Your Security Rabbits report for March 19, 2022

Source: Ransom Watch

Ransomware attacks

conti	Target: bChannels Ltd .	conti	Target: BDX
lockbit2	Target: denro . ca	lockbit2	Target: jewelry . org . hk
conti	Target: Normandeau Associates, Inc .	alphv	Target: vri . maniberia . net
midas	Target: 1	alphv	Target: unapen . internal
conti	Target: Talent Logic Inc .	lockbit2	Target: solvi . com
hiveleak	Target: NSM Insurance Group	conti	Target: NORDEX FOOD
lockbit2	Target: megaproductos . c . . .	lockbit2	Target: kbkbcpa . com/
lockbit2	Target: kbkbcpa . com	lockbit2	Target: genesis . ky
lockbit2	Target: dgordonlcswr . co . . .	lockbit2	Target: centralaccident . . .

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

1 Million Texans Potentially Impacted By Dental Care Data Breach

Jefferson Dental and Orthodontics, which has 72 offices across Texas, reported to the Texas Attorney General's Office a data breach affecting more than a million residents of Texas.

Threatpost

Agencies Warn on Satellite Hacks & GPS Jamming Affecting Airplanes, Critical Infrastructure

The Russian invasion of Ukraine has coincided with the jamming of airplane navigation systems and hacks on the SATCOM networks that empower critical infrastructure.

Security Affairs

Caketap, a new Unix rootkit used to siphon ATM banking data

Experts spotted a new Unix rootkit, called Caketap, that was used to steal ATM banking data. Mandiant researchers discovered a new Unix rootkit named Caketap, which is used to steal ATM banking data, while investigating the activity of the LightBasin cybercrime group (aka UNC1945). The China-linked hacking group

IT Security Guru

76,000 scams taken down through email reporting

The National Cyber Security Centres's (NCSC) Suspicious Email Reporting Service is proving successful. Over 10 million emails have been reported to the service, leading to 76,000 online scams being taken down. The service has been operating for almost two years, enabling members of the public to alert the authorities regarding potential cyberattacks and scams. Scams [...] The post 76,000 scams taken down through email reporting appeared first on IT Security Guru.

CyberScoop

Australia launches program to curb stalkerware

The initial program will help 30,000 survivors. The post Australia launches program to curb stalkerware appeared first on CyberScoop.

Security Affairs

China-linked threat actors are targeting the government of Ukraine

Google's TAG team revealed that China-linked APT groups are targeting Ukraine 's government for intelligence purposes. Google's Threat Analysis Group (TAG) researchers uncovered cyberespionage operations conducted by the Chinese People's Liberation Army (PLA) and other China-linked APT groups and that targeted Ukraine 's government to gather info on the has been active since at least 2016, according […] The post Caketap, a new Unix rootkit used to siphon ATM banking data appeared first on Security Affairs.

CyberScoop

CISA, FBI tell satellite communications network owners to watch out for hacks after Ukraine attack

A Ukrainian official said an attack on Viasat Inc.'s KA-SAT satellite led to diminished communications leading up to the Russian invasion. The post CISA, FBI tell satellite communications network owners to watch out for hacks after Ukraine attack appeared first on CyberScoop.

Cyware News - Latest Cyber News

Cyber Attackers Tap Cloud Native Technologies in Russia-Ukraine War

Researchers at Aqua revealed trends by analyzing data from public repositories that contain code and tools used for the cyber-aggression on both sides of the Russia-Ukraine conflict.

WeLiveSecurity

Defending the data center: The time to act is now

Cyberattacks against data centers may ultimately be everyone's problem - how prepared are their operators for the heightened risk of cyber-assaults? The post Defending the data center: The time to act is now appeared first on WeLiveSecurity

ZDNet | security RSS

Franchises, partnerships emerge in Ransomware-as-a-Service operations

Researchers detail the movers and shakers in the space over 2021.

Cyware News - Latest Cyber News

Google: Chinese state hackers target Ukraine's government

Google's Threat Analysis Group (TAG) says the Chinese People's Liberation Army (PLA) and other Chinese intelligence agencies are trying to get more info on the ongoing Russian war in Ukraine.

