Understanding Cybercrime

OCTOBER 24, 2018

Rebecca Ledingham, Vice President Cyber & Intelligence

Melanie Gersten, Director Cyber & Intelligence

mastercard.

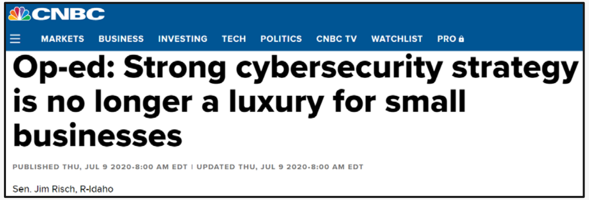
Statement of Confidentiality and Disclaimer

Confidentiality The information contained in these presentations is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both. This material may not be duplicated, published, shared with a third party, or otherwise disclosed, in whole or in part, without the prior written permission of Mastercard. These presentations are intended solely to facilitate discussion between the parties.

Trademarks Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States. All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of these presentations. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to these presentations and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

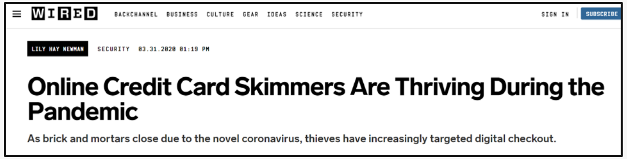
Why is your Small Business a Target?



Op-ed: Strong cybersecurity strategy is no longer a luxury for small businesses

PUBLISHED THU, JUL 9 2020-8:00 AM EDT | UPDATED THU, JUL 9 2020-8:00 AM EDT

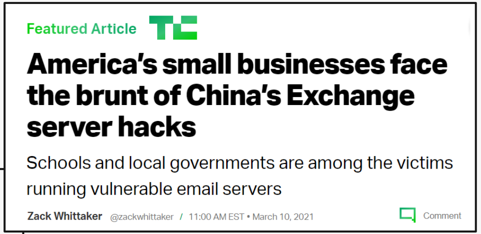
Sen. Jim Risch, R-Idaho



LILY HAY NEWMAN SECURITY 03.31.2020 01:19 PM

Online Credit Card Skimmers Are Thriving During the Pandemic

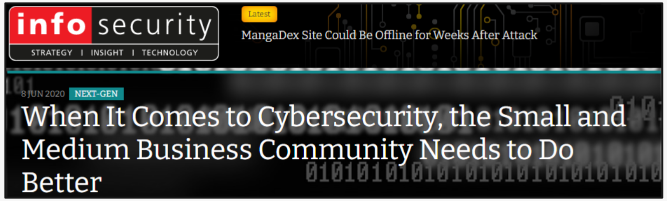
As brick and mortars close due to the novel coronavirus, thieves have increasingly targeted digital checkout.



America's small businesses face the brunt of China's Exchange server hacks

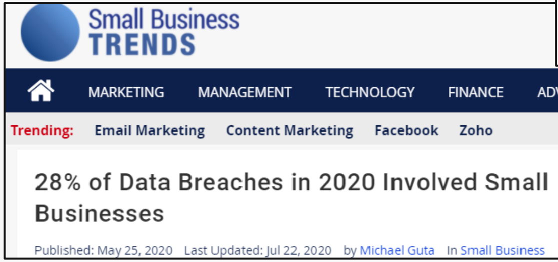
Schools and local governments are among the victims running vulnerable email servers

Zack Whittaker @zackwhittaker / 11:00 AM EST • March 10, 2021


info security
STRATEGY | INSIGHT | TECHNOLOGY
Latest
MangaDex Site Could Be Offline for Weeks After Attack
NEXT-GEN

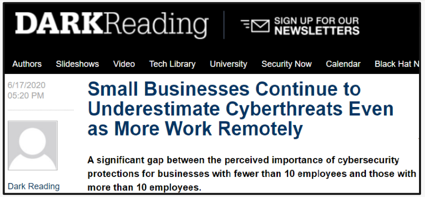
8 JUN 2020

When It Comes to Cybersecurity, the Small and Medium Business Community Needs to Do Better



28% of Data Breaches in 2020 Involved Small Businesses

Published: May 25, 2020 Last Updated: Jul 22, 2020 by Michael Guta In Small Business



6/17/2020 05:20 PM

Dark Reading

Small Businesses Continue to Underestimate Cyberthreats Even as More Work Remotely

A significant gap between the perceived importance of cybersecurity protections for businesses with fewer than 10 employees and those with more than 10 employees.

