

Cybersecurity Threats On the Rise

What Every Organization Needs to Know to Mitigate Risk

May 2022

Welcome



Hank Wolfson
Partner & Chief Operating Officer
Gray, Gray & Gray, LLP
hwolfson@gggllp.com

Today's Presenter



Nate Gravel, CISA, CISM, CRISC
Cybersecurity Consultant
Gray, Gray & Gray, LLP
ngravel@gggllp.com

Agenda

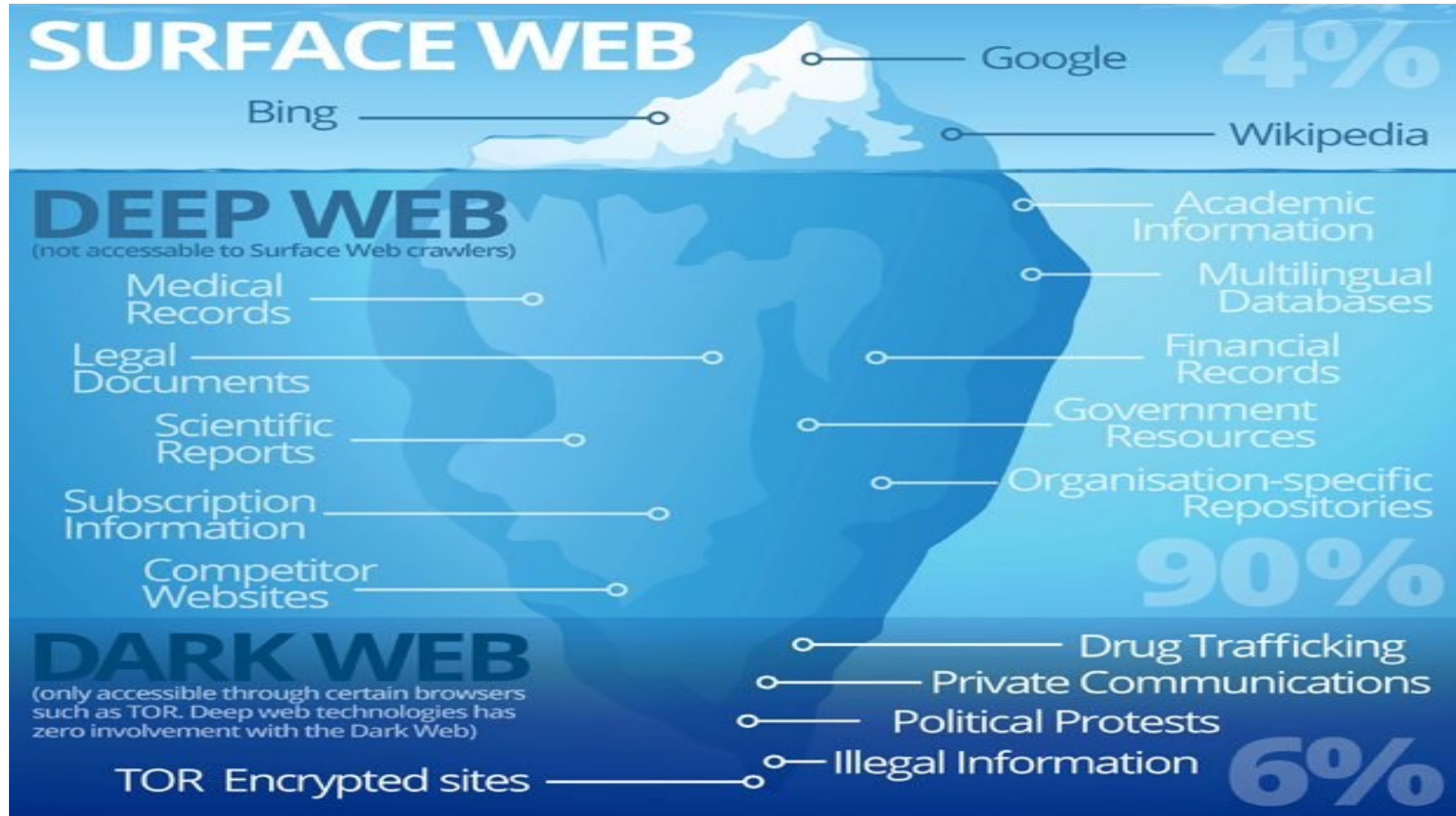
- Cybersecurity Threat Landscape
- Top Threats Facing Our Clients
 - Phishing
 - Malware/Ransomware
 - Credential Theft/Account Takeover
- Mitigation Measures
- Q&A
- Closing Remarks



The Cybercrime Landscape

According to some studies, the global cost of cybercrime is projected to reach over **\$10 trillion** by 2025.

