Security Rabbits

Your Security Rabbits report for March 17, 2022

Source: Ransom Watch

Ransomware attacks

alphv	Target: M . T . B . (2022-03-17)
lockbit2	Target: sbctanzania . co . . . . (2022-03-17)
lockbit2	Target: rebuildingtoget . . . (2022-03-17)
conti	Target: Milan Institute(2022-03-17)
pandora	Target: Jaffe Raitt Heuer & Weiss, P . C . (2022-03-17)
pandora	Target: GlobalWafers Japan(2022-03-17)
lockbit2	Target: www . onedoc . ch/f . . . (2022-03-17)
conti	Target: AllOffice(2022-03-17)
lockbit2	Target: www . comune . vill . . . (2022-03-16)
lockbit2	Target: taguefamilyprac . . . (2022-03-16)
lockbit2	Target: drory . com . cn(2022-03-16)
lockbit2	Target: vvrmc . org | Par . . . (2022-03-17)
pandora	Target: Rosewd(2022-03-17)
lockbit2	Target: onedoc . ch/fr/ca . . . (2022-03-17)
conti	Target: Managed Business Solutions(2022-03-17)
conti	Target: IMT GROUP(2022-03-17)
conti	Target: Empire Electronics Inc . (2022-03-17)
lockbit2	Target: comune . villafra . . . (2022-03-17)
lockbit2	Target: www . rebuildingt . . . (2022-03-16)
lockbit2	Target: vbsharma . ca(2022-03-16)
lockbit2	Target: matteolisrl . it(2022-03-16)
alphv	Target: Bullfrog International | bullfrogspas . com(2022-03-16)

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

'CryptoRom' Crypto Scam is Back via Side-Loaded Apps
Online scammers are bypassing Apple's App Store security, stealing thousands of dollars' worth of cryptocurrency from the unwitting, using the TestFlight and WebClips programs.

Threatpost

Another Destructive Wiper Targets Organizations in Ukraine
CaddyWiper is one in a barrage of data-wiping cyber-attacks to hit the country since January as the war on the ground with Russia marches on.

Naked Security

Beware bogus Betas - cryptocoin scammers abuse Apple's TestFlight system
"Install this moneymaking app" - this one is so special that it isn't available on Google Play or the App Store!

Naked Security

CISA warning: "Russian actors bypassed 2FA" - what happened and how to avoid it
Don't leave old accounts lying around where someone sketchy could reactivate them.

Cyware News - Latest Cyber News

Emotet malware campaign impersonates the IRS for 2022 tax season
In a new report by email security firm Cofense, researchers have spotted multiple phishing campaigns impersonating the Internet Revenue Service (IRS.gov) that use lures related to the 2022 U.S. tax season.

Cyware News - Latest Cyber News

FBI Warns of MFA Flaw used by Nation-State Hackers for Lateral Movement
The FBI says Russian state-backed hackers gained access to an NGO cloud after enrolling their own device in the organization's Duo MFA following the exploitation of misconfigured default MFA protocols.

Threatpost

'CryptoRom' Crypto-Scam is Back via Side-Loaded Apps
Scammers are bypassing Apple's App Store security, stealing thousands of dollars' worth of cryptocurrency from the unwitting, using the TestFlight and WebClips programs.

CyberScoop

Automotive parts maker Denso confirms cyberattack
The attack was related to its German operations, the company said. The post Automotive parts maker Denso confirms cyberattack appeared first on CyberScoop.

Security Affairs

CISA adds 15 new flaws to the Known Exploited Vulnerabilities Catalog
The US Cybersecurity and Infrastructure Security Agency (CISA) added 15 new flaws to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added 15 vulnerabilities to its Known Exploited Vulnerabilities Catalog. According to Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, FCEB agencies have to address the […] The post CISA adds 15 new flaws to the Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

Cyware News - Latest Cyber News

Conti Leaks Exposes its Organizational Structure, Source Code, and Operational Details
The recent leak of Conti source code, chat logs, and other sensitive records have unfolded several secrets of the group. Different researchers studied the findings and laid down their analysis. According to Chainanysis, Conti extorted an estimated $180m last year, making it the top gainer for ransomware operations in 2021. The recent leak of Conti secrets turns out to be a blessing for security researchers tracking the group as it offers insights into the group's activity.