The Hacker News

Hackers Target Bank Networks with new Rootkit to Steal Money from ATM Machines

A financially motivated threat actor has been observed deploying a previously unknown rootkit targeting Oracle Solaris systems with the goal of compromising Automatic Teller Machine (ATM) switching networks and carrying out unauthorized cash withdrawals at different banks using fraudulent cards. Threat intelligence and incident response firm Mandiant is tracking the cluster under the moniker

Cyware News - Latest Cyber News

Microsoft: Here's how this notorious botnet used hacked routers for stealthy communication

Microsoft has filled in one new detail about how the TrickBot gang's IoT C2 devices, namely compromised MikroTik routers, were being used since 2018 for stealthy communication with infected PCs.

OpenSSL patches infinite-loop DoS bug in certificate verification

When it comes to writing loops in your code... never sit

ongoing conflict. Below is the tweet […] The post China-linked threat actors are targeting the government of Ukraine appeared first on Security Affairs.

Cyware News - Latest Cyber News

CISA, FBI warn US critical organizations of threats to SATCOM networks

CISA and the FBI have issued a warning highlighting their intelligence on "possible threats" to satellite communication (SATCOM) networks in the United States and worldwide.

Threatpost

DarkHotel APT Targets Wynn, Macao Hotels to Rip Off Guest Data

A DarkHotel phishing campaign breached luxe hotel networks, including Wynn Palace and the Grand Coloane Resort in Macao, a new report says.

The Hacker News

Experts Find Some Affiliates of BlackMatter Now Spreading BlackCat Ransomware

An analysis of two ransomware attacks has identified overlaps in the tactics, techniques, and procedures (TTPs) between BlackCat and BlackMatter, indicating a strong connection between the two groups. While it's typical of ransomware groups to rebrand their operations in response to increased visibility into their attacks, BlackCat (aka Alphv) marks a new frontier in that the cyber crime cartel

Threatpost

Google Blows Lid Off Conti, Diavol Ransomware Access-Broker Ops

Researchers have exposed the work of Exotic Lily, a full-time cybercriminal initial-access group that uses phishing to infiltrate organizations' networks for further malicious activity.

Cyware News - Latest Cyber News

Hackers hit mass background-check firm used by state agencies, universities

Computer hackers made off with highly sensitive personal records on more than 164,000 job-seekers and license applicants in a virtual "smash and grab" attack last November on Creative Services Inc., a company that conducts background checks.

Cyware News - Latest Cyber News

Japan's Bridgestone confirms ransomware attack at US subsidiary

Japanese tyre manufacturer Bridgestone has confirmed that its US subsidiary had suffered a ransomware attack, just weeks after suppliers of automaker Toyota Motor reported similar attacks.

IT Security Guru

New "initial access broker" working with Conti gang

Google's Threat Analysis Group (TAG) has new initial access broker that it alleges is closely affiliated to a Russian cyber-crime gang infamous for its Conti and Diavol ransomware operations. The financially motivated threat actor, dubbed Exotic Lily, has been detected exploiting a recently patched critical flaw in the Microsoft Windows MSHTML platform (CVE-2021-40444). The exploit […] The post New "initial access broker" working with Conti gang appeared first on IT Security Guru.

Security Affairs

Red TIM Research (RTR) team discovers a bug on Ericsson Network Manager

TIM Red Team Research (RTR) researchers discovered a new flaw on Ericsson Network Manager, aka Ericsson flagship network product. TIM Red Team Research (RTR) team discovered a new vulnerability affecting Ericsson Network Manager, which is known as Ericsson

Naked Security

on the fence!

Security Affairs

[Russia-linked Cyclops Blink botnet targeting ASUS routers](#)

The recently discovered Cyclops Blink botnet, which is believed to be a replacement for the VPNFilter botnet, is now targeting the ASUS routers. The recently discovered Cyclops Blink botnet is now targeting the ASUS routers, reports Trend Micro researchers. The Cyclops Blink malware has been active since at least June 2019, it targets WatchGuard Firebox and other […] The post Russia-linked Cyclops Blink botnet targeting ASUS routers appeared first on Security Affairs.

