Security Rabbits

Your Security Rabbits report for February 08, 2022

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

'Small portion' of customers on Hong Kong online retail site hit by data breach

There was no evidence of financial loss or misuse of customer data, HKTV says, adding it will take responsibility for any unauthorized purchases made as a result of the breach.

Cyware News - Latest Cyber News

APT27 Group Targets German Organizations with HyperBro

Researchers warned against ongoing attacks by China-backed APT27 hacking group that has been targeting commercial organizations in Germany. The goal of the campaign seems to be stealing sensitive information and targeting victims' customers in supply chain attacks. The intelligence agency has published IOCs and YARA rules to help targeted German organizations check for infections.

IT Security Guru

BlackCat gang (ALPHV) linked with BlackMatter/Darkside ransomware operations

The BlackCat ransomware operation, also known as ALPHV has confirmed their former involvement in the notorious BlackMatter/Darkside ransomware operations. BlackCat/ALPHV, launched in November 2021, is a new feature-rich ransomware operation developed, somewhat unusually, in the Rust programming language. The ransomware executable is highly customizable, with different encryption methods and options allowing for attacks on a [...] The post BlackCat gang (ALPHV) linked with BlackMatter/Darkside ransomware operations appeared first on IT Security Guru.

ZDNet | security RSS

Chinese telecom Hytera charged for allegedly recruiting Motorola employees to steal trade secrets

The firm allegedly conspired with employees to steal digital radio technology.

The Hacker News

CISA Orders Federal Agencies to Patch Actively Exploited Windows Vulnerability

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is urging federal agencies to secure their systems against an actively exploited security vulnerability in Windows that could be abused to gain elevated permissions on affected hosts. To that end, the agency has added CVE-2022-21882 (CVSS score: 7.0) to the Known Exploited Vulnerabilities Catalog, necessitating that Federal

Cyware News - Latest Cyber News

Cybercriminals Using SEO Poisoning To Spread Malware

A new SEO poisoning campaign drops Batloader and Atera Agent malware targeting users attempting to download productivity tools, such as Zoom, Visual Studio, and TeamViewer. The researchers claim that some techniques used in the campaigns match with those in the Conti playbooks. It is suggested to check before downloading any software or apps.

Cyware News - Latest Cyber News

DPD Group parcel tracking flaw may have exposed customer data

Researchers at Pen Test Partners explored the system and found that they could try out parcel codes on API calls and get back OpenStreetMap addresses with the recipient's position on the map.

Cyware News - Latest Cyber News

Equifax finalizes data breach settlement with US regulators

Credit reporting agency Equifax finalized a settlement for a 2017 breach that affected over 147 million US citizens and 15 million Brits. Equifax first admitted the massive breach in September 2017.

The Hacker News

Hackers Backdoored Systems at China's National Games Just Before Competition

Systems hosting content pertaining to the National Games of China were successfully breached last year by an unnamed Chinese-language-speaking hacking group. Cybersecurity firm Avast, which dissected the intrusion, said that the attackers gained access to a web server 12 days prior to the start of the event on September 3 to drop multiple reverse web shells for remote access and achieve

IT Security Guru

$4.4 million stolen in attack on blockchain infrastructure

Hackers stole $4.4 million from the blockchain infrastructure company Meter in a cyberattack on Saturday. The company manages infrastructure allowing smart contracts to scale and travel through heterogonous blockchain networks. Both Meter and Moonriver networks were affected. The company said it manages an infrastructure that allows smart contracts to scale and travel through heterogeneous blockchain [...] The post $4.4 million stolen in attack on blockchain infrastructure appeared first on IT Security Guru.

Security Affairs

Avast released a free decryptor for TargetCompany ransomware

Cybersecurity firm Avast has released a decryption tool to allow victims of TargetCompany ransomware to recover their files for free. Czech cybersecurity software firm Avast has released a decryption tool that could allow victims of the TargetCompany ransomware to recover their files for free under certain circumstances. The experts warn that the decryptor consumes most of the [...] The post Avast released a free decryptor for TargetCompany ransomware appeared first on Security Affairs.