CYBER READINESS INSTITUTE

- 89% of small businesses moving to a remote workforce during Covid-19 stay-at-home orders
- 35% of small businesses with fewer than 10 employees do not have an incident response policy.
- 49% of small businesses will still maintain at least a partial remote workforce after Covid-19 restrictions are lifted.
- More than 42% of businesses have provided additional password training or policies over the past two months.
- 30% of small businesses have used new free cybersecurity tools since work-at-home orders began.
- 25% of small business owners anticipate hiring new cybersecurity staff or consultants over the next six months.

What is Cybercrime?

Anything

- Extortion
- Personal Data Breach
- No Lead Value
- Non-Payment Delivery
- Phishing/ Vishing
- Real Estate/Rental
- Government Impersonation
- Health Care Related
- Gambling
- Hacktivism

And

- BEC
- Romance Fraud
- Trolling
- Advanced Fee
- Identify Theft
- Spoofing
- Overpayment
- Employment
- Tech Support
- Lottery
- Misrepresentation

Everything

- Investment
- Malware/Virus
- Corporate Data Breach
- Counterfeit
- Denial of Service
- Ransomware
- Crimes Against Children
- Re-shipping
- Civil matter
- Charity
- Terrorism

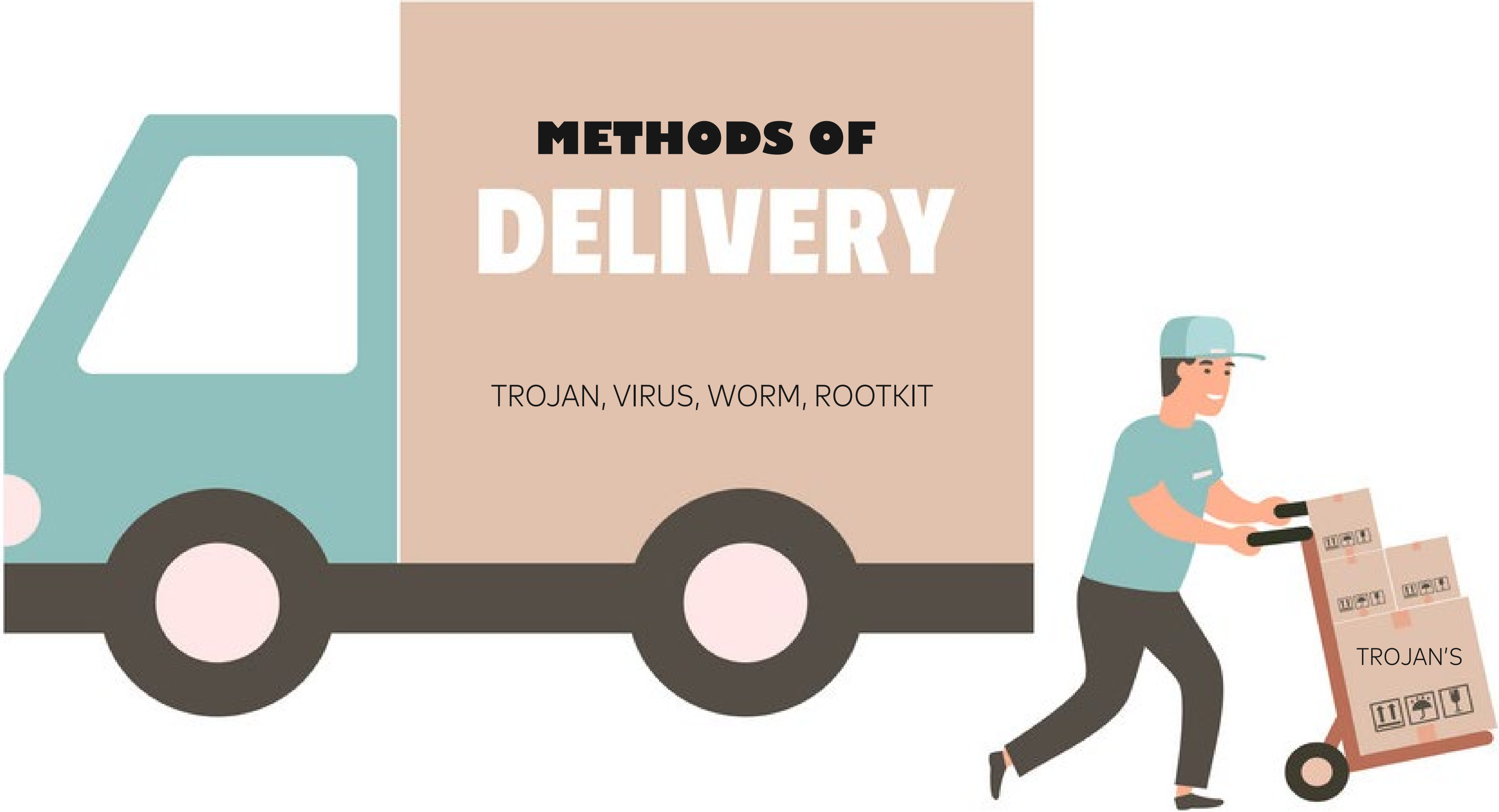
Cyber Big Bang Theory

How it all began

USER
VIRUS
FRAUD
WORM
DANGER!!!
INTERNET!!!
SPAM
TROJAN

METHODS OF DELIVERY

TROJAN, VIRUS, WORM, ROOTKIT



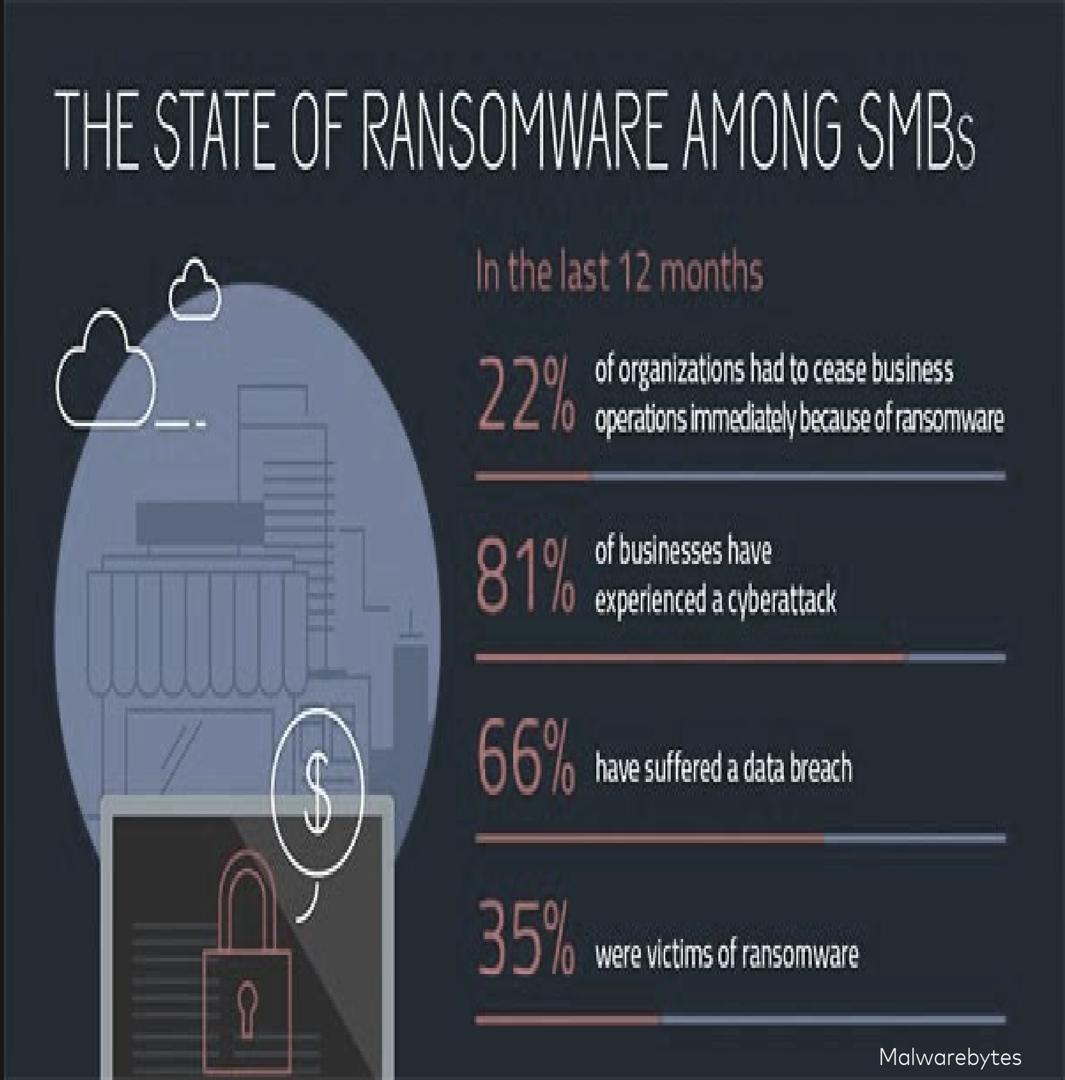
TROJAN'S

Sent Mail
Spam (372)
Trash
NO SPAM!

