Your Security Rabbits report for March 16, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	Target: medinadairy . co . . . . (2022-03-16)	suncrypt	Target: Migros(2022-03-16)
lorenz	Target: Fuji America Corporation(2022-03-15)	midas	Target: Grcouceiro(2022-03-15)
everest	Target: Instituto Nacional de TecnologÃƒÂa Agropecuaria(2022-03-15)	lockbit2	Target: mfi(2022-03-15)
lorenz	Target: VadaTech(2022-03-15)	lorenz	Target: Ward Hadaway(2022-03-15)

Hot topics

Nothing today

News

Naked Security

"Russian actors bypass 2FA" warning - what happened and how to avoid it

Don't leave old accounts lying around where someone sketchy could reactivate them.

CISA Alerts

AA22-074A: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability

Multifactor Authentication (MFA): A Cybersecurity Essential * MFA is one of the most important cybersecurity practices to reduce the risk of intrusions--according to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised. * Every organization should enforce MFA for all employees and customers, and every user should sign up for MFA when available. * Organizations that implement MFA should review default configurations and modify as necessary, to reduce the likelihood that a sophisticated adversary can circumvent this control. The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency ([...]

Cyware News - Latest Cyber News

Anonymous cripples Russian Fed Security Service (FSB) & other top sites

The severity of the attack can be quantified by the fact that even after 18 hours have passed since the attack took place, all targeted websites were still unreachable and offline for visitors.

Cyware News - Latest Cyber News

Beware Gamers! Fake Valorant Cheat Spreads RedLine Stealer

Hackers are now abusing YouTube's new submission rules to disseminate malware. One such malware campaign has been found targeting a gaming community on YouTube, to spread RedLine stealer.

ZDNet | security RSS

CaddyWiper: More destructive wiper malware strikes Ukraine

The wiper avoids domain controllers to stay under the radar.

Security Affairs

CVE-2022-0778 DoS flaw in OpenSSL was fixed

OpenSSL addressed a high-severity denial-of-service (DoS) vulnerability, tracked as CVE-2022-0778, related to certificate parsing. OpenSSL released updates to address a high-severity denial-of-service (DoS) vulnerability, tracked as CVE-2022-0778, that affects the BN_mod_sqrt() function used when certificate parsing. The flaw was discovered by the popular Google Project Zero researchers Tavis Ormandy. An attacker can trigger the vulnerability by crafting [...] The post CVE-2022-0778 DoS flaw in OpenSSL was fixed appeared first on Security Affairs.

Security Affairs

Dirty Pipe Linux flaw impacts most QNAP NAS devices

Taiwanese vendor QNAP warns most of its NAS devices are impacted by high severity Linux vulnerability dubbed 'Dirty Pipe.' Taiwanese hardware vendor QNAP warns most of its Network Attached Storage (NAS) devices are impacted by the recently discovered Linux vulnerability 'Dirty Pipe.' An attacker with local access can exploit the high-severity vulnerability Dirty Pipe to [...] The post Dirty Pipe Linux flaw impacts most QNAP NAS devices appeared first on Security Affairs.

IT Security Guru

A lack of diversity in cybersecurity puts organisations at risk

One week later and International Women's Day is still fresh in our minds. There is still some way to go but every day that we challenge the stigma and bias that impact women in the workplace. Obrela Security Industries have launched a campaign to celebrate women in the cybersecurity industry. You can read their blog [...] The post A lack of diversity in cybersecurity puts organisations at risk appeared first on IT Security Guru.

IT Security Guru

Almost 300k cardiac patients have data exposed

A cyber attack on South Denver Cardiology Associates (SDCA) may have exposed the protected healthcare information (PHI) of thousands of cardiac patients. The healthcare provider issued a notice to its patients, disclosing that its network had been breached in January 2022. The perpetrator(s) are as yet unknown, gaining access to files containing information on 287,652 patients during [...] The post Almost 300k cardiac patients have data exposed appeared first on IT Security Guru.