The Hacker News

Chinese Hackers Target Taiwanese Financial Institutions with a new Stealthy Backdoor

A Chinese advanced persistent threat (APT) group has been targeting Taiwanese financial institutions as part of a "persistent campaign" that lasted for at least 18 months. The intrusions, whose primary intent was espionage, resulted in the deployment of a backdoor called xPack, granting the adversary extensive control over compromised machines, Broadcom-owned Symantec said in a report published

Threatpost

CISA Orders Federal Agencies to Fix Actively Exploited Windows Bug

Feb. 18 is the deadline to patch a bug that affects all unpatched versions of Windows 10 and requires zero user interaction to exploit.

Cyware News - Latest Cyber News

CoinDesk CMS Vulnerability Let Hackers Trade on Nonpublic Info

A vulnerability in the CMS of cryptocurrency news site CoinDesk allowed hackers "to trade on nonpublic information ahead of the publication of at least one article," according to the publication.

IT Security Guru

Cybersecurity compliance still not a priority for many

The most consistent data point in the IBM i Marketplace Survey Results over recent years has been the ever-present cybersecurity threat. This year is no exception. The study shows that 62% of organisations consider cybersecurity a number one concern as they plan their IT infrastructure. 22% cite regulations and compliance in their top five. While companies that [...] The post Cybersecurity compliance still not a priority for many appeared first on IT Security Guru.

IT Security Guru

DPD Parcel tracking flaw may have exposed customer data

DPD Groups' package tracking system has potentially been exploited to access the personally identifiable details of its clients. DPD Group, a parcel delivery service with a global presence that ships around two billion parcels annually worldwide requires customers to track their parcels by entering a parcel code and a post code. Pen Test Partners researchers [...] The post DPD Parcel tracking flaw may have exposed customer data appeared first on IT Security Guru.

ZDNet | security RSS

Google Cloud launches agentless cryptojacking malware scanner

The new security feature is designed to hunt down instances of cryptojacking.

Security Affairs

Hackers breached a server of National Games of China days before the event

An unnamed Chinese-language-speaking hacking group compromised systems at National Games of China in 2021. Researchers at cybersecurity firm Avast discovered that a Chinese-language-speaking threat actor has compromised systems at National Games of China in 2021. The event took place on September 15, 2021 in Shaanxi (China), it is a national version of the Olympics with only local [...] The post Hackers breached a server of National Games of China days before the event appeared first on Security Affairs.

The Hacker News

How Attack Surface Management Preempts Cyberattacks

The wide-ranging adoption of cloud facilities and the subsequent mushrooming of organizations' networks, combined with the recent migration to remote work, had the direct consequence of a massive expansion of organizations' attack surface and led to a growing number of blind spots in connected architectures. The unforeseen results of this expanded and attack surface with fragmented monitoring

CyberScoop

IRS announces it will stop use of facial recognition for identity verification

The Internal Revenue Service will transition away from using a third-party authentication service that deploys facial recognition technology in order to verify new online accounts, the agency announced Monday. The transition will take place "over the coming weeks in order to prevent larger disruptions to taxpayers during filing season," an IRS news release states. The pullback of the plan comes in response to growing concerns from both advocates and lawmakers that the agency's decision to put the biometric data of millions of Americans into the private sector's hands could pose enormous privacy and security risks. The IRS said it is working on developing an authentication process that does n[...]

Cyware News - Latest Cyber News

Law enforcement action push ransomware gangs to surgical attacks

Numerous law enforcement actions leading to the arrests and takedown of ransomware operations in 2021 have forced threat actors to narrow their scope and maximize the efficiency of their operations.

Threatpost

LockBit, BlackCat, Swissport, Oh My! Ransomware Activity Stays Strong

However, groups are rebranding and recalibrating their profiles and tactics to respond to law enforcement and the security community's focus on stopping ransomware attacks.

Threatpost

Medusa Malware Joins Flubot's Android Distribution Network

Two powerful trojans with spyware and RAT capabilities are being delivered in side-by-side campaigns using a common infrastructure.