Phishing

Ransomware

71% of ransomware attacks are targeted at small businesses.[1]



THE STATE OF RANSOMWARE AMONG SMBs

In the last 12 months

22% of organizations had to cease business operations immediately because of ransomware

81% of businesses have experienced a cyberattack

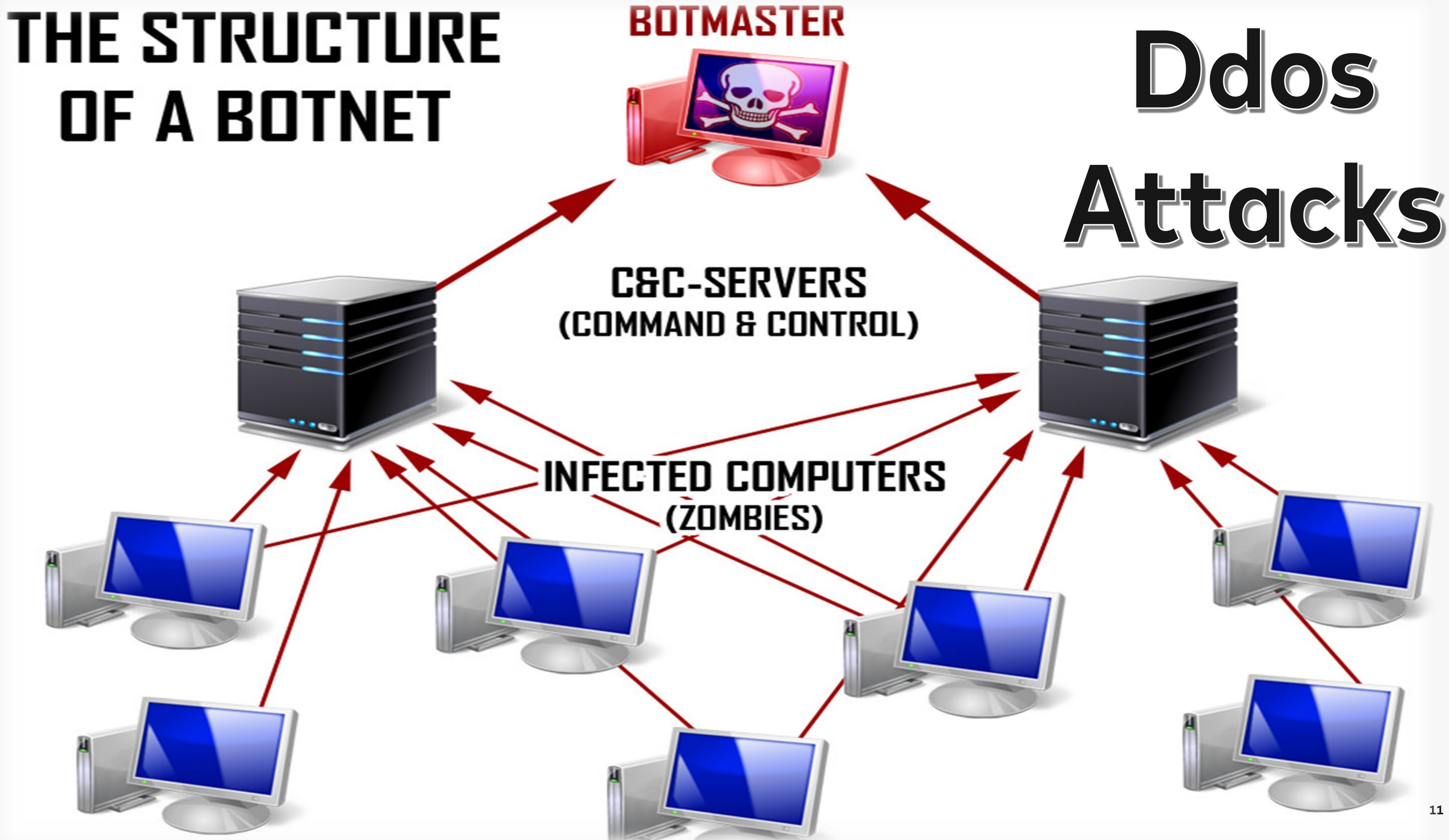
66% have suffered a data breach