The Cybercrime Landscape



The Cybercrime Landscape

Cybercrime is no longer a one man operation. Within the cybercrime underground an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack lifecycle.*

Fraud as a service is constantly changing and adapting to new security solutions, offering end to end technologies, multiple SLA levels and low prices for everything a cybercriminal might need.

Malware

Cost: Free - \$20k (license based)

Trojan designed to steal data, manipulate online banking sessions, inject screens and more.



Exploit Kits

Cost: \$2K (monthly rental)

Toolkits designed to exploit system and software vulnerabilities resulting in a malicious download.



Droppers

Cost: Free - \$10K

Software designed to download malware to an infected device, evading antivirus and research tools.



Money Mules

Cost: Up to 60% of account balance

A person who receives the stolen money from a hacked account and transfers the funds via an anonymous payment service to the mule operator.



Infrastructure

Cost: \$50 - \$1,000 (Rental per month)

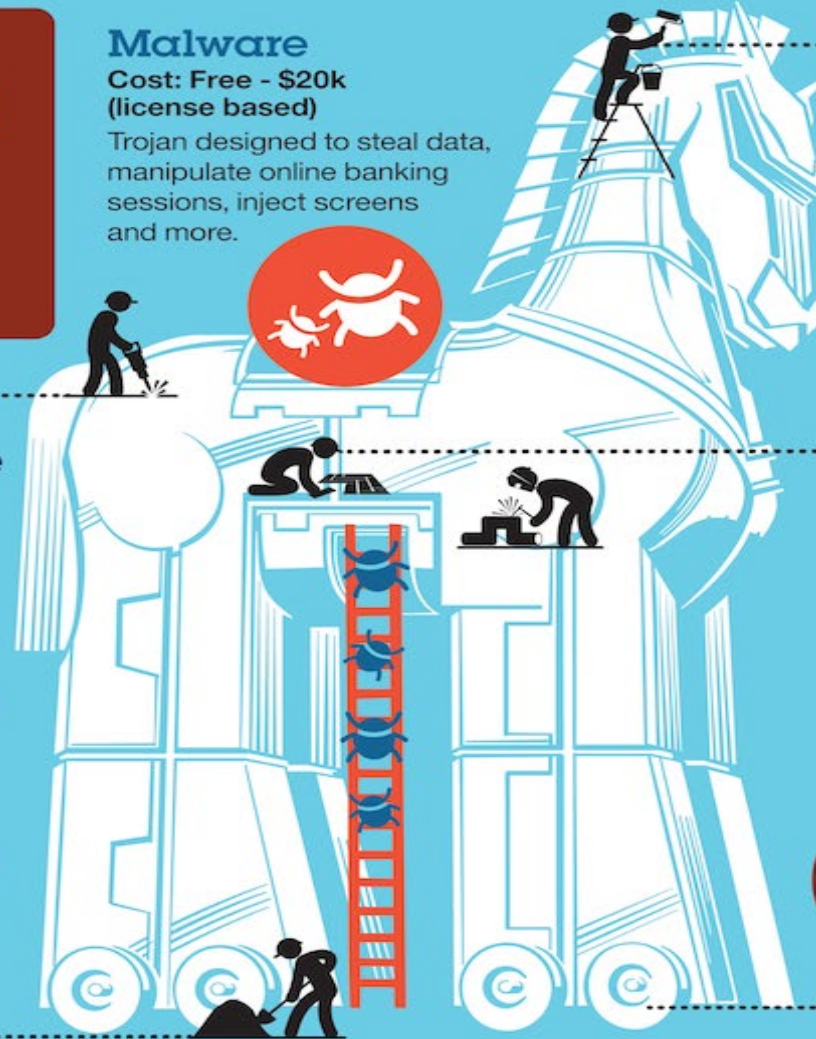
Hosting services for malware update, configuration and command and control servers. Some are fast flux or TOR based.