CyberScoop

Emotet's tax-season phishing is back with new tricks
Researchers at Cofense say the operators behind the Emotet botnet "have upped their game" for 2022's tax season. The post Emotet's tax-season phishing is back with new tricks appeared first on CyberScoop.

The Hacker News

FBI, CISA Warn of Russian Hackers Exploiting MFA and PrintNightmare Bug
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have released a joint advisory warning that Russia-backed threat actors hacked the network of an unnamed non-governmental entity by exploiting a combination of flaws. "As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default [

Cyware News - Latest Cyber News

Fraudsters use intelligent bots to attack financial institutions

Intelligent automated bots are among the newest weapons in the arsenal of cyber criminals, including those seeking to attack financial institutions, as fraud and intrusions increase exponentially on this attack vector.

Cyware News - Latest Cyber News

Google Patches Critical Vulnerability With Chrome 99 Update

The critical flaw, tracked as CVE-2022-0971, has been described as a use-after-free issue affecting the Blink Layout component. Sergei Glazunov of Google Project Zero has been credited for reporting the flaw.

Cyware News - Latest Cyber News

LokiLocker Ransomware-as-a-Service Targets English-speaking Victims and Windows Systems

BlackBerry Threat Intelligence has identified a new Raas family, and tracked its lineage to its probable beta stage release. LokiLocker encrypts your files and will render your machine unusable if you don't pay up in time.

Cyware News - Latest Cyber News

Mobile Threats Hit the Roof

In 2021, 30% of known zero-day vulnerabilities targeted mobile devices, while there was a 466% rise in exploited zero-day vulnerabilities against mobile endpoints, according to Zimperium.

The Hacker News

New Infinite Loop Bug in OpenSSL Could Let Attackers Crash Remote Servers

The maintainers of OpenSSL have shipped patches to resolve a high-severity security flaw in its software library that could lead to a denial-of-service (DoS) condition when parsing certificates. Tracked as CVE-2022-0778 (CVSS score: 7.5), the issue stems from parsing a malformed certificate with invalid explicit elliptic-curve parameters, resulting in what's called an "infinite loop." The flaw

Cyware News - Latest Cyber News

NSA and CISA: Here's how to improve your Kubernetes cluster security

The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have published updated guidance about how to harden Kubernetes for managing container applications.

Security Affairs

Russia's disinformation uses deepfake video of Zelenskyy telling people to lay down arms

Russian disinformation continues, this time it used a deepfake video of Zelenskyy inviting Ukrainians to 'lay down arms.' A deepfake video of the Ukrainian president Volodymyr Zelenskyy telling its citizens to lay down arms is the last example of disinformation conducted by Russia-linked threat actors. The fake video shows President Zelenskyy saying 'It turned out [...] The post Russia's disinformation uses deepfake video of Zelenskyy telling people to lay down arms appeared first on Security Affairs.

Cyware News - Latest Cyber News

Sioux Falls Funds DSU Cybersecurity Lab

Sioux Falls City Council has approved a $10m appropriation toward a Dakota State University (DSU) cybersecurity lab. The funding for the project, which could bring 650 jobs to the Sioux Falls and Madison areas, was approved by a unanimous vote.

Cyware News - Latest Cyber News

This sneaky type of phishing is growing fast because hackers are seeing big paydays

These conversation hijacking attacks have the potential to be more effective because the source of the email is someone the victim trusts and the message comes as part of an ongoing thread.

The Hacker News

TrickBot Malware Abusing Hacked IoT Devices as Command-and-Control Servers

Microsoft on Wednesday detailed a previously undiscovered technique put to use by the TrickBot malware that involves using compromised Internet of Things (IoT) devices as a go-between for establishing communications with the command-and-control (C2) servers. "By using MikroTik routers as proxy servers for its C2 servers and redirecting the traffic through non-standard ports, TrickBot adds

The Hacker News

Unpatched RCE Bug in dompdf Project Affects HTML to PDF Converters

Researchers have disclosed an unpatched security vulnerability in "dompdf," a PHP-based HTML to PDF converter, that, if successfully exploited, could lead to remote code execution in certain configurations. "By injecting CSS into the data processed by dompdf, it can be tricked into storing a malicious font with a .php file extension in its font cache, which can later be executed by accessing it

Cyware News - Latest Cyber News

Watch Out! BazarBackdoor is Abusing Website Contact Forms

Recently, the BazarBackdoor malware was observed spreading via corporate website contact forms rather than its typical phishing email attack chain target firms. To avoid any possible security flag, the attackers use file-sharing services TransferNow and WeTransfer to send malicious files. Website admins are suggested to stay alert whenever receiving suspicious emails from unknown sources.