35% were victims of ransomware

Malwarebytes

[1]- Insureon

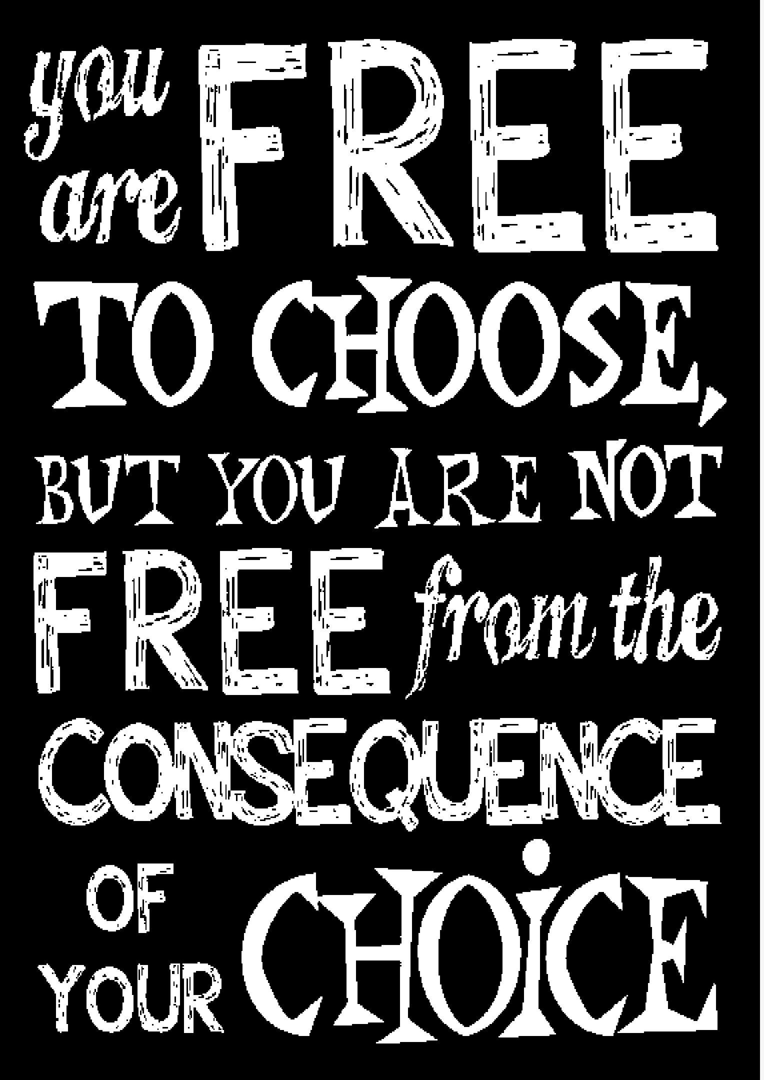
Ddos Attacks



How does a Ddos attack work?

What Are You Worth to a Cybercriminal?

$65+	$$$$	$35+	$60+



Consequences of Risk:
40% of consumers have reported breaches of their personal data by someone who did not have prior consent.

