Your Security Rabbits report for February 26, 2022

Hot topics

Nothing today

News

IT Security Guru

1 in 6 Enterprise Endpoints exposed to identity risks

Yesterday, Illusive released its Analysing Identity Risks (AIR) 2022 report, which examines the unmanaged, misconfigured and exposed identity risks within organisations. The report shows that all organisations are vulnerable to attack, despite the deployment of privileged account management (PAM), multi-factor authentication (MFA) and other identity and access management (IAM) solutions. Illusive's security teams witnessed these [...] The post 1 in 6 Enterprise Endpoints exposed to identity risks appeared first on IT Security Guru.

Threatpost

6 Cyber-Defense Steps to Take Now to Protect Your Company

Ransomware is getting worse, but Daniel Spicer, chief security officer at Ivanti, offers a checklist for choosing defense solutions to meet the challenge.

Security Affairs

Anonymous launched its offensive on Russia in response to the invasion of Ukraine

The popular collective Anonymous declared war on Russia for the illegitimate invasion of Ukraine and announced a series of cyber attacks calling to action its members The Anonymous collective is calling to action against Russia following the illegitimate invasion of Ukraine. The famous groups of hackivists is also calling for action Russian citizens inviting them [...] The post Anonymous launched its offensive on Russia in response to the invasion of Ukraine appeared first on Security Affairs.

IT Security Guru

Biden considers "massive" cyber attack on Russia

An NBC News report suggests that the US could be preparing for its most significant cyber offensive campaign in recent memory as Biden considers his options for action against Russia. The report cites two US intelligence officials, one Western intelligence official and an unnamed person, claiming that a "menu" of options have been placed in [...] The post Biden considers "massive" cyber attack on Russia appeared first on IT Security Guru.

IT Security Guru

Cato Networks experiences near 100% revenue growth for second year in a row

Cato Networks has recently reported its 2021 business results, showing a growing revenue by 96% YoY, increasing headcount by 66%, and a doubling in valuation to $2.5 billion with an added $200 million investment. In a new Total Economic Impact (TEI) study, Forrester Research found that Cato delivers 246% ROI in under six months. Along with performance improvements,

CyberScoop

Conti ransomware group announces support of Russia, threatens retaliatory attacks

An infamous ransomware group with potential ties to Russian intelligence and known for attacking health care providers and hundreds of other targets posted a warning Friday saying it was "officially announcing a full support of Russian government." The gang said that it would use "all possible resources to strike back at the critical infrastructures" of any entity that organizes a cyberattack "or any war activities against Russia." The message appeared

increased [...] The post Cato Networks experiences near 100% revenue growth for second year in a row appeared first on IT Security Guru.

Friday on the dark-web site used by ransomware group Conti to post threats and its victims' data. Security researchers believe the gang to be Russia-based. Conti ransomware was part of more than 400 attacks against mostly U.S. targets between [...]

Cyware News - Latest Cyber News

Data Breach Impacts DNA Data of Sexual Assault Victims Reported to Oklahoma City Police Department

The laboratory processed the DNA evidence from rape victims, known as 'rape kits', for the Oklahoma City Police Department (OKCPD), amongst other clients, over a two-year period.

Naked Security

Did we learn nothing from Y2K? Why are some coders still stuck on two digit numbers?

Calling all website coders: Y2K was then. V1H is now!

CyberScoop

In studying tech supply chain, feds cite open source products, device firmware

Open-source software and device firmware are two of the biggest areas of vulnerability in the supply chains for information and communications technology, according to a federal report Thursday that called for better risk management practices and improved monitoring efforts by government and industry. Another area that potentially affects U.S. cybersecurity is a shrinking manufacturing base for hardware, including a "significant reduction" in the related workforce, the report said. The Biden administration asked the departments of Commerce and Homeland Security for the review under an executive order signed in February 2021 as the White House worked to address challenges in the supply chains[...]

Cyware News - Latest Cyber News

GE SCADA Product Vulnerabilities Show Importance of Secure Configurations

GE Digital has released patches for two high-severity vulnerabilities affecting its Proficy CIMPLICITY HMI/SCADA software, which is used by plants globally to monitor and control operations.

