa customers urged to patch five vulnerabilities found in MXview network management software

The issues affect the Taiwanese company's MXview web-based network management system versions 3.x to 3.2.2 and collectively, ICS-CERT scored the vulnerabilities a 10.0, its highest criticality score.

Cyware News - Latest Cyber News

New Vulnerabilities Can Allow Hackers to Remotely Crash Siemens PLCs

Siemens this week announced the availability of patches and mitigations for a series of severe vulnerabilities that can be exploited to remotely crash some of the company's SIMATIC products.

CyberScoop

Online romance scams expand, now with more cryptocurrency

Reports of online romance scams continued to grow in 2021, according to the Federal Trade Commission, and cryptocurrency payments now represent a big chunk of the money lost. Complaints about these heartbreaking swindles added up to $547 million overall last year, the agency said Thursday, up about 80 percent from the $307 million reported to the FTC in 2020. Of that total, $139 million in reported losses came from cryptocurrency transactions. In those cases, the victims often are subjected to a fancier plea for money than what typically occurs in a romance scam. "People are led to believe their new online companion is a successful investor who, before long, casually offers investment advice[...]

CyberScoop

Project Zero researchers see promising trends in vulnerability fixes

Big tech vendors generally are remediating serious bugs faster than they were three years ago, according to a new report from Google's Project Zero. The data -- while limited to vulnerabilities the group itself reported between January 2019 and December 2021, and influenced by what the group's researchers have chosen to pursue -- offers "a number of promising trends," according to Ryan Schoen of Project Zero. "Vendors are fixing almost all of the bugs that they receive, and they generally do it within the 90-day deadline plus the 14-day grace period when needed," he wrote. In 2021 there was not "a single 90 day deadline exceeded," which could be because responsible disclosure policies are be[...]

Threatpost

Sharp SIM-Swapping Spike Causes $68M in Losses

The attacks, which lead to 2FA defeat and account takeover, have accelerated by several hundred percent in one year, leading to thousands of drained bank accounts.

Security Affairs

Spanish police dismantled SIM swapping gang who stole money from victims' bank accounts

Spanish National Police arrested eight alleged members of a crime ring specialized in SIM swapping attacks. Spanish National Police has arrested eight alleged members of a crime organization who were able to steal money from the bank accounts of the victims through SIM swapping attacks. Crooks conduct SIM swapping attacks to take control of victims' […] The post Spanish police dismantled SIM swapping gang who stole money from victims' bank accounts appeared first on Security Affairs.

Cyware News - Latest Cyber News

The Record by Recorded Future

During an attack on Texan cities, the decision not to pay ransom had a surprising knock-on effect: it forced a notorious ransomware gang, the Russia-based REvil, to rethink how it did business.

Cyware News - Latest Cyber News

University Project Cataloged 1,100 Ransomware Attacks on Critical Infrastructure

The latest version of the critical infrastructure ransomware attacks (CIRWA) database created by researchers catalogs 1,137 incidents reported between November 2013 and January 31, 2022.

Blog â€" Flashpoint

When Every Day Is Valentine's Day: How Threat Actors Prey on Lonely Hearts

Love in the time of threat actors Theoretically, there's isn't anything wrong with Valentine's Day. But let's just say it like it is: Nobody likes Valentine's Day, a guileless push for capital, like Halloween for the heart. To be fair, some people do, but we feel it's safe to say that most people, single or […] The post When Every Day Is Valentine's Day: How Threat Actors Prey on Lonely Hearts appeared first on Flashpoint.

Security Affairs.

Cyware News - Latest Cyber News

Legit Security Launches Out of Stealth with Series A Investment to Secure Software Supply Chains

Legit Security announced its launch out of stealth mode with a Series A $30 million funding announcement with leading venture capital firms Bessemer Venture Partners and TCV.

Cyware News - Latest Cyber News

Microsoft starts killing off WMIC in Windows, will thwart attacks

Microsoft is moving forward with removing the Windows Management Instrumentation Command-line (WMIC) tool, wmic.exe, starting with the latest Windows 11 preview builds in the Dev channel.

IT Security Guru

Nearly $1.3 billion ransom paid to hackers since 2020

Cryptocurrency experts have warned that ransomware payments will likely surpass both the $602m already identified and the 2020 figure. The Ransomware Crypto Crime Report produced by blockchain investigations and analytics company Chainalysis presents significant insight into industry trends. The report shows that average payment size has soared in recent years. In 2019 it was only […] The post Nearly $1.3 billion ransom paid to hackers since 2020 appeared first on IT Security Guru.

Cyware News - Latest Cyber News

NightDragon Leads New Growth Round in ThriveDX alongside Prytek

A dedicated cybersecurity and privacy investment firm, NightDragon joins early strategic partner Prytek (who invested $110 million to date) as the co-lead investor in ThriveDX's current funding round.