Threatpost

[Sandworm APT Hunts for ASUS Routers with Cyclops Blink Botnet](#)

The Russian-speaking APT behind the NotPetya attacks and the Ukrainian power grid takedown could be setting up for additional sinister attacks, researchers said.

Cyware News - Latest Cyber News

[What the Newly Signed US Cyber-Incident Law Means for Security](#)

The new law requires critical infrastructure companies in the 16 industry sectors identified by the federal government to report to the CISA within 72 hours if they are experiencing a cyberattack and within 24 hours of making a ransomware payment.

flagship network product. Ericsson Network Manager and network OSS As mentioned, we're talking about an Ericsson flagship […] The post Red TIM Research (RTR) team discovers a bug on Ericsson Network Manager appeared first on Security Affairs.

Cyware News - Latest Cyber News

[Russian pipeline company Transneft hit by data leak](#)

The data leak came to notice after the leak hosting website Distributed Denial of Secrets published a link to 79GB of emails from the Omega Company, the research and development division of Transneft.

CyberScoop

[South Africa credit bureau breached, data reportedly held for $15M ransom](#)

South Africa tech news site ITWeb reported that a group calling itself N4aughtysecTU is taking responsibility. The post South Africa credit bureau breached, data reportedly held for $15M ransom appeared first on CyberScoop.

CyberScoop

[Zelenskyy deepfake crude, but still might be a harbinger of dangers ahead](#)

A deepfake video of Ukrainian President Volodymyr Zelenskyy was quickly removed from Meta's platform, but experts called it worrisome nonetheless. The post Zelenskyy deepfake crude, but still might be a harbinger of dangers ahead appeared first on CyberScoop.

Twitter

Rep. Val Demings

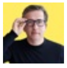
Last night we passed the federal budget to keep us SAFE. I voted to strengthen Americas military and provide strong resources for: - Securing our border - Homeland security grants that protect communities & houses of worship - Cybersecurity - Coast Guard and port security

Gary Gensler

Join us in now at our Investor Advisory Committee Meeting. Todays agenda includes a panel on artificial intelligence and robo-advising and a discussion on cybersecurity disclosures.

Dave Rubin

This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[…]



Spiros Margaris

The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

CVE-2022-26981

Liblouis through 3.21.0 has a buffer overflow in compilePassOpcode in compileTranslationTable.c (called, indirectly, by tools/lou_checktable.c).

HIGH	Vector: local	Created: 2022-03-13	Updated: 2022-03-19

CVE-2022-24128

Timescale TimescaleDB 1.x and 2.x before 2.5.2 may allow privilege escalation during extension installation. The installation process uses commands such as CREATE x IF NOT **EXIST** that allow an unprivileged user to precreate objects. These objects will be used by the installer (which executes as Superuser), leading

CVE-2022-24696

Mirametrix **Glance** before 5.1.1.42207 (released on 2018-08-30) allows a local attacker to elevate privileges. NOTE: this is unrelated to products from the glance.com and glance.net websites.

HIGH	Vector: local	Created: 2022-03-13	Updated: 2022-03-19

CVE-2022-24387

With administrator or admin privileges the application can be tricked into overwriting files to privilege escalation. In order to be able to take advantage of this, an unprivileged user would need to be able to create objects in a database and then get a Superuser to install TimescaleDB into their database. (In the fixed versions, the installation aborts when it finds that an object already exists.)

HIGH | Vector: network | Created: 2022-03-13 | Updated: 2022-03-19

in app_data/Config folder, e.g. the systemsettings.xml file. THis is possible in SmarterTrack **v100**.0.8019.14010

HIGH | Vector: network | Created: 2022-03-14 | Updated: 2022-03-19

Source: NIST

NIST CVE: Medium

CVE-2022-24385

A Direct Object Access vulnerability in **SmarterTools** SmarterTrack leads to information disclosure This issue affects: SmarterTools SmarterTrack 100.0.8019.14010.

MEDIUM | Vector: network | Created: 2022-03-14 | Updated: 2022-03-19

CVE-2022-24384

Cross-site Scripting (XSS) vulnerability in **SmarterTools** SmarterTrack This issue affects: SmarterTools SmarterTrack 100.0.8019.14010.