Cyware News - Latest Cyber News

India's Personal Data Privacy Bill: What does it mean for individuals and businesses?

Indian authorities want to bring the country's data protection law in line with international best practice, with the European Union's General Data Protection Regulation (GDPR) as the preferred model.

Cyware News - Latest Cyber News

Integrity360 acquires Caretower to strengthen its cybersecurity services

Ireland-based Integrity360 and Caretower announced that they have joined forces with Caretower becoming an Integrity360 company. The terms of the transaction were not disclosed.

The Hacker News

Iran's MuddyWater Hacker Group Using New Malware in Worldwide Cyber Attacks

Cybersecurity agencies from the U.K. and the U.S. have laid bare a new malware used by the Iranian government-sponsored advanced persistent threat (APT) group in attacks targeting government and commercial networks worldwide. "MuddyWater actors are positioned both to provide stolen data and accesses to the Iranian government and to share these with other malicious cyber actors," the agencies

Cyware News - Latest Cyber News

Iranian Government-Sponsored MuddyWater APT Conducting Malicious Cyber Operations Against Critical Infrastructure

US and UK agencies today shared information on new malware deployed by the Iranian-backed MuddyWatter hacking group in attacks targeting critical infrastructure worldwide.

Threatpost

Microsoft Exchange Bugs Exploited by 'Cuba' Ransomware Gang

The ransomware gang known as Cuba is increasingly shifting to exploiting Exchange bugs - including crooks' favorites, ProxyShell and ProxyLogon - as initial infection vectors.

Cyware News - Latest Cyber News

Multiple Hacking Groups Targeting ICS/OT Systems

A new report on industrial cybersecurity has revealed three new threat groups, besides LockBit 2.0 and Conti, that have been targeting the industrial sector. Experts spotted three new groups Petrovite, Kostovite, and Erythrite, that have been targeting ICS/OT systems. To protect from threats, the industrial sector ought to have

an in-depth security strategy to overcome and withstand such attacks.

The Hacker News

New "SockDetour" Fileless, Socketless Backdoor Targets U.S. Defense Contractors

Cybersecurity researchers have taken the wraps off a previously undocumented and stealthy custom malware called SockDetour that targeted U.S.-based defense contractors with the goal of being used as a secondary implant on compromised Windows hosts. "SockDetour is a backdoor that is designed to remain stealthily on compromised Windows servers so that it can serve as a backup backdoor in case the

Cyware News - Latest Cyber News

Nvidia confirms it's investigating an 'incident,' reportedly a cyberattack

Nvidia confirmed that it was investigating an "incident" -- hours after media reported that the graphics chipmaking giant had experienced a devastating cyberattack that "completely compromised" the company's internal systems over the past two days.

Cyware News - Latest Cyber News

Ofcom Set to Crack Down on Phone Fraud

Fraudsters often try to spoof the number of banks and other institutions in order to persuade targets of the legitimacy of their request for personal and financial information.

Cyware News - Latest Cyber News

Official website of Russian Parliament, MoD and Kremlin go offline

The affected websites include the Kremlin (kremlin.ru) which is the official website of President Vladimir Putin, the Russian Ministry of Defense, and the official website of the Russian parliament.

Krebs on Security

Russia Sanctions May Spark Escalating Cyber Conflict

President Biden joined European leaders this week in enacting economic sanctions against Russia in response its military invasion of Ukraine. The West has promised tougher sanctions are coming, but experts warn these will almost certainly trigger a Russian retaliation against America and its allies, which could escalate into cyber attacks on Western financial institutions and energy infrastructure.

ZDNet | security RSS

Report: Ukraine calls for volunteer hackers to protect critical infrastructure

The country is reportedly asking volunteers to join digital defensive and surveillance missions.

The Hacker News

Russia-Ukraine War: Phishing, Malware and Hacker Groups Taking Sides

Ukraine's Computer Emergency Response Team (CERT-UA) has warned of Belarusian state-sponsored hackers targeting its military personnel and related individuals as part of a phishing campaign mounted amidst Russia's military invasion of the country. "Mass phishing emails have recently been observed targeting private 'i.ua' and 'meta.ua' accounts of Ukrainian military personnel and related

Cyware News - Latest Cyber News

Russian Sandworm Distributes New Cyclops Blink Malware

The U.S. and U.K released a joint security advisory warning that Russian-backed Sandworm has started using a new malware, dubbed Cyclops Blink. The group has mostly deployed the Cyclops Blink to WatchGuard devices. The joint advisory recommends referring to indicators of compromise and provides guidance on how to better detect any possible activity on networks.