Threatpost

PHP Everywhere Bugs Put 30K+ WordPress Sites at Risk of RCE

The plug-in's default settings spawned flaws that could allow for full site takeover but have since been fixed in an update that users should immediately install, Wordfence researchers said.

Threatpost

SAP Patches Severe 'ICMAD' Bugs

SAP's Patch Tuesday brought fixes for a trio of flaws in the ubiquitous ICM component in internet-exposed apps. One of them, with a risk score of 10, could allow attackers to hijack identities, steal data and more.

ZDNet | security RSS

Spanish police arrest suspects in SIM-swapping ring

Fraudsters used photocopies and stolen data to obtain duplicate SIM cards.

Security Affairs

Spyware, ransomware and Nation-state hacking: Q&A from a recent interview

I transcribed a recent interview, here some questions and answers about nation-state hacking, spyware, and cyber warfare. Enjoy" How has spyware changed the rules of cyber security in recent years? What will cyber security look like now that those tools are all over the internet? In the last decade, we have observed a progressive weaponization […] The post Spyware, ransomware and Nation-state hacking: Q&A from a recent interview appeared first on Security Affairs.

Security Affairs

Threat actors compromised +500 Magento-based e-stores with e-skimmers

Experts uncovered a mass Magecart campaign that compromised over 500 e-store running the Magento 1 eCommerce platform. Researchers from cybersecurity firm Sansec uncovered a massive Magecart campaign that already compromised more than 500 online stores running the Magento 1 eCommerce platform. Threat actors behind this campaign deployed a digital skimmer that was being loaded from the naturalfreshmall(.)com domain. […] The post Threat actors compromised +500 Magento-based e-stores with e-skimmers appeared first on Security Affairs.

Cyware News - Latest Cyber News

Vulnerabilities don't count

No one outside the IT department cares about the vulnerability metrics, or they shouldn't, anyway. They care more about the efficacy of the program. And traditional stats don't show that.

Twitter

AkkuS

[CVE-2022-22831 Unauth Admin Add, CVE-2022-22832 PrivEsc, CVE-2022-22833 MQTT Creds Dump] 3 different #0day s that I discovered on Servisnet were published. #Metasploit modules have been presented to you for the exploitation of vulns. Tech details =>

Prophaze Web Security Platform

iTunesRPC-Remastered os command injection [CVE-2022-23611] #Exploit:No #Local:No #Remote:Yes #Risk:Critical

ThreatMeter

CVE-2021-38172 perM 0.4.0 has a Buffer Overflow related to strncpy. (Debian initially fixed this in 0.4.0-7.) (CVSS:0.0) (Last Update:2022-02-05)

CVE

CVE-2022-24552 StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command.

CIRCL

StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command. - CVE-2022-24552

CVE.report

CVE-2022-22832 : An issue was discovered in Servisnet Tessa 0.0.2. Authorization data is available via an unauthenticated /data-service/users/ request....

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2022-24552 Description: StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a vi... CVSS: 9.24 #rebuild_project #rebuild #CVE #CyberSecurity #DataBreach

Prophaze Web Security Platform

iTunesRPC-Remastered path traversal [CVE-2022-23609] #Exploit:No #Local:No #Remote:Yes #Risk:Critical

Angenoire

#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2013-20004

ThreatMeter

CVE-2022-24552 StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command. (CVSS:0.0) (Last Update:2022-02-06)

RedPacket Security

Servisnet Tessa privilege escalaiton | CVE-2022-22832 -

CVE

CVE-2013-20004 StarWind iSCSI SAN before 6.0 build 2013-03-20 allows a memory leak.

Source: NIST

NIST CVE: Critical

CVE-2022-22831

An issue was discovered in Servisnet Tessa 0.0.2. An attacker can add a new sysadmin user via a manipulation of the Authorization HTTP header.

CRITICAL Vector: network Created: 2022-02-06 Updated: 2022-02-11

CVE-2022-23611

iTunesRPC-Remastered is a **Discord** Rich Presence for iTunes on **Windows** utility. In affected versions iTunesRPC-Remastered did not properly sanitize image file paths leading to OS level command injection. This issue has been patched in commit cdcd48b. Users are advised to upgrade.

CRITICAL Vector: network Created: 2022-02-04 Updated: 2022-02-11

CVE-2021-38172

perM 0.4.0 has a Buffer Overflow related to strncpy. (Debian initially fixed this in 0.4.0-7.)

CRITICAL Vector: network Created: 2022-02-05 Updated: 2022-02-11

CVE-2022-24552

StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command.