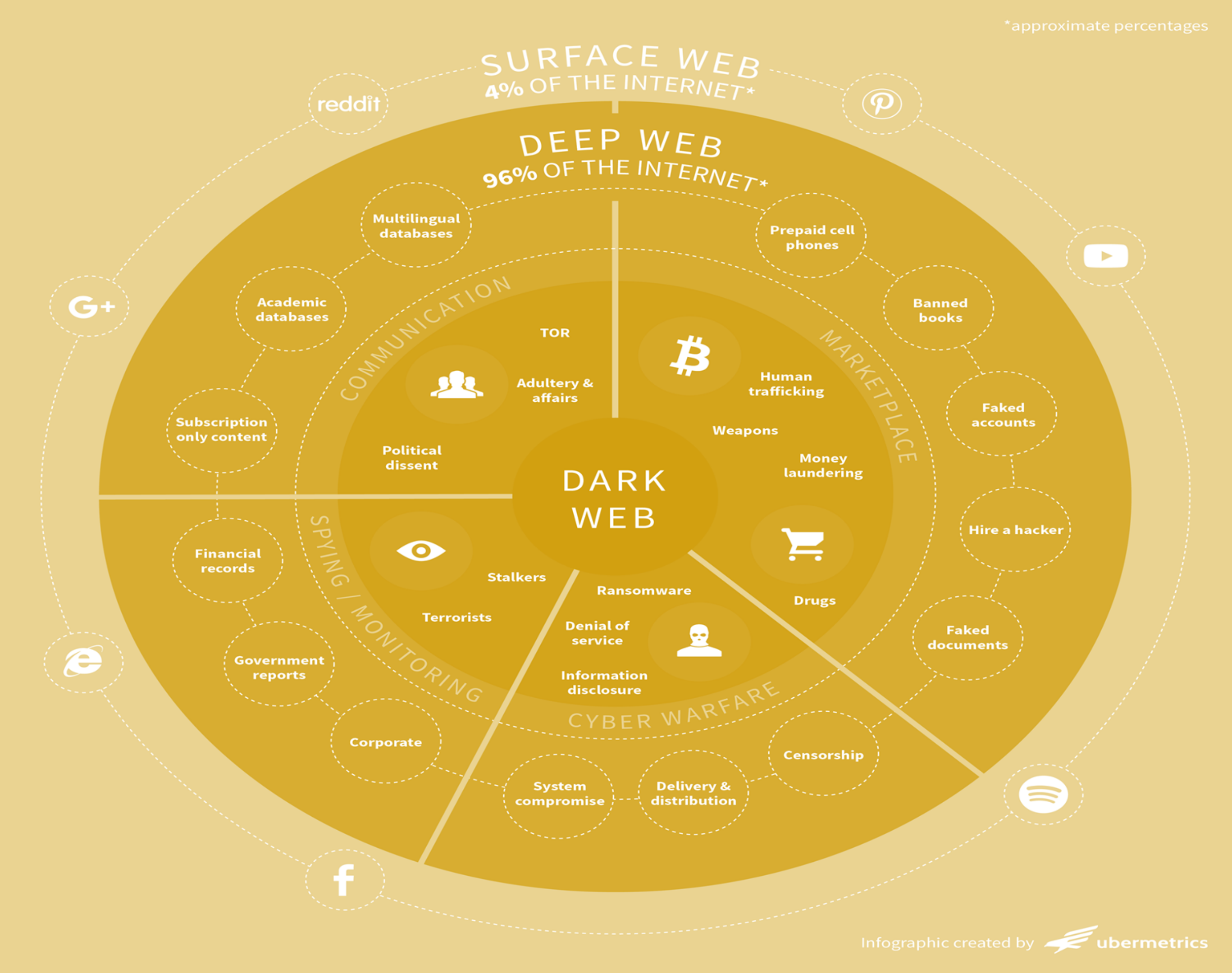
39% of data breaches involved the illegal takeover of devices, while 31% had their personal data stolen or used illegally, and a fifth (20%) had their private data divulged publicly.

By having their data privacy compromised:

- 39% of consumers felt inundated with spam and ads.
- 33% felt stressed.
- 24% believed their personal reputation had been damaged.
- 19% had lost money, were bullied or ended up causing offence to others.
- 16% said they have been blackmailed.
- 14% felt their careers had suffered.
- 10% experienced damage to their romantic relationships, some even ending up in divorce.

- Kaspersky Global Report

What is the Dark Web?



*approximate percentages

SURFACE WEB
4% OF THE INTERNET*

reddit

DEEP WEB
96% OF THE INTERNET*

Multilingual databases

Academic databases

Subscription only content

Financial records

Government reports

Corporate

System compromise

Delivery & distribution

Censorship

Faked documents

Hire a hacker

Faked accounts

Banned books

Prepaid cell phones

COMMUNICATION

TOR

Adultery & affairs

Political dissent

MARKETPLACE

Human trafficking

Weapons

Money laundering

Drugs

SPYING / MONITORING

Stalkers

Terrorists

CYBER WARFARE

Ransomware

Denial of service

Information disclosure

DARK WEB

Infographic created by ubermetrics

2017-09-26

FIRETIGERRR BREACH UPDATE

JOKER's STASH

FIRETIGERRR BREACH at JOKER's STASH

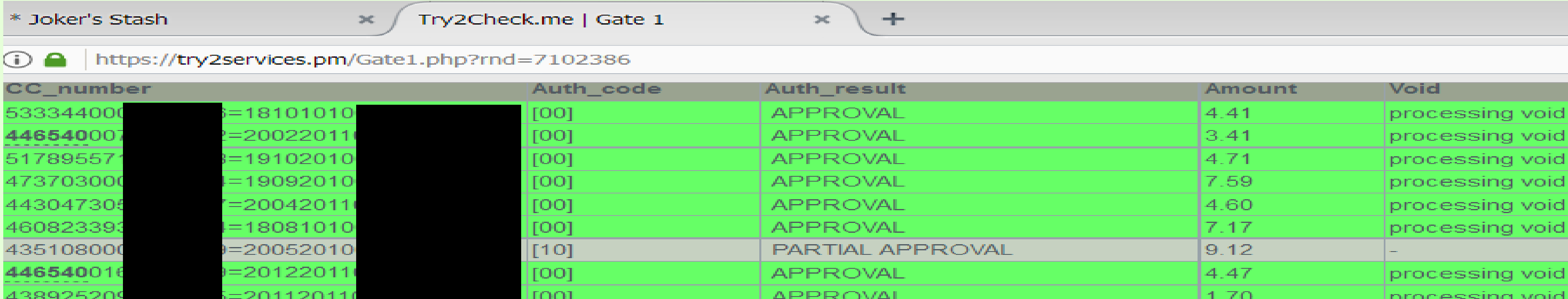
5.000.000 pcs. ALMOST ALL USA STATES.