IT Security Guru

German government warns against using Kaspersky

The German BSI has warned against the use of Kaspersky antivirus security products as the company is headquartered in Russia. The BSI suggested moving away from any Kaspersky product to another vendor, as the company may be forced to carry out offensive cyber operations by the Russian state. The BBC translated the BSI announcement: "A [...] The post German government warns against using Kaspersky appeared first on IT Security Guru.

ZDNet | security RSS

iPhone, Android users lose life savings to romance fraud, cryptocurrency operation

Attackers now 'double dip' to clear out victim bank accounts.

Cyware News - Latest Cyber News

Massive phishing campaign uses 500+ domains to steal credentials

Large-scale phishing activity using hundreds of domains to steal credentials for Naver, a Google-like online platform in South Korea, shows infrastructure overlaps linked to the TrickBot botnet.

The Hacker News

New "B1txor20" Linux Botnet Uses DNS Tunnel and Exploits Log4J Flaw

A previously undocumented backdoor has been observed targeting Linux systems with the goal of corralling the machines into a botnet and acting as a conduit for downloading and installing rootkits. Qihoo 360's Netlab security team called it B1txor20 "based on its propagation using the file name 'b1t,' the XOR encryption algorithm, and the RC4 algorithm key length of 20 bytes."

The Hacker News

New Vulnerability in CRI-O Engine Lets Attackers Escape Kubernetes Containers

A newly disclosed security vulnerability in the Kubernetes container engine CRI-O called cr8escape could be exploited by an attacker to break out of containers and obtain root access to the host. "Invocation of CVE-2022-0811 can allow an attacker to perform a variety of actions on objectives, including execution of malware, exfiltration of data, and lateral movement across pods," CrowdStrike

Security Affairs

Russia-linked threats actors exploited default MFA protocol and PrintNightmare bug to compromise NGO cloud

FBI and CISA warn Russia-linked threats actors gained access to an NGO cloud after enrolling their own device in the organization's Duo MFA. The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) warned that Russia-linked threat actors have gained access to a non-governmental organization (NGO) cloud by exploiting misconfigured default multifactor [...] The post Russia-linked threats actors exploited default MFA protocol and PrintNightmare bug to compromise NGO cloud appeared first on Security Affairs.

Cyware News - Latest Cyber News

Severe Vulnerability Patched in CRI-O Container Engine for Kubernetes

A severe vulnerability affecting the CRI-O container engine for Kubernetes could be exploited to escape the container and gain root access to the host, CrowdStrike reports.

IC3.gov News

Technical and Customer Support Fraud

Blog â€“ Flashpoint

Top 7 Cyber Threats to the Financial Services Sector in 2022

The financial cyber threat landscape In our latest report, we detail seven primary cyber threats that organizations across the financial services sector will face in 2022. Some of them, such as ransomware, are not new but nevertheless remain a serious threat. Others, such as decentralized finance (DeFi) and cryptocurrencies, are newer, so to speak, and [...] The post Top 7 Cyber Threats to the Financial Services Sector in 2022 appeared first on Flashpoint.

The Hacker News

Ukraine Secret Service Arrests Hacker Helping Russian Invaders

The Security Service of Ukraine (SBU) said it has detained a "hacker" who offered technical assistance to the invading Russian troops by providing mobile communication services inside the Ukrainian territory. The anonymous suspect is said to have broadcasted text messages to Ukrainian officials, including security officers and civil servants, proposing that they surrender and take the side of

WeLiveSecurity

US military vs. Silicon Valley - a cultural divide

The US military knows it needs to speed up technology adoption through optimization, something at the heart of Silicon Valley culture The post US military vs. Silicon Valley - a cultural divide appeared first on WeLiveSecurity