CRITICAL Vector: network Created: 2022-02-06 Updated: 2022-02-11

CVE-2022-22832

An issue was discovered in Servisnet Tessa 0.0.2. Authorization data is available via an unauthenticated /data-service/users/ request.

CRITICAL Vector: network Created: 2022-02-06 Updated: 2022-02-11

CVE-2022-23609

iTunesRPC-Remastered is a **Discord** Rich Presence for iTunes on **Windows** utility. In affected versions iTunesRPC-Remastered did not properly sanitize user input used to remove files leading to file deletion only limited by the process permissions. Users are advised to upgrade as soon as possible.

CRITICAL Vector: network Created: 2022-02-04 Updated: 2022-02-11

CVE-2013-20004

StarWind **iSCSI** SAN before 6.0 build 2013-03-20 allows a memory leak.

CRITICAL Vector: network Created: 2022-02-06 Updated: 2022-02-11

Source: NIST

NIST CVE: High

CVE-2022-23947

A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon DCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.

HIGH Vector: local Created: 2022-02-04 Updated: 2022-02-11

CVE-2021-39280

Certain **Korenix** JetWave devices allow authenticated users to execute arbitrary code as root via /syscmd.asp. This affects 2212X before 1.9.1, 2212S before 1.9.1, 2212G before 1.8, 3220 V3 before 1.5.1, 3420 V3 before 1.5.1, and 2311 through 2022-01-31.

HIGH Vector: network Created: 2022-02-06 Updated: 2022-02-11

CVE-2022-24113

Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: **Acronis Cyber Protect** 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home **Office** (Windows) before build 39612, Acronis **True Image** 2021 (Windows) before build 39287

HIGH Vector: local Created: 2022-02-04 Updated: 2022-02-11

CVE-2022-24551

StarWind SAN and NAS before 0.2 build 1685 allows users to reset other users' passwords.

HIGH Vector: network Created: 2022-02-06 Updated: 2022-02-11

CVE-2022-23946

A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon GCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.

HIGH Vector: local Created: 2022-02-04 Updated: 2022-02-11

CVE-2022-23206

In **Apache Traffic Control** Traffic Ops prior to 6.1.0 or 5.1.6, an unprivileged user who can reach Traffic Ops over HTTPS can send a specially-crafted POST request to /user/login/oauth to **scan** a port of a server that Traffic Ops can reach.

HIGH Vector: network Created: 2022-02-06 Updated: 2022-02-11

CVE-2007-20001

StarWind **iSCSI** SAN before 3.5 build 2007-08-09 allows **socket** exhaustion.

HIGH Vector: network Created: 2022-02-06 Updated: 2022-02-11

Source: NIST

NIST CVE: Medium

CVE-2022-0501

Cross-site Scripting (XSS) - Reflected in Packagist ptrofimov/beanstalk_console prior to 1.7.12.

CVE-2022-0502

Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.

MEDIUM Vector: network Created: 2022-02-05 Updated: 2022-02-11

CVE-2022-23600

fleet is an open source device management, built on **osquery**. Versions prior to 4.9.1 expose a limited ability to spoof SAML authentication with missing audience verification. This impacts deployments using SAML SSO in two specific cases: 1. A malicious or compromised **Service Provider** (SP) could reuse the SAML response to log into Fleet as a user -- only if the user has an account with the same email in Fleet, _and_ the user signs into the malicious SP via SAML SSO from the same **Identity Provider** (IdP) configured with Fleet. 2. A user with an account in Fleet could reuse a SAML response intended for another SP to log into Fleet. This is only a concern if the user is blocked from Fleet in the IdP, but continues to have an account in Fleet. If the user is blocked from the IdP entirely, this cannot be exploited. Fleet 4.9.1 resolves this issue. Users unable to upgrade should: Reduce the length of sessions on your IdP to reduce the window for malicious re-use, Limit the amount of SAML Service Providers/Applications used by user accounts with access to Fleet, and When removing access to Fleet in the IdP, delete the Fleet user from Fleet as well.

MEDIUM Vector: network Created: 2022-02-04 Updated: 2022-02-11

MEDIUM Vector: network Created: 2022-02-06 Updated: 2022-02-11

Source: NIST

NIST CVE: Low

CVE-2022-23605

Wire webapp is a **web client** for the wire messaging protocol. In versions prior to 2022-01-27-production.0 expired ephemeral messages were not reliably removed from local chat history of Wire Webapp. In versions before 2022-01-27-production.0 ephemeral messages and assets might still be accessible through the local search functionality. Any attempt to view one of these message in the chat view will then trigger the deletion. This issue only affects locally stored messages. On premise instances of **wire-webapp** need to be updated to 2022-01-27-production.0, so that their users are no longer affected. There are no known workarounds for this issue.