The Hacker News

Microsoft Disables Internet Macros in Office Apps by Default to Block Malware Attacks

Microsoft on Monday said it's taking steps to disable Visual Basic for Applications (VBA) macros by default across its products, including Word, Excel, PowerPoint, Access, and Visio, for documents downloaded from the web in an attempt to eliminate an entire class of attack vector. "Bad actors send macros in Office files to end users who unknowingly enable them, malicious payloads are delivered,

The Hacker News

Microsoft Temporarily Disables MSIX App Installers to Prevent Malware Abuse

Microsoft last week announced that it's temporarily disabling the MSIX ms-appinstaller protocol handler in Windows following evidence that a security vulnerability in the installer component was exploited by threat actors to deliver malware such as Emotet, TrickBot, and Bazaloader. MSIX, based on a combination of .msi, .appx, App-V and ClickOnce installation technologies, is a universal Windows

Cyware News - Latest Cyber News

NetWalker ransomware affiliate sentenced to seven years in prison

The suspect pleaded guilty in front of a judge after he was arrested by Canadian police in January 2021 as part of an international law enforcement crackdown against NetWalker.

Cyware News - Latest Cyber News

Newly Found Sugar Ransomware is Now Being Offered as RaaS

The cyber threat team at retail giant Walmart has uncovered the new ransomware family Sugar, which is now being made available to cybercriminals as a Ransomware-as-a-Service (RaaS).

ZDNet | security RSS

Pay to play PrivateLoader spreads Smokeloader, Redline, Vidar malware

The pay-per-install malware is one of the most popular loaders on the market today.

Threatpost

QuaDream, 2nd Israeli Spyware Firm, Weaponizes iPhone Bug

The now-patched flaw that led to the ForcedEntry exploit of iPhones was exploited by both NSO Group and a different, newly detailed surveillance vendor.

The Hacker News

IoT/connected Device Discovery and Security Auditing in Corporate Networks

Today's enterprise networks are complex environments with different types of wired and wireless devices being connected and disconnected. The current device discovery solutions have been mainly focused on identifying and monitoring servers, workstation PCs, laptops and infrastructure devices such as network firewalls, switches and routers, because the most valuable information assets of

Krebs on Security

IRS To Ditch Biometric Requirement for Online Access

The Internal Revenue Service (IRS) said today it will be transitioning away from requiring biometric data from taxpayers who wish to access their records at the agency's website. The reversal comes as privacy experts and lawmakers have been pushing the IRS and other federal agencies to find less intrusive methods for validating one's identity with the U.S. government online.

CyberScoop

Lawmakers want IRS to address security concerns with use of facial recognition on taxpayers

Democrats and Republicans are turning up the pressure on the Internal Revenue Service to address privacy and security concerns with its plan to use facial recognition on millions of Americans who access the agency's website for tax documents and payments. Sen. Ron Wyden, D-Ore., asked the agency Monday to reverse its decision and halt its work with facial-recognition-based identity verification provider, ID.me. "While the IRS had the best of intentions -- to prevent criminals from accessing Americans' tax records, using them to commit identity theft, and make off with other people's tax refunds -- it is simply unacceptable to force Americans to submit to scans using facial recognition techno[...]

The Hacker News

Medusa Android Banking Trojan Spreading Through Flubot's Attacks Network

Two different Android banking Trojans, FluBot and Medusa, are relying on the same delivery vehicle as part of a simultaneous attack campaign, according to new research published by ThreatFabric. The ongoing side-by-side infections, facilitated through the same smishing (SMS phishing) infrastructure, involved the overlapping usage of "app names, package names, and similar icons," the Dutch mobile

Naked Security

Microsoft blocks web installation of its own App Installer files

It's a big deal when a vendor decides to block one of its own "features" for security reasons. Here's why we think it's a good idea.

Security Affairs

Microsoft disables the ms-appinstaller protocol because it was abused to spread malware

Microsoft temporarily disabled the ms-appinstaller protocol for MSIX because it was abused by malware, such as Emotet. Microsoft announced to have temporarily disabled the ms-appinstaller protocol for MSIX because it was abused by malware, such as Emotet. In December, Microsoft addressed a vulnerability, tracked as CVE-2021-43890, in AppX installer that affects Microsoft Windows which is under active exploitation. "We have [...] The post Microsoft disables the ms-appinstaller protocol because it was abused to spread malware appeared first on Security Affairs.

