Security Rabbits

Your Security Rabbits report for March 10, 2022

Hot topics

Nothing today

Source: Ransom Watch

Ransomware attacks

alphv Target: Carpenter & Zuckerman | cz . law(2022-03-08)

snatch Target: Warren Resources(2022-03-08)

snatch Target: Xtera(2022-03-08)

News

Cyware News - Latest Cyber News

Access:7 - Supply Chain Flaws Impacting IoT and Medical Devices
The seven flaws have been dubbed Access:7 and are present in PTC's Axeda agent, which is used for remote access and management of more than 150 connected devices across over 100 vendors.

Cyware News - Latest Cyber News

Adobe Patches 'Critical' Security Flaws in Illustrator, After Effects
The patches, scheduled as part of Adobe's Patch Tuesday release cycle, address a range of arbitrary code execution and memory leak vulnerabilities that could expose data to malicious hacker attacks.

Security Affairs

Anonymous hacked Russian cams, websites, announced a clamorous leak
The collective Anonymous has hacked public cameras in Russia and transmitted their live feed on a website, it also announced a clamorous leak. Anonymous and other hacker groups continue to target Russia, in a recent attack the collective has taken over more than 400 Russian cameras in support of Ukraine. The hacktivist shared the live feed […] The post Anonymous hacked Russian cams, websites, announced a clamorous leak appeared first on Security Affairs.

Threatpost

APT41 Spies Broke Into 6 US State Networks via a Livestock App
The China-affiliated state-sponsored threat actor used Log4j and zero-day bugs in the USAHerds animal-tracking software to hack into multiple government networks.

Cyware News - Latest Cyber News

Attackers Exploit Flaw in Mitel Systems to Launch Terabyte Scale DDoS Attack in the Wild
The flaw resides in around 2,600 incorrectly provisioned Mitel MiCollab and MiVoice Business Express systems that act as PBX-to-internet gateways and have a test mode that should not be exposed to the internet.

CyberScoop

Biden signs executive order on digital assets, including security measures
The White House says the executive order "the first ever, whole-of-government approach" to cryptocurrencies and other digital assets. The post Biden signs executive order on digital assets, including security measures appeared first on CyberScoop.

Cyware News - Latest Cyber News

Charity scams target people's generosity amid Russia-Ukraine conflict
To guard against the attacks, SingCert urged the public to practice good cyber hygiene habits like checking links before clicking on them and verifying attachments before downloading them.

Cyware News - Latest Cyber News

Chinese Hackers Target U.S. Gmail Users
Google's TAG warned several Gmail users of being targeted in phishing campaigns performed by a Chinese hacking group. The warnings came after Gmail's defenses automatically blocked the emails.

Cyware News - Latest Cyber News

CISA updates Conti ransomware alert with nearly 100 domain names
The federal agency notes that while the domains have been used in malicious operations, some of them may be abandoned or may share similar characteristics coincidentally.

The Hacker News

Critical Bugs Could Let Attackers Remotely Hack, Damage APC Smart-UPS Devices
Three high-impact security vulnerabilities have been disclosed in APC Smart-UPS devices that could be abused by remote adversaries as a physical weapon to access and control them in an unauthorized manner. Collectively dubbed TLStorm, the flaws "allow for complete remote takeover of Smart-UPS devices and the ability to carry out extreme cyber-physical attacks," Ben Seri and Barak Hadad,

Cyware News - Latest Cyber News

Cybercriminals Use War as a Lure for Malware Propagation
Since March 1, two phishing campaigns have been using the war theme to gain remote access, perform network reconnaissance, pilfer sensitive information, disable security software, and make space for further payloads.

Cyware News - Latest Cyber News

DDoS Ransomware Actors Target Website with 2.5 Million Requests Per Second
Security researchers discovered DDoS ransomware actors, impersonating REvil, to extort from targeted companies and also impact their stock prices. A day after the attacks, the attackers sent 15 million requests to the same site with a new message that warned the CEO to tank the company's stock price by hundreds of millions in market cap. Organizations are suggested to invest sufficiently in their network security systems to stay protected.