LOW Vector: local Created: 2022-02-04 Updated: 2022-02-11

Source: NIST

NIST CVE: Unrated

CVE-2022-23102

A vulnerability has been identified in SINEMA Remote **Connect** Server (All versions < V2.0). Affected products contain an open redirect vulnerability. An attacker could trick a valid authenticated user to the device into clicking a malicious link there by leading to phishing attacks.

UNRATED Vector: unkown Created: 2022-02-09 Updated: 2022-02-11

CVE-2022-23773

cmd/go in Go before 1.16.14 and 1.17.x before 1.17.7 can misinterpret branch names that falsely appear to be version tags. This can lead to incorrect access control if an actor is supposed to be able to create branches but not tags.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-24958

drivers/usb/gadget/legacy/inode.c in the **Linux** kernel through 5.16.8 mishandles dev->buf release.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-24955

Foxit PDF Reader before 11.2.1 and Foxit PDF Editor before 11.2.1 have an Uncontrolled Search Path Element for DLL files.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-0557

OS Command Injection in Packagist microweber/microweber prior to 1.2.11.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-24959

An issue was discovered in the **Linux** kernel before 5.16.5. There is a memory leak in yam_siocdevprivate in drivers/net/hamradio/yam.c.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-23806

Curve.IsOnCurve in crypto/elliptic in Go before 1.16.14 and 1.17.x before 1.17.7 can incorrectly return true in situations with a big.Int value that is not a valid field element.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-24954

Foxit PDF Reader before 11.2.1 and Foxit PDF Editor before 11.2.1 have a Stack-Based Buffer Overflow related to XFA, for the 'subform colSpan="-2"' and 'draw colSpan="1"' substrings.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-24961

In **Portainer** Agent before 2.11.1, an API server can continue running even if not associated with a Portainer instance in the past few days.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

CVE-2022-23772

Rat.SetString in math/big in Go before 1.16.14 and 1.17.x before 1.17.7 has an overflow that can lead to Uncontrolled Memory Consumption.

UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-11

Source: Hybrid Analysis

Top malicious files

100% Threat score	tmp7ph_1rvu
100% Threat score	Fly_Crypter_v2f (.) exe
100% Threat score	DHL DELIVERY DOCUMENTS (.) exe
100% Threat score	Firefox Setup 97 (.) 0 (.) x86 (.) exe
100% Threat score	locker (.) exe
91% Threat score	ISSVULHWACHLPTGHUNSEZBHITDJCYSVUKKGQHLSCPYQYLHSHFDDDKXHBOOLHYAHOOCFW (.) VBS
100% Threat score	Minecraft_Virus (.) vir
100% Threat score	setup (.) exe
100% Threat score	Firefox Setup 97 (.) 0 (.) x64 (.) exe
100% Threat score	locker (.) exe
100% Threat score	cerberusv4 (.) exe
85% Threat score	HD (.) Tune (.) Pro (.) v5 (.) 50 (.) exe

85%
Threat score

Primo (.) Ramdisk (.) Ult (.) Mui (.) Setup (.) 5 (.) 5 (.) 0 (.) exe

80%
Threat score

JotterPad_v13 (.) 0 (.) 11-pi_Mod_Apk4all (.) com (.) apk

79%
Threat score

malwy

75%
Threat score

ThesyconDriverInstaller64 (.) exe

Source: Hybrid Analysis

Top malicious URL

100%
Threat score

http://main-datings (.) top/

94%
Threat score

http://main-datings (.) top/

93%
Threat score

http://27 (.) 5 (.) 25 (.) 86:55228/Mozi (.) m

87%
Threat score

http://kaleidoscope (.) in/

78%
Threat score

http://api (.) obfuscatorjavascript (.) com/?getsrc=ok&ref&url=http%3A%2F%2Fwww (.) plaintiffthumb (.) legal%2Fzrtdfqvel%2Favvqsejb-s5xhc8lfsygbvw25ulzdfna45qevtdjqozbhjubwz9qxbeboa5m0hj5zjpscraft4rvkbzeumaaisvjfmex3hfpiq_terhalztan2o5ypqbgcwvxylssexq44jkrr3bzt2cricofou_o9fdi3jy4fi6cmidizxezrd (.) c99reqpl-lv5enkuavvfwiybj_3cikbsfx6lrmrxx_k

77%
Threat score

https://sitio (.) nu/

76%
Threat score

https://160928 (.) clicks (.) tstes (.) net/track/click?u=2804041&p=3136303932383a3138323a3138303a303a303a30&s=0afc0651b281491219f94dcaa0552a99&m=276789

72%
Threat score

http://instalacja-pendrive (.) pl/

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 France
- #7 Singapore
- #8 United Kingdom
- #9 India
- #10 Canada