Cyware News - Latest Cyber News

MuddyWater APT Associated with Recent Attacks on Turkey

Iranian MuddyWater APT has reportedly launched fresh attacks targeting the users in the Turkish government and other private organizations in the country. Hackers lure victims via maldocs that masquerade as genuine documents from the Turkish Health and Interior Ministries. Targeted organizations are required in-depth and multi-layered security infrastructure to stay protected.

The Hacker News

New CapraRAT Android Malware Targets Indian Government and Military Personnel

A politically motivated advanced persistent threat (APT) group has expanded its malware arsenal to include a new remote access trojan (RAT) in its espionage attacks aimed at Indian military and diplomatic entities. Called CapraRAT by Trend Micro, the implant is an Android RAT that exhibits a high "degree of crossover" with another Windows malware known as CrimsonRAT that's associated with Earth

CyberScoop

Palestinian hacking group evolving with new malware, researchers say

A Palestinian-aligned hacking group has targeted Middle Eastern governments, foreign policy think tanks and a state-affiliated airline with a new malware implant as part of "highly targeted intelligence collection campaigns," according to research published Tuesday. The findings, from researchers with cybersecurity firm Proofpoint, unpack the latest activities of an established and well-documented Arabic-speaking hacking group known as MoleRATs and its deployment of a new intelligence-gathering trojan they call "NimbleMamba." The malware serves an intelligence-gathering trojan and, according to the researchers, is likely designed gain initial access to a target system. The group has gone aft[...]

IT Security Guru

QBot steals data in 30 minutes

Qbot, also known as Qakbot or QuakBot, has recently returned to lightning speed attacks, with analysts reporting that it only takes 30 minutes from infection to steal emails and credentials. A new report by DFIR suggests that Qbot was carrying out data-snatching operations in October 2021. It is now believed that the threat actors behind [...] The post QBot steals data in 30 minutes appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Roaming Mantis Android Malware Spreads via SMS Phishing, Malicious Apps in Germany and France

The Roaming Mantis SMS phishing campaign has finally reached Europe, as researchers detect campaigns targeting Android and iPhone users in Germany and France with malicious apps and phishing pages.

Roaming Mantis SMSishing campaign now targets Europe

Threatpost

Roaming Mantis Expands Android Backdoor to Europe
The 'smishing' group lives up to its name, expanding globally and adding image exfiltration to the Wroba RAT it uses to infect mobile victims.

IT Security Guru

Russia arrests hacking group
According to Russian media, 6 men have been arrested at the request of the Ministry of Internal Affairs of the Russian Federation. The men are suspected of stealing and selling credit cards online. "The Tverskoy Court of Moscow received petitions from the investigation to select a measure of restraint in the form of detention against […] The post Russia arrests hacking group appeared first on IT Security Guru.

IT Security Guru

Sensitive information of over 500k people leaked
Morley Companies has announced that it was hit with a ransomware attack last year that resulted in the sensitive information of more than 500,000 people being leaked. The organisation provides business services to dozens of Fortune 500 companies. In a press release, the company said the ransomware attack began on August 1 and made their data […] The post Sensitive information of over 500k people leaked appeared first on IT Security Guru.

Security Affairs

US Telecom providers requested $5.6B to replace Chinese equipment
The Federal Communications Commission (FCC) says that small telecom providers have requested $5.6 billion to replace Chinese gear. The U.S. government has requested telecom providers to replace Chinese equipment in their networks due to security issues and allocated $1.9 billion to support the companies in the transaction. The Federal Communications Commission (FCC) said that the […] The post US Telecom providers requested $5.6B to replace Chinese equipment appeared first on Security Affairs.

IT Security Guru

Washington suspects POLARIS breach
The Washington State Department of Licensing (DOL) has closed down their Professional Online Licensing and Regulatory Information System (POLARIS) as a precaution against suspicious activity. The system stores information regarding license holders and applicant. The information varies but may include Social Security numbers, dates of birth, drivers licence numbers and a range of other personally […] The post Washington suspects POLARIS breach appeared first on IT Security Guru.