MEDIUM | Vector: network | Created: 2022-03-14 | Updated: 2022-03-19

CVE-2021-46709

phpLiteAdmin through 1.9.8.2 allows XSS via the index.php newRows parameter (aka num or number).

MEDIUM | Vector: network | Created: 2022-03-13 | Updated: 2022-03-19

CVE-2022-24386

Stored XSS in **SmarterTools** SmarterTrack This issue affects: SmarterTools SmarterTrack 100.0.8019.14010.

MEDIUM | Vector: network | Created: 2022-03-14 | Updated: 2022-03-19

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-27226

A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction.

UNRATED | Vector: unkown | Created: 2022-03-19 | Updated: 2022-03-19

CVE-2022-0991

Insufficient Session Expiration in **GitHub** repository admidio/admidio prior to 4.1.9.

UNRATED | Vector: unkown | Created: 2022-03-19 | Updated: 2022-03-19

Source: Hybrid Analysis

Top malicious files

100% Threat score	dnQjiyCcSvTbX	100% Threat score	v9 (.) exe
100% Threat score	FreeZIPPasswordCracker (.) exe	100% Threat score	ç”Ÿæˆå™¨ (.) exe
100% Threat score	Phasmophobia Trainer Setup (.) exe	98% Threat score	ARES (.) Updater (.) exe
96% Threat score	keygen (.) exe	78% Threat score	scenario

75% Threat score	domainname PayCopy[54205] (.) html

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://topadmin (.) topinteriors (.) co (.) in/tabler-dist/ga2l8Ioyrba/
93% Threat score	http://117 (.) 201 (.) 196 (.) 92:53828/Mozi (.) m
82% Threat score	http://marathiyt (.) com/
77% Threat score	http://kalden-sa (.) com/
72% Threat score	http://trk (.) e (.) loft (.) com/ss/c/QGeMhX6toQUbCOxfWLuswGWV73oqKLe7e4_D6PT6K-O-pooA-e57eHtYmpiViq-JKMWZ5puy0sjc37jkSK5y3w/3kg/60e7UspNR6679RsBjdi55Q/h55/7d6fWnoIpVHsTQHRwaP-KTyo91_VihxMvUw9E-VzkTc
97% Threat score	http://dreamlogicdigital (.) com/
93% Threat score	http://125 (.) 40 (.) 105 (.) 50:58108/Mozi (.) m
77% Threat score	https://www (.) jujutsukaisen0themovie (.) com/
72% Threat score	http://builtky (.) com/

Source: SpamHaus

Top spamming countries

- 🇺🇸 #1 United States of America
- 🇨🇳 #2 China
- 🇷🇺 #3 Russian Federation
- 🇲🇽 #4 Mexico
- 🇩🇴 #5 Dominican Republic
- 🇸🇦 #6 Saudi Arabia
- 🇮🇳 #7 India
- 🇧🇷 #8 Brazil
- 🇺🇾 #9 Uruguay
- 🇯🇵 #10 Japan

Source: SpamHaus

Top spammers

🇺🇦 #1 **Canadian Pharmacy**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.

🇺🇸 #2 **PredictLabs / Sphere Digital**
This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.

🇺🇸 #3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.

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

🇺🇸 #5 **RetroCubes**

🇺🇸 #6 **Cyber World Internet Services/ e-Insites**
Bulletproof spam host operating Cyber World Internet

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.

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 Algeria

#7 Viet Nam

#8 Brazil

#9 Iran (Islamic Republic of)

#10 Pakistan

Source: SpamHaus

Top phishing countries

#1 United States

#2 Russia

#3 Germany

#4 Singapore

#5 Netherlands

#6 India

#7 Australia

#8 Hong Kong

#9 France

#10 Japan

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- United States (27%)
- Russia (14%)
- Germany (11%)

Source: Imperva DDOS Map

Top DDOS country targets

- Russia (62%)
- Ukraine (18%)
- United States (8%)

Source: Imperva DDOS Map

Top DDOS techniques

81%	**DDoS**
13%	**Automated Threat**
6%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

65%	**Financial Services**
21%	**Business**
5%	**Computing & IT**