Naked Security

Apple patches 87 security holes - from iPhones and Macs to Windows

Lots of fixes, with data leakage flaws and code execution bugs patched on iPhones, Macs and even Windows.

The Hacker News

Build Your 2022 Cybersecurity Plan With This Free PPT Template

The end of the year is coming, and it's time for security decision-makers to make plans for 2022 and get management approval. Typically, this entails making a solid case regarding why current resources, while yielding significant value, need to be reallocated and enhanced. The Definitive 2022 Security Plan PPT Template is built to simplify this task, providing security decision-makers with an

Security Affairs

Critical flaws affect Veeam Data Backup software

Veeam addressed two critical vulnerabilities impacting the Backup & Replication product for virtual environments. Veeam has released security patches to fix two critical vulnerabilities, tracked as CVE-2022-26500 and CVE-2022-26501 (CVSS score of 9.8), impacting the Backup & Replication solution for virtual environments. The solution implements data backup and restore capabilities for virtual machines running on [...] The post Critical flaws affect Veeam Data Backup software appeared first on Security Affairs.

Threatpost

Cyberattacks Against Israeli Government Sites: 'Largest in the Country's History'

DDoS attacks against Israel telecom companies took down government sites, sparking a temporary state of emergency.

The Hacker News

Facebook Hit With $18.6 Million GDPR Fine Over 12 Data Breaches in 2018

The Irish Data Protection Commission (DPC) on Tuesday slapped Facebook and WhatsApp owner Meta Platforms a fine of EUR17 million (~$18.6 million) for a series of security lapses that occurred in violation of the European Union's GDPR laws in the region. "The DPC found that Meta Platforms failed to have in place appropriate technical and organizational measures which would enable it to readily

CyberScoop

FCC rules requiring foreign governments to disclose broadcast time take effect

FCC Commissioner Jessica Rosenworcel said new rules requiring foreign governments to disclose when they lease broadcast time in the U.S. will increase transparency. The post FCC rules requiring foreign governments to disclose broadcast time take effect appeared first on CyberScoop.

CyberScoop

German government issues warning about Kaspersky products

The Federal Office for Information Security, or BSI, did not accuse Kaspersky of any specific violations of customers' trust. The post German government issues warning about Kaspersky products appeared first on CyberScoop.

Security Affairs

Hacker breaches key Russian ministry in blink of an eye

In mere seconds, a hacker remotely accessed a computer belonging to a regional Russian Ministry of Health, taking advantage of sloppy cybersecurity practices to expose its entire network. Original post at https://cybernews.com/cyber-war/hacker-breaches-key-russian-ministry-in-blink-of-an-eye/ Spielerkid89, who wished to remain anonymous, did not intend to harm the organization and left its systems intact. However, his experiment is a [...] The post Hacker breaches key Russian ministry in blink of an eye appeared first on Security Affairs.

CyberScoop

Ireland slaps Facebook with $19M fine over 2018 data breaches

The complaint refers to the company's handling of 12 data breaches that occurred in 2018. The post Ireland slaps Facebook with $19M fine over 2018 data breaches appeared first on CyberScoop.

Cyware News - Latest Cyber News

Lampion Trojan Returns with its Old Attack Infrastructure

One of the most active banking trojans has been spotted tweaking its technique but using the same old infrastructure to target its victims in banking the sector. The attackers use fake banking templates impersonating Portuguese organizations to bait victims. Organizations are recommended to make use of provided IOCs for better detection of such threats.

Cyware News - Latest Cyber News

Malicious web application requests skyrocketing, bad actors stealthier than ever before

Between 2020 and 2021, the number of malicious web application requests climbed 88%, more than double the year-over-year growth rate in distributed denial-of-service (DDoS) attacks, which were up 37% over 2020.

Cyware News - Latest Cyber News

MuddyWater Uses SloughRAT To Target Turkey and Arabian Peninsula

Iranian MuddyWater APT launched a new series of attacks targeting Turkey and the Arabian Peninsula. The recent intrusions appear to be a continuation of a November 2021 campaign targeting Turkish entities. Its malicious activities shows group's peaked interest in the region and geopolitics.