The Hacker News

Social Media Hijacking Malware Spreading Through Gaming Apps on Microsoft Store

A new malware capable of controlling social media accounts is being distributed through Microsoft's official app store in the form of trojanized gaming apps, infecting more than 5,000 Windows machines in Sweden, Bulgaria, Russia, Bermuda, and Spain. Israeli cybersecurity company Check Point dubbed the malware "Electron Bot," in reference to a command-and-control (C2) domain used in recent

WeLiveSecurity

The past is present: Riffing on a cybersecurityappropriate tune for Black History Month

What can social movements of the past teach you about the future - and about protecting your digital self? The post The past is present: Riffing on a cybersecurityappropriate tune for Black History Month appeared first on WeLiveSecurity

cyberscoop

TrickBot malware suddenly got quiet, researchers say, but it's hardly the end for its operators

CyberScoop

The operators of TrickBot have essentially shut down the notorious malware, multiple reports say, but evidence suggests the gang has begun using other platforms or folded operations into another cybercrime group altogether. Researchers at Intel471 and AdvIntel noted a sharp dip in recent TrickBot activity in separate reports Thursday, even though the command-and-control infrastructure for the malware remains operational. Intel471 said "it's likely that the Trickbot operators have phased Trickbot malware out of their operations in favor of other platforms," probably Emotet -- a development researchers have been tracking for months. AdvIntel's Yelisey Boguslavskiy, meanwhile, said in his repor[...]

Threatpost

TrickBot Takes a Break, Leaving Researchers Scratching Their Heads

The infamous trojan is likely making some major operational changes, researchers believe.

Security Affairs

UK's NHS Digital warns of an RCE in Okta Advanced Server Access client

The UK's NHS Digital agency warns of an RCE in the Windows client for the Okta Advanced Server Access authentication management platform. The UK's NHS Digital agency published a security advisory to warn organizations of a remote code execution flaw, tracked as CVE-2022-24295, impacting the Windows client for the Okta Advanced Server Access authentication management [...] The post UK's NHS Digital warns of an RCE in Okta Advanced Server Access client appeared first on Security Affairs.

Security Affairs

Ukraine calls on independent hackers to defend against Russia, Russian underground responds

While Ukraine calls for hacker underground to defend against Russia, ransomware gangs make their moves. Ukraine's government is asking for volunteers from the hacker underground to provide their support in protecting critical infrastructure and carry out offensive operations against Russian state-sponsored hackers, reported Reuters which cited two e experts involved in the project. The call [...] The post Ukraine calls on independent hackers to defend against Russia, Russian underground responds appeared first on Security Affairs.

Security Affairs

Ukraine: Belarusian APT group UNC1151 targets military personnel with spear phishing

The CERT of Ukraine (CERT-UA) warned of a spear-phishing campaign targeting Ukrainian armed forces personnel. The Computer Emergency Response Team of Ukraine (CERT-UA) is warning of an ongoing spear-phishing campaign targeting private email accounts belonging to Ukrainian armed forces personnel. The Ukrainian agency attributes the campaign to the Belarus-linked cyberespionage group tracked as UNC1151. In [...] The post Ukraine: Belarusian APT group UNC1151 targets military personnel with spear phishing appeared first on Security Affairs.

CyberScoop

Ukrainian cyber officials warn of new wave of phishing attacks

Ukrainian officials warned Friday that Belarusian hackers are sending a wave of phishing emails targeting Ukrainian soldiers and civilians. "Mass phishing emails have recently been observed targeting private 'i.ua' and 'meta.ua' accounts of Ukrainian military personnel and related individuals," Ukraine's Computer Emergency Response Team wrote in a Facebook post Friday. Both URLs belong to Ukraine-based email services. Once an account is compromised, hackers gain access to the target's messages and their contact details, allowing them to send additional phishing emails to their contacts, the CERT said. Ukraine's State Service of Special Communications and Information Protection issued a separ[...]