100% FRESH 100% FIRE DUMPS

WARRAX (FIRETIGERRR BREACH) : **USA by STATE/CITY/ZIP TR1+TR2/TR2**, uploaded 2017-09-25
first 3 days NO REFUNDS !
after 3 days TIME FOR REFUNDS: 3 HOURS (GOLD USERS 12H, SILVER 9H, BRONZE 6H)

WARRAX-EXTRA (FIRETIGERRR BREACH) : **USA by STATE/CITY/ZIP TR1+TR2/TR2**, uploaded 2017-09-25
first 3 days NO REFUNDS !
after 3 days TIME FOR REFUNDS: 3 HOURS (GOLD USERS 12H, SILVER 9H, BRONZE 6H)

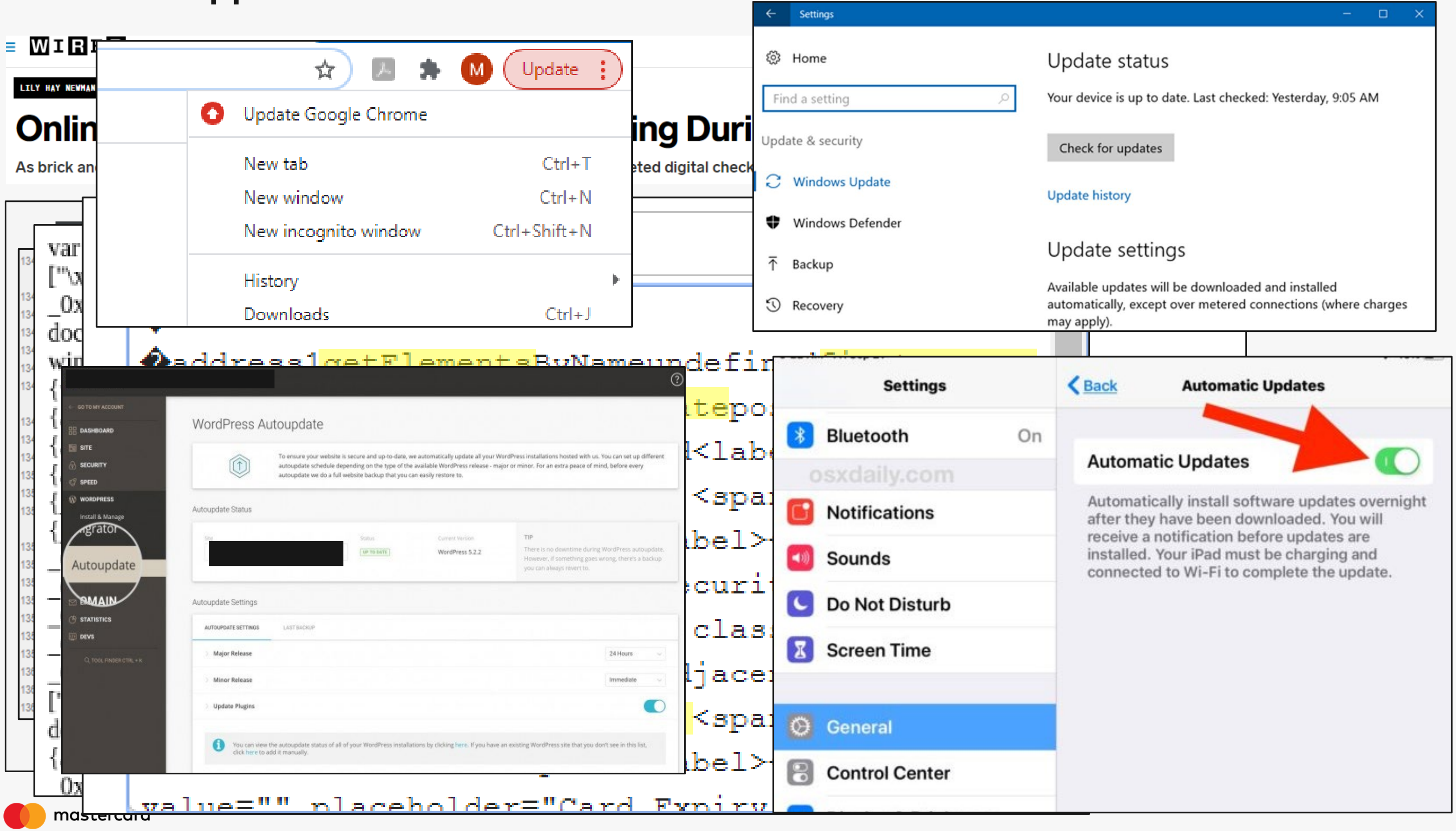
FIRETIGERRR random dumps valid test (try2services checker):