The Hacker News

Nearly 34 Ransomware Variants Observed in Hundreds of Cyberattacks in Q4 2021

As many as 722 ransomware attacks were observed during the fourth quarter of 2021, with LockBit 2.0, Conti, PYSA, Hive, and Grief emerging as the most prevalent strains, according to new research published by Intel 471. The attacks mark an increase of 110 and 129 attacks from the third and second quarters of 2021, respectively. In all, 34 different ransomware variants were detected during the

Threatpost

Pandora Ransomware Hits Giant Automotive Supplier Denso

Denso confirmed that cybercriminals leaked stolen, classified information from the Japan-based car-components manufacturer after an attack on one of its offices in Germany.

Cyware News - Latest Cyber News

Prison service for England and Wales recorded more than 2,000 data breaches over 12 months

The organization's sensitive personal data was apparently exposed because of unauthorized access gained to the Justice Academy, an online learning and careers platform used by MoJ and other public sector staff.

Cyware News - Latest Cyber News

SentinelOne to Acquire Attivo Networks, Bringing Identity to XDR

Under the terms of the agreement, SentinelOne will acquire Attivo Networks in a cash and stock transaction valued at $616.5 million. The acquisition is expected to close in SentinelOne's upcoming fiscal second quarter.

CyberScoop

Top Ukrainian cyber official praises volunteer hacks on Russian targets, offers updates

Ukraine's Victor Zhora said the so-called IT Army has done "useful" things, and he offered information about the "CaddyWiper" incident. The post Top Ukrainian cyber official praises volunteer hacks on Russian targets, offers updates appeared first on CyberScoop.

CyberScoop

FTC settlement requires CafePress owners to pay $500,000 to victims of 2019 data breach

The commission accused the company of covering up the hack. The post FTC settlement requires CafePress owners to pay $500,000 to victims of 2019 data breach appeared first on CyberScoop.

The Hacker News

German Government Warns Against Using Russia's Kaspersky Antivirus Software

Russian cybersecurity firm Kaspersky on Tuesday responded to an advisory released by Germany's Federal Office of Information Security (BSI) against using the company's security solutions in the country over "doubts about the reliability of the manufacturer." Calling that the decision was made on "political grounds," the company said it will "continue to assure our partners and customers of the

ZDNet | security RSS

How cloud services become weapons in Russia-Ukraine cyber conflict

DDoS tools and how-to guides are being spread through cloud technologies.

Cyware News - Latest Cyber News

Kronos ransomware attack raises questions of vendor liability

The December ransomware attack against workforce management company Ultimate Kronos Group hindered the ability of its customers to process payrolls. The attack, which has far-reaching ramifications, has stakeholders looking for who is to blame.

Krebs on Security

Lawmakers Probe Early Release of Top RU Cybercrook

Aleksei Burkov, a cybercriminal who long operated two of Russia's most exclusive underground hacking forums, was arrested in 2015 by Israeli authorities. The Russian government fought Burkov's extradition to the U.S. for four years -- even arresting and jailing an Israeli woman to force a prisoner swap. That effort failed: Burkov was sent to America, pleaded guilty, and was sentenced to nine years in prison. But a little more than a year later, he was quietly released and deported back to Russia. Now some Republican lawmakers are asking why a Russian hacker once described as "an asset of supreme importance" was allowed to shorten his stay.

Threatpost

Most QNAP NAS Devices Affected by 'Dirty Pipe' Linux Flaw

The "Dirty Pipe" Linux kernel flaw - a high-severity vulnerability in all major distros that grants root access to unprivileged users who have local access - affects most of QNAP's network-attached storage (NAS) appliances, the Taiwanese manufacturer warned on Monday. Dirty Pipe, a recently reported local privilege-escalation vulnerability, affects the Linux kernel on QNAP NAS [...]