Twitter

huntr Hacktivity

Use of Hard-coded Cryptographic Key in (CVE-2022-0664) reported by mrsuicideparrot - Patch: #bugbounty #infosec #opensource

CVE

CVE-2022-0664 Use of Hard-coded Cryptographic Key in Go prior to 0.8.5,0.9.4,0.10.0,0.10.1.

RedPacket

Airspan Networks Mimosa product line command execution | CVE-2022-21143 -

CVE

CVE-2022-21141 MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API

Security

functions. An attacker may...

RedPacket Security

Airspan Networks Mimosa product line code execution | CVE-2022-21141 -

SRM IT Risk

IT Risk: Airspan Networks MimosaCVSS v3:10.0 -2/3 Mimosa CVE-2022-21196 CVE-2022-21141 CVE-2022-21215 CVE-2022-21176

CVE

CVE-2022-21215 This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions t...

Remotely Alerts

Severity: | Use of Hard-coded Cryptographic Key in G... | CVE-2022-0664 | Link for more:

CVE

CVE-2022-21196 MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes....

Vulmon Vulnerability Feed

CVE-2022-21143 Airspan Networks Mimosa

SRM IT Risk

IT Risk: Airspan Networks MimosaCVSS v3:10.0 -3/3 CVE-2022-0138 CVE-2022-21143 CVE-2022-21800

SRM IT Risk

IT Risk: CVSS v3:10.0 Vulnerability in Airspan Networks Mimosa -3/3 CVE-2022-21196 CVE-2022-21141 CVE-2022-21215 CVE-2022-21176 CVE-2022-0138 CVE-2022-21143 CVE-2022-21800

Michael Saylor

I recently had the chance to discuss crypto market volatility and how #bitcoin can clean up cyberspace and dramatically upgrade our cybersecurity with @KenzieSigalos.

Source: NIST

NIST CVE: Critical

CVE-2022-0671

A flaw was found in vscode-xml in versions prior to 0.19.0. **Schema** download could lead to blind SSRF or DoS via a large file.

CRITICAL Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-21196

MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.

CRITICAL Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-21141

MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.

CRITICAL Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-21143

MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.

CRITICAL Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-21215

This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.

CRITICAL Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-0664

Use of Hard-coded Cryptographic Key in Go **github**.com/gravitl/netmaker prior to 0.8.5,0.9.4,0.10.0,0.10.1.

CRITICAL Vector: network Created: 2022-02-18 Updated: 2022-02-26

Source: NIST

NIST CVE: High

CVE-2022-0646

A flaw use after free in the **Linux** kernel Management Component Transport Protocol (MCTP) subsystem was found in the way user triggers cancel_work_sync after the unregister_netdev during removing device. A local user could use this flaw to crash the system or escalate their privileges on the system. It is actual from **Linux Kernel** 5.17-rc1 (when mctp-serial.c introduced) till 5.17-rc5.

HIGH Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-0666

CRLF Injection leads to Stack Trace Exposure due to lack of filtering at https://demo.microweber.org/ in Packagist microweber/microweber prior to 1.2.11.

HIGH Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-21176

MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.

HIGH Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-0138

MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.

HIGH Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2021-46570

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current

CVE-2021-46082

Moxa TN-5900 v3.1 series routers, MGate 5109 v2.2 series protocol gateways, and MGate 5101-PBM-MN v2.1 series protocol gateways were discovered to contain a memory leak which allows attackers to cause a Denial of Service (DoS) via crafted packets.

Vector: Created: Updated:

HIGH	network	2022-02-18	2022-02-26

process. Was ZDI-CAN-15364.

HIGH	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

CVE-2021-46606

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15400.

HIGH	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

CVE-2021-46605

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15399.

HIGH	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

CVE-2021-46583

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15377.

HIGH	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

CVE-2021-46603

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15397.

HIGH	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

CVE-2021-46582

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15376.

HIGH	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

CVE-2021-46563

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14990.

HIGH	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

CVE-2021-46562

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14987.