Twitter

Rep. Val Demings

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

Gary Gensler

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

Dave Rubin

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

Spiros Margaris

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

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

CVE-2022-24931

Improper access control vulnerability in dynamic **receiver** in ApkInstaller prior to SMR MAR-2022 Release allows unauthorized attackers to execute arbitrary activity without a proper permission

HIGH Vector: local Created: 2022-03-10 Updated: 2022-03-17

CVE-2022-24644

ZZ Inc. KeyMouse **Windows** 3.08 and prior is affected by a remote code execution vulnerability during an unauthenticated update. To exploit this vulnerability, a user must trigger an update of an affected installation of KeyMouse.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-17

CVE-2022-24732

Maddy **Mail** Server is an open source **SMTP** compatible email server. Versions of maddy prior to 0.5.4 do not implement password expiry or account expiry checking when authenticating using PAM. Users are advised to upgrade. Users unable to upgrade should manually remove expired accounts via existing filtering mechanisms.

HIGH Vector: network Created: 2022-03-09 Updated: 2022-03-17

Source: NIST

NIST CVE: Medium

CVE-2022-24932

Improper Protection of Alternate Path vulnerability in Setup wizard process prior to SMR Mar-2022 Release 1 allows physical attacker package installation before finishing Setup wizard.

MEDIUM Vector: physical Created: 2022-03-10 Updated: 2022-03-17

Source: NIST

NIST CVE: Low

CVE-2022-24930

An Improper access control vulnerability in StRetailModeReceiver in Wear OS 3.0 prior to Firmware update MAR-2022 Release allows untrusted applications to reset default app settings without a proper permission

LOW Vector: local Created: 2022-03-10 Updated: 2022-03-17

Source: NIST

NIST CVE: Unrated

CVE-2022-22273

** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure **Remote Access** (SRA) products and older firmware versions of **Secure Mobile Access** (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-26534

FISCO-BCOS release-3.0.0-rc2 was discovered to contain an issue where a malicious node, via a malicious viewchange packet, will cause normal nodes to change view excessively and stop generating blocks.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-25516

stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function stbtt__find_table at stb_truetype.h.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-25514

stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function ttUSHORT() at stb_truetype.h.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-24073

The Web Request API in **Whale** browser before 3.12.129.18 allowed to deny access to the extension store or redirect to any URL when users access the store.

CVE-2022-26300

EOS v2.1.0 was discovered to contain a heap-buffer-overflow via the function txn_test_gen_plugin.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2021-42219

Go-Ethereum v1.10.9 was discovered to contain an issue which allows attackers to cause a denial of service (DoS) via sending an excessive amount of messages to a node. This is caused by missing memory in the component /ethash/algorithm.go.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-25515

stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function ttULONG() at stb_truetype.h.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-24072

The devtools API in **Whale** browser before 3.12.129.18 allowed extension developers to inject arbitrary JavaScript into the extension store web page via devtools.inspectedWindow, leading to extensions downloading and uploading when users open the developer tool.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-24074

Whale Bridge, a default extension in Whale browser before 3.12.129.18, allowed to receive any SendMessage request from the content script itself that could lead to controlling Whale Bridge if the rendering

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

CVE-2022-24075

Whale browser before 3.12.129.18 allowed extensions to replace JavaScript files of the HWP viewer website which could access to local HWP files. When the HWP files were opened, the replaced script could read the files.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

process compromises.

UNRATED Vector: unkown Created: 2022-03-17 Updated: 2022-03-17

Source: Hybrid Analysis

Top malicious files

100%
Threat score
Rundll32 (.) exe

100%
Threat score
Josho (.) x86

100%
Threat score
SAUY_901780065432 (.) exe

100%
Threat score
Address and payment info (.) xlsm

100%
Threat score
800MT Purchase LOI (.) exe

100%
Threat score
Payment_Advice (.) exe

100%
Threat score
20220316_395254_009 (.) xlsm

91%
Threat score
Pokyny (.) docm

80%
Threat score
Type32install (.) exe

80%
Threat score
Aktuelt (.) aspx

75%
Threat score
esta (.) pdf

75%
Threat score
ArmouryCrateInstaller (.) exe

Source: Hybrid Analysis

Top malicious URL

100%
Threat score
https://gayapinddaanpandit (.) com/css/asballantine/index (.) php