The Hacker News

Multiple Flaws Uncovered in ClickHouse OLAP Database System for Big Data

Researchers have disclosed seven new security vulnerabilities in an open-source database management system solution called ClickHouse that could be weaponized to crash the servers, leak memory contents, and even lead to the execution of arbitrary code. "The vulnerabilities require authentication, but can be triggered by any user with read permissions," Uriya Yavnieli and Or Peles, researchers

Cyware News - Latest Cyber News

New B1txor20 Linux Backdoor Threat Uses DNS Tunnel

B1txor20 uses DNS Tunnel to establish C2 channel, support direct connection and relay, while using ZLIB compression, RC4 encryption, BASE64 encoding to protect the traffic of the backdoor.

Threatpost

Phony Instagram 'Support Staff' Emails Hit Insurance Company

The phishing scam tried to steal login credentials by threatening account shutdown, due to users having purportedly shared "fake content."

Cyware News - Latest Cyber News

Raccoon Stealer Using Telegram for Hidden Communications

The credential-stealing Raccoon Stealer is spotted using the chat app to store and update C2 addresses as adversaries find creative new ways to distribute the malware. The cybercriminals are attempting to evade detection by packing the credential stealer, using Themida or malware packers. Experts think that the developers of this malware will continue to add new features to it to make it efficient.

Security Affairs

The German BSI agency recommends replacing Kaspersky antivirus software

German Federal Office for Information Security agency, also known as BSI, recommends consumers not to use Kaspersky anti-virus software. The German Federal Office for Information Security agency, aka BSI, recommends consumers uninstall Kaspersky anti-virus software. The Agency warns the cybersecurity firm could be implicated in hacking attacks during the ongoing Russian invasion of Ukraine. According [...] The post The German BSI agency recommends replacing Kaspersky antivirus software appeared first on Security Affairs.

Cyware News - Latest Cyber News

Update: Thousands of Secret Keys Found in Leaked Samsung Source Code

An analysis of the recently leaked Samsung source code revealed that thousands of secret keys have been exposed, including many that could be highly useful to malicious actors.

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

CVE-2022-25818

Improper boundary check in UWB stack prior to SMR Mar-2022 Release 1 allows arbitrary code execution.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-16

CVE-2021-42786

It was discovered that the **SteelCentral AppInternals** Dynamic Sampling Agent (DSA) has Remote Code Execution vulnerabilities in multiple instances of the API requests. The affected endpoints do not have any input validation of the user's input that allowed a malicious payload to be injected.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-16

Source: NIST

NIST CVE: High

CVE-2022-24512

.NET and Visual **Studio** Remote Code Execution Vulnerability.

HIGH Vector: network Created: 2022-03-09 Updated: 2022-03-16

CVE-2022-24506

Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24469, CVE-2022-24515, CVE-2022-24518, CVE-2022-24519.

HIGH Vector: network Created: 2022-03-09 Updated: 2022-03-16

CVE-2022-24510

Microsoft Office Visio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24461, CVE-2022-24509.

HIGH Vector: local Created: 2022-03-09 Updated: 2022-03-16

CVE-2022-25225

Network Olympus version 1.8.0 allows an authenticated admin user to inject SQL queries in '/api/eventinstance' via the 'sqlparameter' JSON parameter. It is also possible to achieve remote code execution in the default installation (PostgreSQL) by exploiting this issue.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-25814

PendingIntent hijacking vulnerability in Wearable Manager Installer prior to SMR Mar-2022 Release 1 allows local attackers to perform unauthorized **action** without permission via hijacking the PendingIntent.

HIGH Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-24505

Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23283, CVE-2022-23287.

HIGH Vector: local Created: 2022-03-09 Updated: 2022-03-16

CVE-2022-24508

Windows SMBv3 Client/Server Remote Code Execution Vulnerability.

HIGH Vector: network Created: 2022-03-09 Updated: 2022-03-16

CVE-2021-32025

An elevation of privilege vulnerability in the QNX Neutrino Kernel of affected versions of **QNX Software Development Platform** version(s) 6.4.0 to 7.0, **QNX Momentics** all 6.3.x versions, QNX OS for **Safety** versions 1.0.0 to 1.0.2, QNX OS for Safety versions 2.0.0 to 2.0.1, QNX for Medical versions 1.0.0 to 1.1.1, and QNX OS for Medical version 2.0.0 could allow an attacker to potentially access data, modify behavior, or permanently crash the system.