HIGH | Vector: local | Created: 2022-02-18 | Updated: 2022-02-26

CVE-2021-46581

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15375.

HIGH | Vector: local | Created: 2022-02-18 | Updated: 2022-02-26

CVE-2021-46564

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15023.

HIGH | Vector: local | Created: 2022-02-18 | Updated: 2022-02-26

CVE-2021-46598

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15392.

HIGH | Vector: local | Created: 2022-02-18 | Updated: 2022-02-26

CVE-2021-46580

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15374.

HIGH | Vector: local | Created: 2022-02-18 | Updated: 2022-02-26

CVE-2021-46601

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15395.

HIGH | Vector: local | Created: 2022-02-18 | Updated: 2022-02-26

CVE-2021-46579

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a

CVE-2021-46578

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a

malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15373.

HIGH Vector: local Created: 2022-02-18 Updated: 2022-02-26

malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15372.

HIGH Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2021-46604

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PNG images. Crafted data in a PNG image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15398.

HIGH Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2021-46571

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15365.

HIGH Vector: local Created: 2022-02-18 Updated: 2022-02-26

Source: NIST

NIST CVE: Medium

CVE-2022-0673

A flaw was found in LemMinX in versions prior to 0.19.0. Cache poisoning of external **schema** files due to directory traversal.

MEDIUM Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-0672

A flaw was found in LemMinX in versions prior to 0.19.0. Insecure redirect could allow unauthorized access to sensitive information locally if LemMinX is run under a privileged user.

MEDIUM Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-0678

Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11.

MEDIUM Vector: network Created: 2022-02-19 Updated: 2022-02-26

CVE-2022-0690

Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11.

MEDIUM Vector: network Created: 2022-02-19 Updated: 2022-02-26

CVE-2022-0451

Dart SDK contains the **HTTPClient** in dart:io library whcih includes authorization headers when handling cross **origin** redirects. These headers may be explicitly set and contain sensitive information. By default, HttpClient handles **redirection** logic. If a request is sent to example.com with authorization header and it redirects to an attackers site, they

CVE-2022-21800

MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not **salt** the hash. As a result, attackers may be able to **crack** the

might not expect attacker site to receive authorization header. We recommend updating the Dart SDK to version 2.16.0 or beyond.

MEDIUM Vector: network Created: 2022-02-18 Updated: 2022-02-26

CVE-2022-0689

Use multiple time the one-time coupon in Packagist microweber/microweber prior to 1.2.11.

MEDIUM Vector: network Created: 2022-02-19 Updated: 2022-02-26

hashed passwords.

MEDIUM Vector: network Created: 2022-02-18 Updated: 2022-02-26

Source: NIST

NIST CVE: Low

CVE-2021-46602

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15396.

LOW Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2021-46607

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15401.

LOW Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2021-46608

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15402.

LOW Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2021-46600

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15394.

LOW Vector: local Created: 2022-02-18 Updated: 2022-02-26

CVE-2021-46599

This vulnerability allows remote attackers to disclose sensitive information on affected installations

of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15393.

LOW	Vector: local	Created: 2022-02-18	Updated: 2022-02-26

Source: NIST

NIST CVE: Unrated

CVE-2021-44132

A command injection vulnerability in the function formImportOMCIShell of C-DATA ONU4FERW V2.1.13_X139 allows attackers to execute arbitrary commands via a crafted file.

UNRATED	Vector: unkown	Created: 2022-02-25	Updated: 2022-02-26

CVE-2021-42244

A cross-site scripting (XSS) vulnerability in PaquitoSoftware Notimoo v1.2 allows attackers to execute arbitrary web scripts or HTML via a crafted title or message in a notification.

UNRATED	Vector: unkown	Created: 2022-02-25	Updated: 2022-02-26

CVE-2021-37504

A cross-site scripting (XSS) vulnerability in the fileNameStr parameter of jQuery-Upload-File v4.0.11 allows attackers to execute arbitrary web scripts or HTML via a crafted file with a Javascript payload in the file name.

UNRATED	Vector: unkown	Created: 2022-02-25	Updated: 2022-02-26

CVE-2020-36516

An issue was discovered in the **Linux** kernel through 5.16.11. The mixed IPID assignment method with the hash-based IPID assignment policy allows an off-path attacker to inject data into a victim's TCP session or terminate that session.