IT Security Guru

DSbD claims UK is on the path to "cyber disaster"
Professor John Goodacre, challenge director - Digital Security by Design, UKRI, and Professor of Computer Architectures, The University of Manchester, told attendees at the last leg of the DSbD roadshow in Wales that the UK is on the path to "cyber disaster". He claimed that the current approach of discovering and patching vulnerabilities is growing […] The post DSbD claims UK is on the path to "cyber disaster" appeared first on IT Security Guru.

The Hacker News

Emotet Botnet's Latest Resurgence Spreads to Over 100,000 Computers
The insidious Emotet botnet, which staged a return in November 2021 after a 10-month-long hiatus, is once again exhibiting signs of steady growth, amassing a swarm of over 100,000 infected hosts for perpetrating its malicious activities. "While Emotet has not yet attained the same scale it once had, the botnet is showing a strong resurgence with a total of approximately 130,000 unique bots

Cyware News - Latest Cyber News

Excel Add-ins Deliver JSSLoader Malware
First observed in 2019, JSSLoader is used by the GOLD NIAGARA cybercrime group. An Excel add-in extends Excel functionality, typically uses the '.xll' file extension, and functions similar to a DLL.

Security Affairs

Google blocked China-linked APT31's attacks targeting U.S. Government
Google has blocked a phishing campaign conducted by China-linked group APT31 aimed at Gmail users associated with the U.S. government. Google announced to have blocked a phishing campaign originating conducted by China-linked cybereaspionage group APT31 (aka Zirconium, Judgment Panda, and Red Keres) and aimed at Gmail users associated with the U.S. government. The campaign took […] The post Google blocked China-linked APT31's attacks targeting U.S. Government appeared first on Security Affairs.

The Hacker

Hackers Abuse Mitel Devices to Amplify DDoS Attacks by 4 Billion Times
Threat actors have been observed abusing a high-impact reflection/amplification method to stage sustained distributed denial-of-service (DDoS) attacks for up to

Security Affairs

HP addressed 16 UEFI firmware flaws impacting laptops, desktops, PoS systems
Researchers disclosed 16 high-severity flaws in different implementations of Unified Extensible Firmware Interface (UEFI) firmware impacting multiple HP enterprise devices. Researchers from cybersecurity firm Binarly discovered 16

News

14 hours with a record-breaking amplification ratio of 4,294,967,296 to 1. The attack vector - dubbed TP240PhoneHome (CVE-2022-26143) - has been weaponized to launch significant DDoS attacks targeting broadband access ISPs, financial

Krebs on Security

Microsoft Patch Tuesday, March 2022 Edition

Microsoft on Tuesday released software updates to plug at least 70 security holes in its Windows operating systems and related software. For the second month running, there are no scary zero-day threats looming for Windows users (that we know of), and relatively few "critical" fixes. And yet we know from experience that attackers are already trying to work out how to turn these patches into a roadmap for exploiting the flaws they fix. Here's a look at the security weaknesses Microsoft says are most likely to be targeted first.

Security Affairs

Multiple Russian government websites hacked in a supply chain attack

Threat actors hacked Russian federal agencies' websites in a supply chain attack involving the compromise of a stats widget. Some Russian federal agencies' websites were compromised in a supply chain attack, threat actors compromised the stats widget used to track the number of visitors by several government agencies. Threat actors were able to deface the [...] The post Multiple Russian government websites hacked in a supply chain attack appeared first on Security Affairs.

Cyware News - Latest Cyber News

New Nokoyawa Ransomware Possibly Related to Hive

The relatively unknown Nokoyawa ransomware is likely connected with Hive, as the two families share some striking similarities in their attack chain, from the tools used to the order in which they execute various steps.

Cyware News - Latest Cyber News

Ragnar Locker Breached 52 Organizations and Counting, FBI Warns

The FBI issued an alert about the Ragnar Locker ransomware group that has claimed 52 entities as its victims across 10 critical infrastructure sectors in the U.S, so far. The IOCs in the alert has information from Bitcoin addresses where hackers collect the ransom to the email addresses of operators. The FBI also urges security professionals to share any related information, which can help others fend off the attack.

Threatpost

Russian APTs Furiously Phish Ukraine - Google

Also on the rise: DDoS attacks against Ukrainian sites and phishing activity capitalizing on the conflict, with China's Mustang Panda targeting Europe.