Security Affairs

The Roaming Mantis SMS phishing campaign is now targeting Android and iPhone users in Europe with malicious apps and phishing pages. Roaming Mantis surfaced in March 2018 when hacked routers in Japan redirecting users to compromised websites. Roaming Mantis is a credential theft and malware campaign that leverages smishing to distribute malicious Android apps in the format of […] The post Roaming Mantis SMSishing campaign now targets Europe appeared first on Security Affairs.

Security Affairs

Russian Gamaredon APT is targeting Ukraine since October
Russia-linked APT group Gamaredon is behind spear-phishing attacks against Ukrainian entities and organizations since October 2021. Russia-linked cyberespionage group Gamaredon (aka Armageddon, Primitive Bear, and ACTINIUM) is behind the spear-phishing attacks targeting Ukrainian entities and organizations related to Ukrainian affairs, since October 2021, Microsoft said. This week, Palo Alto Networks' Unit 42 reported that the […] The post Russian Gamaredon APT is targeting Ukraine since October appeared first on Security Affairs.

Cyware News - Latest Cyber News

UN Experts: North Korea Stealing Millions in Cyber Attacks
Cyber-actors stole more than $50 million between 2020 and mid-2021 from at least three cryptocurrency exchanges in North America, Europe, and Asia, the panel of U.N. experts noted.

Cyware News - Latest Cyber News

Use-after-free bug spotted in Google Chrome could lead to code execution
CVE-2021-38008 is a use-after-free vulnerability that triggers if the user opens a specially crafted web page in Chrome that could lead to the execution of remote code on the targeted machine.

Twitter

Nothing today

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: NIST

NIST CVE: Medium

Nothing today

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-0505

Cross-Site Request Forgery (CSRF) in Packagist microweber/microweber prior to 1.2.11.

UNRATED Vector: unkown Created: 2022-02-08 Updated: 2022-02-08

CVE-2022-0504

Generation of Error Message Containing Sensitive Information in Packagist microweber/microweber prior to 1.2.11.

UNRATED Vector: unkown Created: 2022-02-08 Updated: 2022-02-08

CVE-2022-0506

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

UNRATED Vector: unkown Created: 2022-02-08 Updated: 2022-02-08

CVE-2022-24450

NATS nats-server before 2.7.2 has Incorrect Access Control. Any authenticated user can obtain the privileges of the System account by misusing the "dynamically provisioned sandbox accounts" feature.

UNRATED Vector: unkown Created: 2022-02-08 Updated: 2022-02-08

Source: Hybrid Analysis

Top malicious files

100% MQ-3018 (.) pdf (.) vbs

100% tmpifci74cl

Threat score	
100% Threat score	36191324866472994010 (.) xls
100% Threat score	2022-08-02_0812 (.) xls
100% Threat score	notepad (.) phpactiondownloadfilenamenotepad_data2FMalware2F2022-02-08-Kaufvertrag_exe2FKaufvertrag20Auto201 (.) exe
100% Threat score	RENSEN-DRIESSEN_0802188 (.) exe
87% Threat score	Ad Clicker Bot - Private - Free-Hack VIP Tool (.) exe
85% Threat score	npp (.) 8 (.) 3 (.) Installer (.) exe
85% Threat score	settings (.) dll
85% Threat score	ScreenToGif (.) exe
71% Threat score	Chronolator internal chronology YP LBK 07 (.) 02 (.) 2022 (.) docm

Threat score	
100% Threat score	2022-07-02_1454 (.) xls
100% Threat score	tmp6sdw9i2o
100% Threat score	2022-04-02_1542 (.) xls
100% Threat score	TraceLoggingEventTyp (.) exe
86% Threat score	ATT35028 (.) HTM
85% Threat score	aiv111 (.) ocx
85% Threat score	f_008eee (.) pdf
71% Threat score	ExtractUsnJrnl (.) exe