UNRATED	Vector: unkown	Created: 2022-02-26	Updated: 2022-02-26

CVE-2022-0762

Business Logic Errors in **GitHub** repository microweber/microweber prior to 1.3.

UNRATED	Vector: unkown	Created: 2022-02-26	Updated: 2022-02-26

CVE-2022-0763

Cross-site Scripting (XSS) - Stored in **GitHub** repository microweber/microweber prior to 1.3.

UNRATED	Vector: unkown	Created: 2022-02-26	Updated: 2022-02-26

CVE-2022-23921

Exploitation of this vulnerability may result in local privilege escalation and code execution. GE maintains exploitation of this vulnerability is only possible if the attacker has login access to a machine actively running CIMPLICITY, the CIMPLICITY server is not already running a project, and the server is licensed for multiple projects.

UNRATED	Vector: unkown	Created: 2022-02-25	Updated: 2022-02-26

CVE-2022-25095

Home Owners Collection Management System v1.0 allows unauthenticated attackers to compromise user accounts via a crafted POST request.

UNRATED	Vector: unkown	Created: 2022-02-26	Updated: 2022-02-26

CVE-2022-25094

Home Owners Collection Management System v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the parameter "cover" in SystemSettings.php.

UNRATED Vector: unkown Created: 2022-02-26 Updated: 2022-02-26

CVE-2022-25096

Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in /members/view_member.php.

UNRATED Vector: unkown Created: 2022-02-26 Updated: 2022-02-26

CVE-2022-25262

In **JetBrains** Hub before 2022.1.14434, SAML request takeover was possible.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25264

In **JetBrains TeamCity** before 2021.2.3, environment variables of the "password" type could be logged in some cases.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25260

JetBrains Hub before 2021.1.14276 was vulnerable to blind Server-Side Request Forgery (SSRF).

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25259

JetBrains Hub before 2021.1.14276 was vulnerable to reflected XSS.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25261

JetBrains TeamCity before 2021.2.2 was vulnerable to reflected XSS.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25263

JetBrains TeamCity before 2021.2.3 was vulnerable to OS command injection in the Agent Push feature configuration.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-24442

JetBrains YouTrack before 2021.4.40426 was vulnerable to SSTI (Server-Side Template Injection) via FreeMarker templates.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-24986

KDE KCron through 21.12.2 uses a temporary file in /tmp when saving, but reuses the filename during an editing session. Thus, someone watching it be created the **first** time could potentially intercept the file the following time, enabling that person to run unauthorized commands.

UNRATED Vector: unkown Created: 2022-02-26 Updated: 2022-02-26

CVE-2022-25359

On ICL ScadaFlex II SCADA Controller SC-1 and SC-2 1.03.07 devices, unauthenticated remote attackers can overwrite, delete, or create files.

UNRATED Vector: unkown Created: 2022-02-26 Updated: 2022-02-26

CVE-2021-40046

PCManager versions 11.1.1.95 has a privilege escalation vulnerability. Successful exploit could allow the attacker to access certain resource beyond its privilege.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22441

Some **Huawei** products have an integer overflow vulnerability. Successful exploitation of this vulnerability may lead to kernel crash.

Created: Updated:

CVE-2022-21798

The affected product is vulnerable due to cleartext **transmission** of credentials seen in the **CIMPLICITY** network, which can be easily spoofed and used to log in to make operational changes to the system.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25170

The affected product is vulnerable to a stack-based buffer overflow while processing project files, which may allow an attacker to execute arbitrary code

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-21209

The affected product is vulnerable to an out-of-bounds read while processing project files, which allows an attacker to craft a project file that would allow arbitrary code execution.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-23985

The affected product is vulnerable to an out-of-bounds write while processing project files, which allows an attacker to craft a project file that would allow arbitrary code execution.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22478

The interface of a certain HarmonyOS module has a UAF vulnerability. Successful exploitation of this vulnerability may lead to information leakage.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22480

The interface of a certain HarmonyOS module has an integer overflow vulnerability. Successful exploitation of this vulnerability may lead to heap memory overflow.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22479