WeLiveSecurity

Securing healthcare: An IT health check on the state of the sector

No sector or organization is immune to rapidly escalating cyberthreats, but when it comes to healthcare, the stakes couldn't be higher The post Securing healthcare: An IT health check on the state of the sector appeared first on WeLiveSecurity

The Hacker News

The Incident Response Plan - Preparing for a Rainy Day

The unfortunate truth is that while companies are investing more in cyber defenses and taking cybersecurity more seriously than ever, successful breaches and ransomware attacks are on the rise. While a successful breach is not inevitable, it is becoming more likely despite best efforts to prevent it from happening. Just as it wasn't raining when Noah built the ark, companies must face the fact

The Hacker News

Ukrainian Hacker Linked to REvil Ransomware Attacks Extradited to United States

Yaroslav Vasinskyi, a Ukrainian national, linked to the Russia-based REvil ransomware group has been extradited to the U.S. to face charges for his role in carrying out the file-encrypting malware attacks against several companies, including Kaseya last July. The 22-year-old had been previously arrested in Poland in October 2021, prompting the U.S. Justice Department (DoJ) to file charges of

Cyware News - Latest Cyber News

Updated SharkBot Variant Makes its Way into Google Play Store

Researchers exposed cybercriminals distributing the SharkBot banking trojan via Google Play Store. The malware is using Automatic Transfer Systems (ATS) to transfer money by abusing the Accessibility permission on devices and grants itself additional required permissions. Smartphone users are requested to be careful with the type of apps they download from various app stores and perform additional checks, if not sure.

high-severity vulnerabilities in various implementations of Unified Extensible Firmware Interface (UEFI) firmware impacting multiple HP enterprise devices. An attacker can exploit these vulnerabilities to implant a firmware that survives [...] The post HP addressed 16 UEFI firmware flaws impacting laptops, desktops, PoS systems appeared first on Security Affairs.

Threatpost

Most ServiceNow Instances Misconfigured, Exposed

Customers aren't locking down access correctly, leading to ~70 percent of ServiceNow implementations tested by AppOmni being vulnerable to malicious data extraction.

Cyware News - Latest Cyber News

New attack bypasses hardware defenses for Spectre flaw in Intel and ARM CPUs

It is an extension of the 2017 Spectre version 2 attack, also known as Spectre-BTI (Branch Target Injection) and, just like Spectre v2, can result in the leak of sensitive information from the privileged kernel memory space.

Cyware News - Latest Cyber News

NVIDIA's Code Signing Certificates Stolen and Abused in Attacks

Lapsus$, responsible for the recent attack on Nvidia, reportedly released two of the company's old code-signing certificates, and threat actors have started abusing it. In some cases, the stolen certificates were used to sign Cobalt Strike beacons, Mimikatz, backdoors, and remote access trojans. Admins are suggested to configure Windows Defender Application Control policies to control NVIDIA drivers loaded into Windows OS.

CyberScoop

REvil member accused of Kaseya ransomware attack arraigned in Texas

Yaroslav Vasinskyi faces up to 115 years in jail. The post REvil member accused of Kaseya ransomware attack arraigned in Texas appeared first on CyberScoop.

CyberScoop

SEC weighs reporting requirements for publicly traded companies

The amendments follow a similar proposal the agency released last month aimed at tightening security for investment firms and advisers. The post SEC weighs reporting requirements for publicly traded companies appeared first on CyberScoop.

Cyware News - Latest Cyber News

Siemens Addresses Over 90 Vulnerabilities Affecting Third-Party Components

Siemens has released 15 new advisories to inform customers about more than 100 vulnerabilities affecting its products, including over 90 security flaws introduced by the use of third-party components.

Security Affairs

TLStorm flaws allow to remotely manipulate the power of millions of enterprise UPS devices

Three flaws in APC Smart-UPS devices, tracked as TLStorm, could be exploited by remote attackers to hack and destroy them. Researchers from IoT security company Armis have discovered three high-impact security flaws, collectively tracked as TLStorm, affecting APC Smart-UPS devices. The flaws can allow remote attackers to manipulate the power of millions of enterprise devices carrying out extreme [...] The post TLStorm flaws allow to remotely manipulate the power of millions of enterprise UPS devices appeared first on Security Affairs.