https://try2services.pm/Gate1.php?rnd=7102386

CC_number	Auth_code	Auth_result	Amount	Void
533344000[redacted]6=18101010[redacted]	[00]	APPROVAL	4.41	processing void
446540007[redacted]2=20022011[redacted]	[00]	APPROVAL	3.41	processing void
517895571[redacted]3=19102010[redacted]	[00]	APPROVAL	4.71	processing void
473703000[redacted]4=19092010[redacted]	[00]	APPROVAL	7.59	processing void
443047305[redacted]7=20042011[redacted]	[00]	APPROVAL	4.60	processing void
460823393[redacted]4=18081010[redacted]	[00]	APPROVAL	7.17	processing void
435108000[redacted]9=20052010[redacted]	[10]	PARTIAL APPROVAL	9.12	-
446540016[redacted]9=20122011[redacted]	[00]	APPROVAL	4.47	processing void
438925209[redacted]5=20112011[redacted]	[00]	APPROVAL	1.70	processing void

Outdated application software



WIRED
LILY HAY NEWMAN
Onlin… …ing Duri…
As brick an… …eted digital check…
address1 getElementsByName undefin…
value="" placeholder="Card Expiry…

Update

Update Google Chrome

New tab Ctrl+T

New window Ctrl+N

New incognito window Ctrl+Shift+N

History

Downloads Ctrl+J

Settings

Home

Find a setting

Update & security

Windows Update

Windows Defender

Backup

Recovery

Update status

Your device is up to date. Last checked: Yesterday, 9:05 AM

Check for updates

Update history

Update settings

Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

[redacted]

GO TO MY ACCOUNT

DASHBOARD

SITE

SECURITY

SPEED

WORDPRESS

Install & Manage

…grator

Autoupdate

…MAIN

STATISTICS

DEVS

TOOL FINDER CTRL + K

WordPress Autoupdate

To ensure your website is secure and up-to-date, we automatically update all your WordPress installations hosted with us. You can set up different autoupdate schedule depending on the type of the available WordPress release - major or minor. For an extra peace of mind, before every autoupdate we do a full website backup that you can easily restore to.

Autoupdate Status

Site: [redacted]

Status: UP TO DATE

Current Version: WordPress 5.2.2

TIP: There is no downtime during WordPress autoupdate. However, if something goes wrong, there's a backup you can always revert to.

Autoupdate Settings

AUTOUPDATE SETTINGS | LAST BACKUP

Major Release: 24 Hours

Minor Release: Immediate

Update Plugins: ●

You can view the autoupdate status of all of your WordPress installations by clicking here. If you have an existing WordPress site that you don't see in this list, click here to add it manually.

Settings

Bluetooth On

osxdaily.com

Notifications

Sounds

Do Not Disturb

Screen Time

General

Control Center

Back

Automatic Updates

Automatic Updates ●

Automatically install software updates overnight after they have been downloaded. You will receive a notification before updates are installed. Your iPad must be charging and connected to Wi-Fi to complete the update.

Best Practices

Keep software up to date with the latest patches

Consider "Automatic Updates" when available

Use Multifactor Authentication

Don't reuse the same passwords across multiple sites

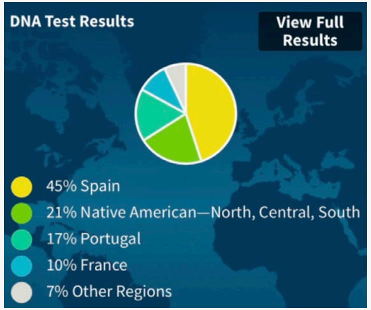
If you use remote login, only enable the connection when needed

Hold your third-party service providers to high standards

Avoid clicking on links and attachments in emails

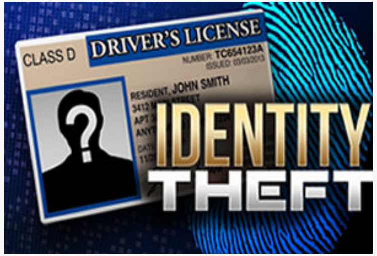
If you weren't expecting the email, verify using a trusted phone number

How can you avoid being a victim of cybercrime?



Pay

mastercard



Questions?

mastercard