The interface of a certain HarmonyOS module has an invalid address access vulnerability. Successful exploitation of this vulnerability may lead to kernel crash.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-40043

The laser command injection vulnerability exists on **AIS-BW80H-00** versions earlier than AIS-BW80H-00 9.0.3.4(H100SP13C00). The devices cannot effectively defend against external malicious interference. Attackers need the device to be visually exploitable and successful triggering of this vulnerability could execute **voice** commands on the device.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-23495

The package **karma** before 6.3.16 are vulnerable to Open Redirect due to missing validation of the return_url query parameter.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22394

There is a buffer overflow vulnerability in smartphones. Successful exploitation of this vulnerability may cause DoS of the apps during Multi-Screen **Collaboration**.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22395

There is a code injection vulnerability in smartphones. Successful exploitation of this vulnerability may affect service confidentiality.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22489

There is a DoS vulnerability in smartphones. Successful exploitation of this vulnerability may affect service availability.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-37027

There is a DoS vulnerability in smartphones. Successful exploitation of this vulnerability may affect service integrity.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2021-22430	There is a logic bypass vulnerability in smartphones. Successful exploitation of this vulnerability may cause code injection.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22429	There is a memory address out of bounds in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22433	There is a memory address out of bounds in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22426	There is a memory address out of bounds in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22434	There is a memory address out of bounds vulnerability in smartphones. Successful exploitation of this vulnerability may cause malicious code to be executed.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22437	There is a software integer overflow leading to a TOCTOU condition in smartphones. Successful exploitation of this vulnerability may cause random address access.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22432	There is a vulnerability when configuring permission isolation in smartphones. Successful exploitation of this vulnerability may cause out-of-bounds access.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22431	There is a vulnerability when configuring permission isolation in smartphones. Successful exploitation of this vulnerability may cause out-of-bounds access.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-37103	There is an improper permission management vulnerability in the **Wallet** apps. Successful exploitation of this vulnerability may affect service confidentiality.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22319	There is an improper verification vulnerability in smartphones. Successful exploitation of this vulnerability may cause integer overflows.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-22448	There is an improper verification vulnerability in smartphones. Successful exploitation of this vulnerability may cause unauthorized read and write of some files.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-26617	This issues due to insufficient verification of the various input values from user's input. The vulnerability allows remote attackers to execute malicious code in Firstmall via navercheckout_add function.	UNRATED	Vector: unkown	Created: 2022-02-25 Updated: 2022-02-26
CVE-2021-46702	**Tor Browser** 9.0.7 on **Windows** 10 build 10586 is vulnerable to information disclosure. This could allow local attackers to bypass the intended anonymity feature and obtain information regarding the onion services visited by a local user. This can be accomplished by analyzing RAM memory even several			
CVE-2022-25061	**TP-LINK** TL-WR840N(ES)_V6.20_180709 was discovered to contain a command injection vulnerability via the component oal_setIp6DefaultRoute.			

hours after the local user used the product. This occurs because the product doesn't properly free memory.

UNRATED Vector: unkown Created: 2022-02-26 Updated: 2022-02-26

CVE-2022-25060

TP-LINK TL-WR840N(ES)_V6.20_180709 was discovered to contain a command injection vulnerability via the component oal_startPing.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25062

TP-LINK TL-WR840N(ES)_V6.20_180709 was discovered to contain an integer overflow via the function dm_checkString. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-23308

valid.c in **libxml2** before 2.9.13 has a use-after-free of ID and IDREF attributes.

UNRATED Vector: unkown Created: 2022-02-26 Updated: 2022-02-26

CVE-2021-42952

Zepl Notebooks before 2021-10-25 are affected by a sandbox escape vulnerability. Upon launching Remote Code Execution from the Notebook, users can then use that to subsequently escape the running context sandbox and proceed to access internal Zepl assets including cloud metadata services.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-25064

TP-LINK TL-WR840N(ES)_V6.20_180709 was discovered to contain a remote code execution (RCE) vulnerability via the function oal_wan6_setIpAddr.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-0615

Use-after-free in eset_rtp kernel module used in ESET products for **Linux** allows potential attacker to trigger denial-of-service condition on the system.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-24710

Weblate is a copyleft software web-based continuous localization system. Versions prior to 4.11 do not properly neutralize user input used in user name and language fields. Due to this improper neutralization it is possible to perform cross-site scripting via these fields. The issues were fixed in the 4.11 release. Users unable to upgrade are advised to add their own neutralize logic.