IT Security Guru

Up to 30% of WordPress plugin bugs don't get patched

A global leader in WordPress security and threat intelligence, Patchstack, recently released a whitepaper highlighting the sorry state of WordPress security in 2021. Reported vulnerabilities grew 150% in 2021 from the previous year. Perhaps most alarmingly, 29% of the critical flaws in WordPress plugins never received an update. WordPress is used in 43.2% of websites [...] The post Up to 30% of WordPress plugin bugs don't get patched appeared first on IT Security Guru.

IT Security Guru

US critical infrastructure hit by ransomware

A new FBI report has revealed that at least 52 critical national infrastructure (CNI) entities have been compromised by a ransomware variant. The FBI has claimed that organisations across 10 CNI sectors had been impact as of January this year.# Key sectors include manufacturing, financial services, government and IT. A prolific ransomware variant has compromised [...] The post US critical infrastructure hit by ransomware appeared first on IT Security Guru.

Twitter

Open Source CVEs

(CVE-2022-0265): Improper Restriction of XML External Entity Reference in hazelcast/hazelcast. Disclosed by , fixed by @hazelcast... #opensource #CVE #bugbounty #security #vulnerability

Remotely Alerts

Severity: | Existing CommBuffer checks in SmmEntryPo... | CVE-2021-38578 | Link for more:

NEW: CVE-2021-38577 Heap Overflow in BaseBmpSupportLib. Severity: CRITICAL

CVE

CVE-2022-0265 Improper Restriction of XML External Entity Reference in GitHub repository hazelcast/hazelcast prior to 5.1.

Remotely Alerts

Severity: | Improper Restriction of XML External Ent... | CVE-2022-0265 | Link for more:

Severity: | Heap Overflow in BaseBmpSupportLib.... | CVE-2021-38577 | Link for more:

Threat Intel Center

Threat Intel Center

NEW: CVE-2021-38577 Heap Overflow in BaseBmpSupportLib. Severity: CRITICAL

Threat Intel Center

NEW: CVE-2021-38577 Heap Overflow in BaseBmpSupportLib.

eyetsystems

CVE-2021-38577 Heap Overflow in BaseBmpSupportLib.

Nancy Pelosi

This historic legislation will carry major bipartisan legislation that has been in the making for years including reauthorization of the Violence Against Women Act & new cybersecurity protections to fight against cyber attacks to our infrastructure by Russia & other bad actors.

Remotely Alerts

CVE Analysis

CVE-2021-38577 #HarsiaInfo

Debra M. Fezza Reed #SecRiskRptSME

RT: CVE-2021-38577 Heap Overflow in BaseBmpSupportLib. CVE (@CVEnew) Mar 3, 2022

Hernan Espinoza

CVEnew: CVE-2021-38577 Heap Overflow in BaseBmpSupportLib.

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (20%)

Germany (11%)

Singapore (9%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (55%)

Ukraine (30%)

United States (5%)

Source: Hybrid Analysis

Top malicious URL

100%
Threat score

http://theirsmonopoly (.) top/omannairo/tb (.) php?ypqvxufq1646823884628

89%
Threat score

http://185 (.) 148 (.) 168 (.) 220:8080/

85%
Threat score

http://miharafuturelab (.) com/ (.) well-known/pki-validation/bidhistory/scriptaculous/index (.) php?semicrepe=10bseav56kgha7&episiohematoma=ophthalmodiastimete