87%
Threat score
http://r (.) sender (.) mea-finance (.) com/mk/cl/f/ulfQUKgBiiqwgBBnnUSg4Lu9aUn3ZTELLkrXGLfMWhWOoJ0S-MH46Z7ajxuqDyQgqrRRbpkUFnTzWsnlR7813u9DZozzx0fiUgcKjKcOyPTsQpYvinvB9HkmiXrQNCKdFbuoQASkgr5QOJYDYvtYDvkWXYnXxHc-V-7qXj0anMiGOMgc4R9svp3A-pzE-SUsUrBa7u73TJo-B44P7reLqP2cndMCMi0I2awlgmEbXppTSMkjnU35AEuNy-UIZhVoKBznM2oQSTAZTf9w3Fxuuh9bn-vmeTJpAnUPcDAK2vt286OOPxUegGXT2_dpytgTZKgBwgXbtI0BLGoMlhxdJVNIVAA-3ZnR-3tf2svVDO6vE2M

82%
Threat score
http://ethhex (.) com/

77%
Threat score
http://u (.) k5t (.) brlnet (.) in/? (.) # (.) gmlueul (.) aHR0cHM6Ly9zcHVyaW91cy1mbHV0dGVyaW5nLW93bmVyLmdsaXRjaC5tZS91cGRhdGUuaHRtbCNzdGV2ZW4udHlsZXJAaW5zaWdodC5jb20%3D

77%
Threat score
http://sandelf (.) com/r/p (.) html?f=jiuquttt&e=1315302425164

74%
Threat score
https://auto-kontent (.) ru/

91%
Threat score
http://103 (.) 136 (

86%
Threat score
http://ccalaire (.) c

79%
Threat score
https://rlpromotion

77%
Threat score
http://sofia (.) ager
co/AgentiNSlive/vi

77%
Threat score
http://www (.) icsp

72%
Threat score
http://www (.) echo
com/d1r/cm9tYWx

Source: SpamHaus

Top spamming countries

#1 United States of America

#2 China

#3 Russian Federation

#4 Mexico

#5 Dominican Republic

#6 Saudi Arabia

#7 India

#8 Brazil

#9 Japan

#10 Uruguay

Source: SpamHaus

Top spammers

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

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

#3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of inexpensive, automated

VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.

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

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

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

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

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

#9 **Richpro Trade Inc. / Richvestor GmbH**
Uses botnets or hires botnet spammers to send spam linking back to suspect investment, "quack-health-cures" and other sites that he owns or is an affiliate of. Botnet spamming and hosting sites on hacked servers is fully criminal in much of the world. Managed or owned by a Timo Richert.

Source: SpamHaus

Top countries with botnet

#1 China

#2 India

#3 United States of America

#4 Thailand

#5 Indonesia

#6 Algeria

#7 Viet Nam

#8 Brazil

#9 Iran (Islamic Republic of)

#10 Japan

Source: SpamHaus

Top phishing countries

#1 United States

#2 Singapore

#3 Germany

#4 Japan

#5 Netherlands

#6 Russia

#7 United Kingdom

#8 Bulgaria

#9 France

#10 India

Source: Have I been pwned?

Have I been pwnd

CDEK (cdek.ru)
In early 2022, a collective known as IT Army whose stated goal is to "completely de-anonymise most Russian users by leaking hundreds of gigabytes of databases" published over 30GB of data allegedly sourced from Russian courier service CDEK. The data contained over 19M unique email addresses along with names and phone numbers. The authenticity of the breach could not be independently established and has been flagged as "unverfieid".

Count: 19218203 Created: 2022-03-09 Updated: 2022-03-17

Source: Imperva DDOS Map

Top DDOS attackers

United States (21%)

Germany (12%)

Russia (11%)

Source: Imperva DDOS Map

Top DDOS country targets

🇷🇺	**Russia (65%)**
🇺🇦	**Ukraine (18%)**
🇺🇸	**United States (7%)**

Source: Imperva DDOS Map

Top DDOS techniques

84%	**DDoS**
11%	**Automated Threat**
5%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

68%	**Financial Services**
21%	**Business**
4%	**Computing & IT**