HIGH Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-25821

Improper use of SMS buffer pointer in Shannon baseband prior to SMR Mar-2022 Release 1 allows OOB read.

HIGH Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-24509

Microsoft Office Visio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24461, CVE-2022-24510.

HIGH Vector: local Created: 2022-03-09 Updated: 2022-03-16

CVE-2021-40376

otris **Update Manager** 1.2.1.0 allows local users to achieve SYSTEM access via unauthenticated calls to exposed interfaces over a **.NET** named pipe. A remote attack may be possible as well, by leveraging WsHTTPBinding for HTTP traffic on TCP port 9000.

HIGH Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-25815

PendingIntent hijacking vulnerability in Weather application prior to SMR Mar-2022 Release 1 allows local attackers to perform unauthorized **action** without permission via hijacking the PendingIntent.

HIGH Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-24507

Windows Ancillary Function Driver for **WinSock** Elevation of Privilege Vulnerability.

HIGH Vector: local Created: 2022-03-09 Updated: 2022-03-16

Source: NIST

NIST CVE: Medium

CVE-2022-25820

A vulnerable design in fingerprint matching algorithm prior to SMR Mar-2022 Release 1 allows physical attackers to perform brute force attack on **screen lock** password.

MEDIUM Vector: physical Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-25816

Improper authentication in **Samsung Lock** and mask apps setting prior to SMR Mar-2022 Release 1 allows attacker to change enable/disable without authentication

MEDIUM Vector: physical Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-25819

OOB read vulnerability in hdcp2 device node prior to SMR Mar-2022 Release 1 allow an attacker to view Kernel stack memory.

MEDIUM Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-25822

An use after free vulnerability in sdp driver prior to SMR Mar-2022 Release 1 allows kernel crash.

MEDIUM Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-24511

Microsoft Office Word Tampering Vulnerability.

MEDIUM Vector: local Created: 2022-03-09 Updated: 2022-03-16

CVE-2022-24503

Remote Desktop Protocol Client Information Disclosure Vulnerability.

MEDIUM Vector: network Created: 2022-03-09 Updated: 2022-03-16

CVE-2021-41657

SmartBear CodeCollaborator v6.1.6102 was discovered to contain a vulnerability in the web UI which would allow an attacker to conduct a clickjacking attack.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-16

CVE-2021-32006

This issue affects: **Secomea** GateManager Version 9.6.621421014 and all prior versions. Permission Issues vulnerability in LinkManager web portal of Secomea GateManager allows logged in LinkManager user to access stored **SiteManager backup** files.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-25368

Spectre BHB is a variant of Spectre-v2 in which malicious code uses the shared branch history (stored in the CPU BHB) to influence mispredicted branches in the victim's hardware context. Speculation caused by these mispredicted branches can then potentially be used to cause cache allocation, which can then be used to infer information that should be protected.

MEDIUM Vector: local Created: 2022-03-10 Updated: 2022-03-16

CVE-2022-24502

Windows HTML Platforms Security Feature Bypass Vulnerability.

MEDIUM Vector: network Created: 2022-03-09 Updated: 2022-03-16

Source: NIST

NIST CVE: Low

CVE-2022-25817

Improper authentication in **One UI** Home prior to SMR Mar-2022 Release 1 allows attacker to generate pinned-shortcut without user consent.

LOW Vector: local Created: 2022-03-10 Updated: 2022-03-16

Source: NIST

NIST CVE: Unrated

CVE-2021-43957

Affected versions of **Atlassian Fisheye** & **Crucible** allowed remote attackers to browse local files via an Insecure Direct Object References (IDOR) vulnerability in the WEB-INF directory and bypass the fix for CVE-2020-29446 due to a lack of url decoding. The affected versions are before version 4.8.9.