84%
Threat score

http://159 (.) 69 (.) 237 (.) 188:443/

82%
Threat score

http://mail (.) gms (.) pwc (.) com/ls/click?upn=w2i3qkzj-2BZr7plnkJ5K3BdhHelFEBn83qG9SGC9-2Fmt3-2BLCvwmkEqCC40Q0HCOdNjyjqa2Tdh4TWx-2BzmRO-2Fitp5E197cqn8Bbt53wwBUFEu5n8MnH2wTyfNGnRRvFUkCxkFA-2B2UWSfbk-2Bbag5-2B5ZkPmutDIHykdw-2Bxf-2B5kcrYMl4-3Dzo_A_IqFiwqbfFz6tQ-2FquBMtnxIr3e7t7i6TYkmIwv93eB0GGOONq2bIt2eIwWEpWYbYilJkC3zDb1VpVIW-2FDbx0zC1cTnwPyYvk6bveZSTUcC3X0rk9-2B5CunUEwfhagpaYdRZuHayK-2BT1Mf
2F8r21oAufuj1lMuKUQywtbOmAqrj6lu3KxcnkonHv0WTxXyhL6Z6rVr4liHdl5ygJzLnMpj3J0ivsgZZT-2B-2BVn-2BivqmaClas2XuQvF4w8cFH6sD1IH5S2gNKT5XpyBTa6qH
2Bt53R2m9ZMvwgbkmIo6-2FjXs-2FWIXHslCMM5eFDTl9CYea-2By9TnBh7jibPcUdX2dbX9OY4uB24UtOd-2FeHRHzbBGNO5KiiZc-2FVpueV1se3SGkozV53OvyZssV8Qm
2BCv8PHALHCPEBQCEDBRZIEl9EIVOSHn4uNF7aVs1pPRo9C1Pao1ijliPgxv2kauf-2FX1JEiVIYJUiGUd-2BvNQXAnG0a3HWhdmImhgEGWnQ2CABJBbSHCu7zikYDK8bJs
2FSOoz8f9awG9ll7NVGy9bpzCf7K2GdWteHIUd

81%
Threat score

https://euroexpressonline (.) xyz/systemmonitor20022/imming_control_930393903223 (.) php?Email=mauroicev%40societe (.) com

79%
Threat score

https://dhbhbdc (.) r (.) af (.) d (.) sendibt2 (.) com/

78%
Threat score

http://inail (.) greek-books (.) gr/bGl2b3Jub0BpbmFpbC5pdA==&data=04%7C01%7Clivorno@inail (.) it%7Cad8448f9e6c7492b8fb008da02826883%7C418322d35401446f99969e2e03ee3a5e%7C0%7C0%7C637825056717252344%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAw

77%
Threat score

http://hautarztzentrum-gummersbach (.) de/assets/witsec-mailform/mailform (.) js

72%
Threat score

http://ao-litija (.) si/

72%
Threat score

https://tinyurl (.) su/h861999728/

72%
Threat score

http://www (.) mountainhostel (.) com/

Source: NIST

NIST CVE: Critical

CVE-2021-38578

Existing CommBuffer checks in SmmEntryPoint will not catch underflow when computing BufferSize.

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

CVE-2022-0265

Improper Restriction of XML External Entity Reference in **GitHub** repository hazelcast/hazelcast prior to 5.1.

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

CVE-2021-38577

Heap Overflow in BaseBmpSupportLib.

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

Source: NIST

NIST CVE: High

CVE-2021-26259

A flaw was found in **htmldoc** in v1.9.12. Heap buffer overflow in render_table_row(),in ps-pdf.cxx may lead to arbitrary code execution and denial of service.

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

CVE-2021-26948

Null pointer dereference in the **htmldoc** v1.9.11 and before may allow attackers to execute arbitrary code and cause a denial of service via a crafted html file.

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

CVE-2021-3623

A flaw was found in **libtpms**. The flaw can be triggered by specially-crafted TPM 2 command packets containing illegal values and may lead to an out-of-bounds access when the volatile state of the TPM 2 is marshalled/written or unmarshalled/read. The highest threat from this vulnerability is to system availability.

HIGH Vector: network Created: 2022-03-02 Updated: 2022-03-10

Source: NIST

NIST CVE: Medium

CVE-2022-23710

A cross-site-scripting (XSS) vulnerability was discovered in the Data Preview Pane (previously known as Index Pattern Preview Pane) which could allow arbitrary JavaScript to be executed in a victim's browser.

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

CVE-2022-25220

PeteReport Version 0.5 allows an authenticated admin user to inject persistent JavaScript code inside the **markdown** descriptions while creating a product, report or finding.

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

CVE-2022-25138

Axelor Open Suite v5.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Name parameter.