Spammers

Cost: \$1 - \$4 per 1000 emails

Spam botnet operators that spread emails with attachments or links leading to a Trojan infection.



* This infographic shows one possible scenario of a cybercriminal attack lifecycle. Prices for this scenario are estimates.

The Cybercrime Landscape

CC CC Orders **Buy Dumps** Dump orders Checker Tickets

Hello, [redacted] Cart (1) 9.45\$ Balance: 3.0\$ [Add money](#) [Replace policy](#)

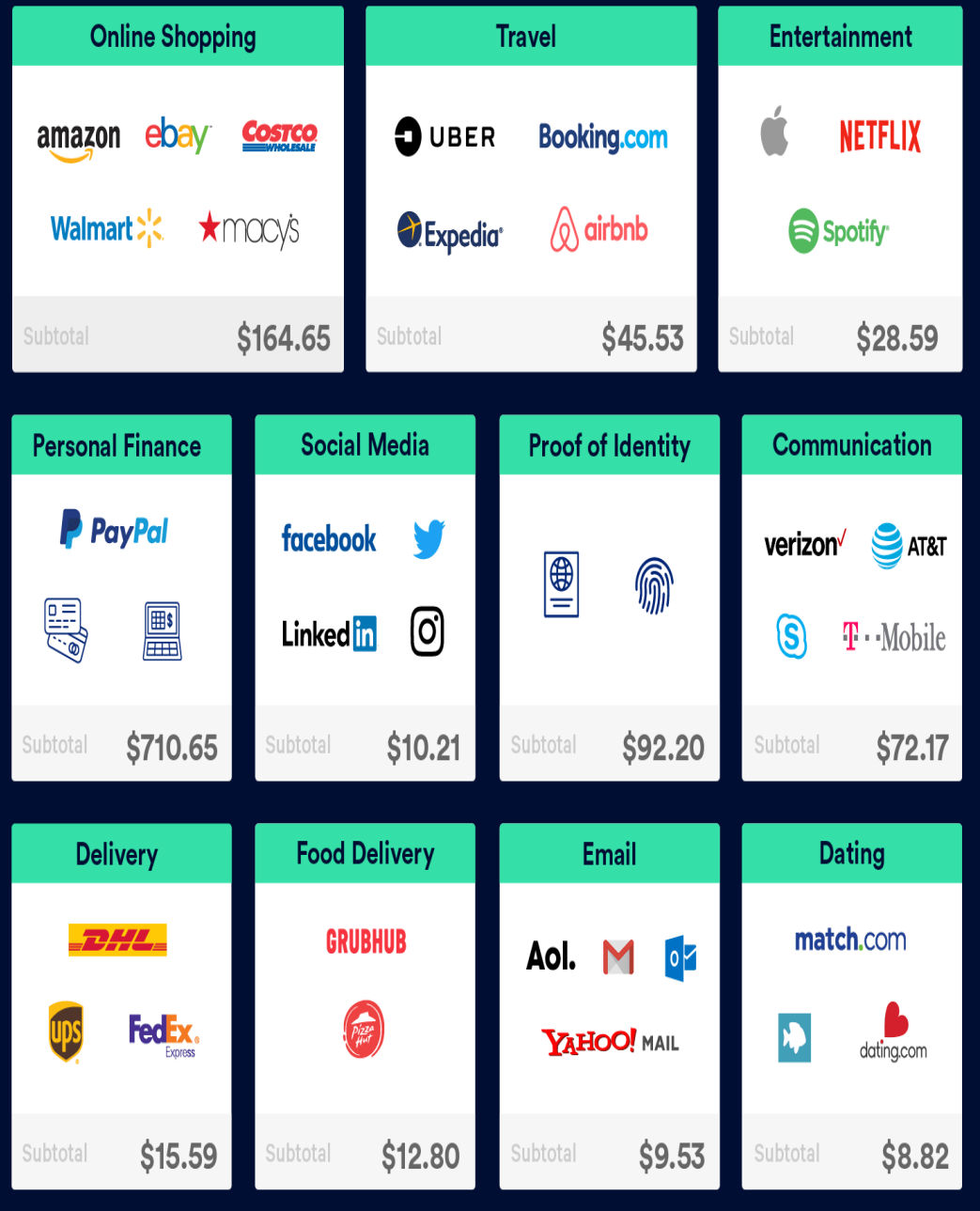
101
 201

dn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [Bulk Orders - Low Prices!](#)