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

CVE-2022-27225

Gradle Enterprise before 2021.4.3 relies on cleartext data **transmission** in some situations. It uses **Keycloak** for **identity management** services. During the sign-in process, Keycloak sets browser cookies that effectively provide remember-me functionality. For backwards compatibility with older **Safari** versions, Keycloak sets a duplicate of the cookie without the Secure attribute, which allows the cookie to be sent when accessing the location that cookie is set for via HTTP. This creates the potential for an attacker (with the ability to impersonate the Gradle Enterprise host) to capture the login session of a user by having them click an http:// link to the server, despite the real server requiring HTTPS.

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

CVE-2020-36519

Mimecast **Email Security** before 2020-01-10 allows any admin to spoof any domain, and pass DMARC alignment via SPF. This occurs through misuse of the address rewrite feature. (The domain being spoofed must be a customer in the Mimecast **grid** from which the spoofing occurs.)

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

CVE-2021-43956

The **jQuery** deserialize library in **Fisheye** and **Crucible** before version 4.8.9 allowed remote attackers to to inject arbitrary HTML and/or JavaScript via a prototype pollution vulnerability.

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

CVE-2022-0911

Cross-site Scripting (XSS) - Stored in **GitHub** repository pimcore/pimcore prior to 10.4.0.

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

CVE-2022-27223

In drivers/usb/gadget/udc/udc-xilinx.c in the **Linux** kernel before 5.16.12, the endpoint index is not validated and might be manipulated by the host for out-of-array access.

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

CVE-2021-43955

The /rest-service-fecru/server-v1 resource in **Fisheye** and **Crucible** before version 4.8.9 allowed authenticated remote attackers to obtain information about installation directories via information disclosure vulnerability.

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

CVE-2021-43958

Various rest **resources** in **Fisheye** and **Crucible** before version 4.8.9 allowed remote attackers to brute force user login credentials as rest resources did not check if users were beyond their max failed login limits and therefore required solving a **CAPTCHA** in addition to providing user credentials for authentication via a improper restriction of excess authentication attempts vulnerability.

UNRATED Vector: unkown Created: 2022-03-16 Updated: 2022-03-16

Source: Hybrid Analysis

Top malicious files

100% Threat score	enmta (.) xlsb
100% Threat score	stsbtimrueipo (.) xlsb
100% Threat score	form (.) xlsm
100% Threat score	LPo
100% Threat score	RFQ (.) exe
100% Threat score	Dark Souls FOV Fix v1 (.) 0-1063-1-0 (.) exe
100% Threat score	robloxhack_protected (.) exe
100% Threat score	2022-03-16_1716 (.) xlsm
100% Threat score	Electronic form (.) xlsm
100% Threat score	ignit (.) vbs
100% Threat score	tseumapomcvuludti (.) xlsb
100% Threat score	636VZ-1182135970 (.) xlsm
100% Threat score	sp55548 (.) exe
100% Threat score	AntiPublic_Cracked & Fixed (.) exe
100% Threat score	file (.) htm
100% Threat score	456 (.) xlsm

Threat score	
100% Threat score	51742d7e916aa7b4a0ba1ac6ec286e1ecbf71b0e3690fc40a2274f6f3925e12f (.) dll
100% Threat score	Mail_95207 (.) xlsm
100% Threat score	INV_16-03-2022_0070009404825 (.) exe
97% Threat score	Runtime (.) exe
93% Threat score	6Um2UUl7RHHi8UUp7 (.) dll
93% Threat score	9dc79fe03de3d5402aeeff0c2a0da5fdef4cc2220edf05beddc58cfab54a345f
85% Threat score	FastHelpTrialSetup (.) exe
75% Threat score	BrowserCrashFix (.) exe
75% Threat score	VisualStudioSetup (.) exe
73% Threat score	X-0684 (.) xlsm
72% Threat score	Lock-New folder-XP-32bit (.) exe