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://worldpassporte (.) com/
97% Threat score	http://181 (.) 191 (.) 237 (.) 154:38793/Mozi (.) m
94% Threat score	http://main-datings (.) top/
92% Threat score	http://www (.) hazirfilm (.) com/makas-eller-izle/
92% Threat score	http://bpyo (.) in:8080/bkfHH2hqmU/P79BXJMV417
77% Threat score	https://processor-itsm1 (.) xyz/be/
77% Threat score	http://typing (.) yoisha (.) dev/
77% Threat score	http://vintagames (.) weebly (.) com/chess-prime-3d (.) html
77% Threat score	https://ipfs (.) io/ipfs/QmZpGgpEZUf9Kuc9GmLoEy8sBeerQNgjJ5ExMxfcnXrMs2?#ltara%40icrc (.) org%3Fmc_phishing_protection_id%3D28047-c80bfuadu81e3v72090g
75% Threat score	http://fxqb-oss (.) sunnys (.) top/
74% Threat score	https://zasobygwp (.) pl/
71% Threat score	https://dnsnameservice (.) com (.) cn/?xid=e403cb6bebac4c72a2c3e65d5a0cf070&mc_phishing_protection_id=28047-c811gdadu8188q46tk40

100% Threat score	http://gaminghost873737-38124 (.) portmap (.) io/
95% Threat score	http://122 (.) 195 (.) 39 (.) 111:60634/mozi (.) a
93% Threat score	http://115 (.) 52 (.) 22 (.) 156:53584/i
92% Threat score	http://yahoo-movie (.) spiritx (.) ga/
82% Threat score	http://protegerips (.) com/roo/index (.) html
77% Threat score	http://theautolive (.) co/v1/
77% Threat score	https://vps8042 (.) inmotionhosting (.) com/
77% Threat score	http://url8415 (.) lendeers1 (.) com/ls/click?upn=4gwc6NW8cKObUEKcdfnUpHP-2Fp430qPBFtklNYdscf1ruH7WTmT2DCzcALGAtMgE5gFTF2CK0CMNZCiYFJoYn1UJP 2FifRdfYhBeWgeIBpBeYyqh2l93HW7VF5MVpxY8PV5Ygwh6hmQjd8k108M1aB0WKrbl 2BcxrXWhElmy4sxl-2FC3w3Cv2kJEUNkbJyi1P-2FpRRYMOzLG7gTd8sRhBNQR-2FTBf 2FhfBwBRDVsFKt4g6dtPSxNOy2bKydBYdv-2BVr-2F8ZvPvp4l6PEcBECtUNriASXWUY 2Fldlk337EoOtuzjuFLrKIhL8Eb7vmhzQque7RebKZtHyGLkf2U3kcpPZ2rPcpJorB0E8op 2F00wnvdvwEu8BC4rlMIYuwuMynof1X03EgEz8HaW72RtDTu79KQs0YwNXzKAV0giC 2Fl0UKtC8l3d3ZWc47AEiY-2BesFEquSp-2BUNulXWZrnJABMCYh4Eh17s9mhbshAky8 2FmbgQOiIg9l55LE1WNnZWjO3l4dUhpmPHw2uXc1horEgwOTI4SC-2BAfG675790GM
75% Threat score	http://fanxingqb (.) sunnys (.) top/
74% Threat score	https://www (.) magicinepharma (.) com/injection/keytruda-pembrolizymab
72% Threat score	http://stratawise (.) com/

Source: SpamHaus

Top spamming countries

#1 United States of America

#2 China

#3 Russian Federation

#4 Mexico

#5 Dominican Republic

#6 India

#7 Saudi Arabia

#8 Japan

#9 Brazil

#10 Korea, Republic of

Source: SpamHaus

Top spammers

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

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

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

#4 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#5 **RetroCubes**
Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

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

#7 **Cyber World Internet Services/ e-Insites**
Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.

#8 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#9 **Kobeni Solutions**
High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.

Source: SpamHaus

Top countries with botnet

#1 India

#2 China

#3 United States of America

#4 Thailand

#5 Indonesia

#6 Algeria

#7 Brazil

#8 Viet Nam

#9 Iran (Islamic Republic of)

#10 Pakistan

Source: SpamHaus

Top phishing countries

#1 United States

#2 Germany

#3 Russia

#4 Netherlands

#5 Hong Kong

#6 France

#7 Singapore

#8 India

#9 Bulgaria

#10 United Kingdom