UNRATED Vector: unkown Created: 2022-02-25 Updated: 2022-02-26

CVE-2022-21706

Zulip is an open-source team **collaboration** tool with topic-based threading. **Zulip Server** version 2.0.0 and above are vulnerable to insufficient access control with multi-use invitations. A Zulip Server deployment which hosts multiple organizations is vulnerable to an attack where an invitation created in one organization (potentially as a role with elevated permissions) can be used to join any other organization. This bypasses any restrictions on required domains on users' email addresses, may be used to gain access to organizations which are only accessible by invitation, and may be used to gain access with elevated privileges. This issue has been patched in release 4.10. There are no known workarounds for this issue. ### Patches _Has the problem been patched? What versions should users upgrade to?_ ### Workarounds _Is

UNRATED | Vector: unkown | Created: 2022-02-25 | Updated: 2022-02-26

there a way for users to fix or remediate the vulnerability without upgrading?_ ### References _Are there any links users can visit to **find** out more?_ ### For more information If you have any questions or comments about this advisory, you can discuss them on the [developer community Zulip server] (https://zulip.com/developer-community/), or email the [Zulip security team] (mailto:security@zulip.com).

UNRATED | Vector: unkown | Created: 2022-02-26 | Updated: 2022-02-26

Source: Hybrid Analysis

Top malicious files

100% Threat score	kg (.) exe
100% Threat score	FileZilla20Client (.) exe
100% Threat score	Activation 2 (Execute online after install done) (.) exe
100% Threat score	DropboxInstaller (.) exe
100% Threat score	maple (.) exe
86% Threat score	Main__Setup (.) exe
85% Threat score	epubor_ultimate (1) (.) exe
100% Threat score	Hawkshaw-v1 (.) 17-17042020-1252 (.) apk
100% Threat score	Qbase (.) exe
100% Threat score	PdfPro (.) exe
100% Threat score	x
95% Threat score	Loveware (.) bat
85% Threat score	recover-data-202 (.) exe
80% Threat score	ESET_v7 (.) 2 (.) 19 (.) 0_Mod_By_ZackModz_A2ZAPK (.) COM (.) apk

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://112 (.) 31 (.) 8 (.) 172:46923/mozi (.) a
94% Threat score	http://112 (.) 167 (.) 165 (.) 139:42570/bin (.) sh
93% Threat score	http://182 (.) 118 (.) 162 (.) 232:33185/i
93% Threat score	http://59 (.) 99 (.) 194 (.) 52:47522/bin (.) sh
95% Threat score	http://115 (.) 54 (.) 126 (.) 250:56781/i
93% Threat score	http://182 (.) 123 (.) 255 (.) 139:60066/Mozi (.) m
93% Threat score	http://112 (.) 81 (.) 75 (.) 6:52856/mozi (.) m
90% Threat score	http://43 (.) 240 (.) 23 (.) 158:1598/ (.) i

88% Threat score	http://115 (.) 55 (.) 52 (.) 133:52450/Mozi (.) m
88% Threat score	http://171 (.) 38 (.) 149 (.) 34:40960/bin (.) sh
83% Threat score	http://61 (.) 3 (.) 189 (.) 114:32906/i
74% Threat score	https://grudoings (.) cc/wall/report (.) php
88% Threat score	http://117 (.) 196 (.) 59 (.) 0:52766/Mozi (.) m
83% Threat score	http://77 (.) 95 (.) 56 (.) 158:16705/ (.) i
77% Threat score	http://ijojoijoijiojoij (.) tk/
74% Threat score	http://www (.) bitstream (.) com/font_rendering/products/dev_fonts/vera (.) html

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

#6 **Michael Persaud**

business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

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 Pakistan

#10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

#1 United States

#2 Indonesia

#3 Germany

#4 Japan

#5 Russia

#6 Netherlands

#7 Iran

#8 Hong Kong

#9 France

#10 United Kingdom