Source: *Hybrid Analysis*

Top malicious URL

Threat score	
100% Threat score	https://aspotlessreputation (.) com/closing
99% Threat score	http://h (.) lookmind (.) net/
97% Threat score	http://103 (.) 120 (.) 135 (.) 100:36521/Mozi (.) m
93% Threat score	http://125 (.) 41 (.) 205 (.) 253:59861/bin (.) sh
88% Threat score	http://117 (.) 198 (.) 255 (.) 147:59453/Mozi (.) m
82% Threat score	http://maduras (.) top/tag/zoofilia-animal/
82% Threat score	http://url2691 (.) carpetcleaning (.) hk/ls/click?upn=b68d7HScTZY-2BTR8Dx2rOi9zEFxl-2BOTpCBu1hx7Mz74hnFd3FNX9-2BqNZ6KVkuyCp12ZhgcrUpOxYW7vY7IIEgoQ-3D-3DLQoj_CvWZ0IqD2jxSsZiuFRdV-2F6STUmlziqeb2sfwzIlCxnYP0S6jWo1oVImQyHeemZM07N1gqEji2rEXi43xf0dB47EkNbtiCKum-2BBxs284e5HxoQCtXa6tZUn96BJ5Ap1O3HnATkWouNEIAzkFu5V3YVTN6KTKT2P0XYBNGnKL1BFPGf3jX2S9tm2chic2zScEE7LVIgK-2FApvlgEOfocjOnwoziOU0ZC4BgtsFvlHJpiSU-3D
77% Threat score	http://www (.) goodtoshop (.) net/
77% Threat score	https://protect2 (.) fireeye (.) com/v1/url?k=d76bc3a0-b771bb2d-d7690ea2-ac1f6bdccb7c-b6acbcffc807bdce&q=1&e=3620e89c-d86d-41f2-9919-61e4c2a25bf8&u=http%3A%2F%2Fsendy (.) walaplus (.) com%2Fl%2FX3bgWFtbNzsdgxRrTqYzbw%2FcYiHhKHhqmOw70n7ViuQxA%2FPEtUv61qjalzinnZXKrmJQ
77% Threat score	http://new (.) clearoffers (.) eu/?utm_medium=e5072aecd585f8623f5e50299fb427d03812f7dd&utm_campaign=main&1=510&2=382&cid=Avd4xu0AAAF_jgiXVwAABG0AAAF-AAAAAA
72% Threat score	http://em (.) featuredit (.) com/c/1RSCNgv9hF9YJXa4RJzsjgbh
100% Threat score	http://www (.) polarrou (.) com/
99% Threat score	http://rushhourapplian (.) com/modern-maid-appliance-repair/
95% Threat score	http://59 (.) 93 (.) 30 (.) 205:47399/Mozi (.) m
93% Threat score	http://123 (.) 7 (.) 43 (.) 138:37709/Mozi (.) m
83% Threat score	http://117 (.) 214 (.) 20 (.) 136:54433/i
82% Threat score	http://www (.) xmovies (.) top/mulligans-2008/
77% Threat score	http://tredirectaserbi (shop/lqdim/
77% Threat score	http://safe-portal (.) fra (.) digitaloceanspaces (com/
77% Threat score	https://worldradiomap com/
75% Threat score	http://chuiadyallprows (.) shop/

Source: *SpamHaus*

Top spamming countries

#1 United States of America	#2 China
#3 Russian Federation	#4 Mexico
#5 Dominican Republic	#6 Saudi Arabia
#7 India	#8 Brazil
#9 Japan	#10 Uruguay

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 Thailand

#5 Indonesia

#6 Algeria

#7 Viet Nam

#8 Brazil

#9 Iran (Islamic Republic of)

#10 Japan

Source: SpamHaus

Top phishing countries

#1 United States

#2 Russia

#3 Germany

#4 Netherlands

#5 Singapore

#6 Japan

#7 Hong Kong

#8 France

#9 India

#10 Indonesia

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

Source: Imperva DDOS Map

Top DDOS country targets

Source: Imperva DDOS Map

Top DDOS techniques

Source: Imperva DDOS Map

Top DDOS industry targets