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

CVE-2022-24723

URI.js is a Javascript URL mutation library. Before version 1.19.9, whitespace characters are not removed from the beginning of the protocol, so URLs are not parsed properly. This issue has been patched in version 1.19.9. Removing leading whitespace from values before passing them to URI.parse can be used as a workaround.

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

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-38296

Apache Spark supports end-to-end encryption of RPC connections via "spark.authenticate" and "spark.network.crypto.enabled". In versions 3.1.2 and earlier, it uses a **bespoke** mutual authentication protocol that allows for full encryption key recovery. After an initial interactive attack, this would allow someone to decrypt plaintext traffic offline. Note that this does not affect security mechanisms controlled by "spark.authenticate.enableSaslEncryption", "spark.io.encryption.enabled", "spark.ssl", "spark.ui.strictTransportSecurity". Update to Apache Spark 3.1.3 or later

UNRATED Vector: unkown Created: 2022-03-10 Updated: 2022-03-10

CVE-2022-0890

NULL Pointer Dereference in **GitHub** repository mruby/mruby prior to 3.2.

UNRATED Vector: unkown Created: 2022-03-10 Updated: 2022-03-10

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

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

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

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

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

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

Source: SpamHaus

Top countries with botnet

#1 China

#2 India

#3 United States of America

#4 Thailand

#5 Indonesia

#6 Algeria

#7 Viet Nam

#8 Brazil

#9 Iran (Islamic Republic of)

#10 Pakistan

Source: SpamHaus

Top phishing countries

#1 United States

#2 Germany

#3 Iran

#4 Russia

#5 Netherlands

#6 Singapore

#7 Belgium

#8 Hong Kong

#9 France

#10 Bulgaria

Source: Hybrid Analysis

Top malicious files

100% Threat score	58449491b26acb660888a2387610c28211575007fed33d3d979d36ffc3effb24 (.) exe
100% Threat score	da0e01d3ae7432cf852122b9d5369c75dc5a1a04ec601b218
100%	DEVOLUCIÃ“N DE PAGO (.) PDF (.) exe
100%	55161ff4f1bc162ddbbead231ebc7a95e522833163f8c5bc3fc

Threat score	
100% Threat score	post_MULTI_MIX_HEAVY_413ebd37620cfcb229322a0f3217ae8a6a61163eb73b14a30e3d8d5a68847f1b_0 (.) exe
100% Threat score	0000000508 (.) pdf (.) exe
100% Threat score	30b41335dc285ef66c5609133a26790e4e2d3bbb23e0a4fe11180b04c46e49cd
100% Threat score	4208433292605d930948527220d3791fda7af1d00ab7765853ff098116a75ef5
100% Threat score	a1 (.) ocx
100% Threat score	8a1cfc683ee4328f2bf3c5966c23b1c2
90% Threat score	midotsvc (.) dll
77% Threat score	224NOFEo040009 (.) doc
75% Threat score	1ClickSearch (.) exe
75% Threat score	installer (.) exe

Threat score	sample
100% Threat score	d3fe483e5a42de0b80bc3da74c83dd059ae24babcdfe52c31f
100% Threat score	64a3a3ec70d20636299b8fe4f50c2b4d077f9934ee2d6ccf7d4
100% Threat score	Scan_Payment Copy (.) (.) (.) (.) Pdf (.) exe
100% Threat score	454292D8865B5992C2A423DA68C743C501E8EC45B6984B
100% Threat score	f65fa71e8ffe11bb6e7c6c84c3d365f4fe729e1e9c38cb4f073d
100% Threat score	ADNOC BOQ's AND SPECIFICATIONS (.) exe
80% Threat score	CineTrak Your Movie and TV Show Diary v0 (.) 8 (.) 2 Premi {CracksHash} (.) apk
75% Threat score	Inquiry for Uzbekistan (.) exe
75% Threat score	Online Banking Payment Advice (.) pdf (.) exe
75% Threat score	PMSetup_5 (.) 22 (.) 102 (.) msi

Source: Imperva DDOS Map

Top DDOS techniques

83%	**DDoS**
9%	**Automated Threat**
8%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

60%	**Financial Services**
31%	**Business**
2%	**Computing & IT**