Clear

Search

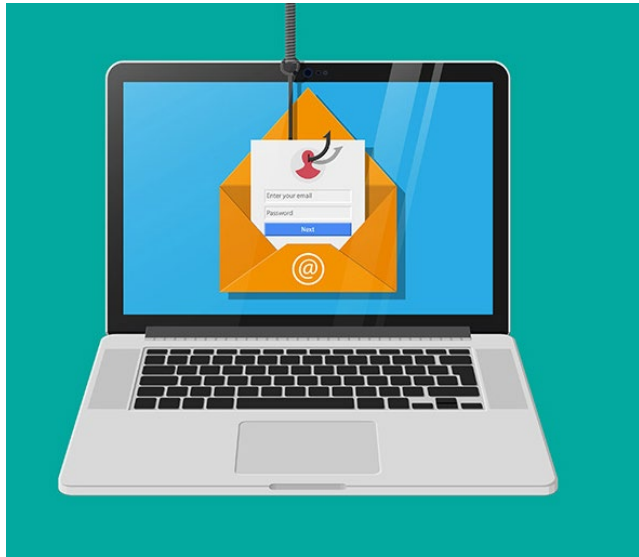
	Bin	Card	Debit/Credit	Mark	Expres	Track 1	Code	Country	Bank	Base	Price	Cart
	371736	AMEX	CREDIT		07/15	Yes	110	United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14	30\$	<input data-bbox="2135 582 2204 621" type="button" value="+"/>
	371555	AMEX	CREDIT		09/16	Yes	101	United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14	30\$	<input data-bbox="2135 696 2204 735" type="button" value="+"/>
	371736	AMEX	CREDIT		03/17	Yes	101	United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14	30\$	<input data-bbox="2135 782 2204 821" type="button" value="+"/>
	371564	AMEX	CREDIT		05/15	Yes	110	United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14	30\$	<input data-bbox="2135 868 2204 906" type="button" value="+"/>
	371554	AMEX	CREDIT		04/17	Yes	101	United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14	30\$	<input data-bbox="2135 953 2204 992" type="button" value="+"/>
	371242	AMEX	CREDIT	GREEN	06/17	Yes	101	United States, 98512, Olympia, WA	AMERICAN EXPRESS COMPANY	American Sanctions 14	30\$	<input data-bbox="2135 1039 2204 1078" type="button" value="+"/>
	371570	AMEX	CREDIT		10/16	Yes	101	United States, 97123, Hillsboro, OR	BANK OF AMERICA	American Sanctions 14	30\$	<input data-bbox="2135 1153 2204 1192" type="button" value="+"/>
	371381	AMEX	CREDIT		10/16	Yes	201	United States, 30328, Atlanta, GA	CITIBANK <small>Dump or cc of this particular bank (BIN)</small>	American Sanctions 14	24\$	<input data-bbox="2135 1239 2204 1278" type="button" value="+"/>



The Cybercrime Landscape

The average consumer is worth about **\$1,200** on the Dark Web.

Top Threats Facing Our Clients



Phishing



Credential Theft
(Business E-mail Compromise)



Malware
(Ransomware)

Phishing

FW: Transfer - Message (HTML)

FILE MESSAGE

Thu 8/27/2015 2:29 PM

Debbie [REDACTED] <debbiea@[REDACTED].com>

FW: Transfer

To Nathaniel C. Gravel

Message CSKX Wire Instructions.pdf (122 KB)

From: Lee [REDACTED] [[mailto:lee@\[REDACTED\].com](mailto:lee@[REDACTED].com)]
Sent: Wednesday, August 26, 2015 1:01 PM
To: Debbie [REDACTED]
Subject: RE: Transfer

Please go to the bank and make a transfer for \$104,549.36 and the purpose for the wire is Admin services. Send me the confirmation once done.

Lee

Lee [REDACTED]

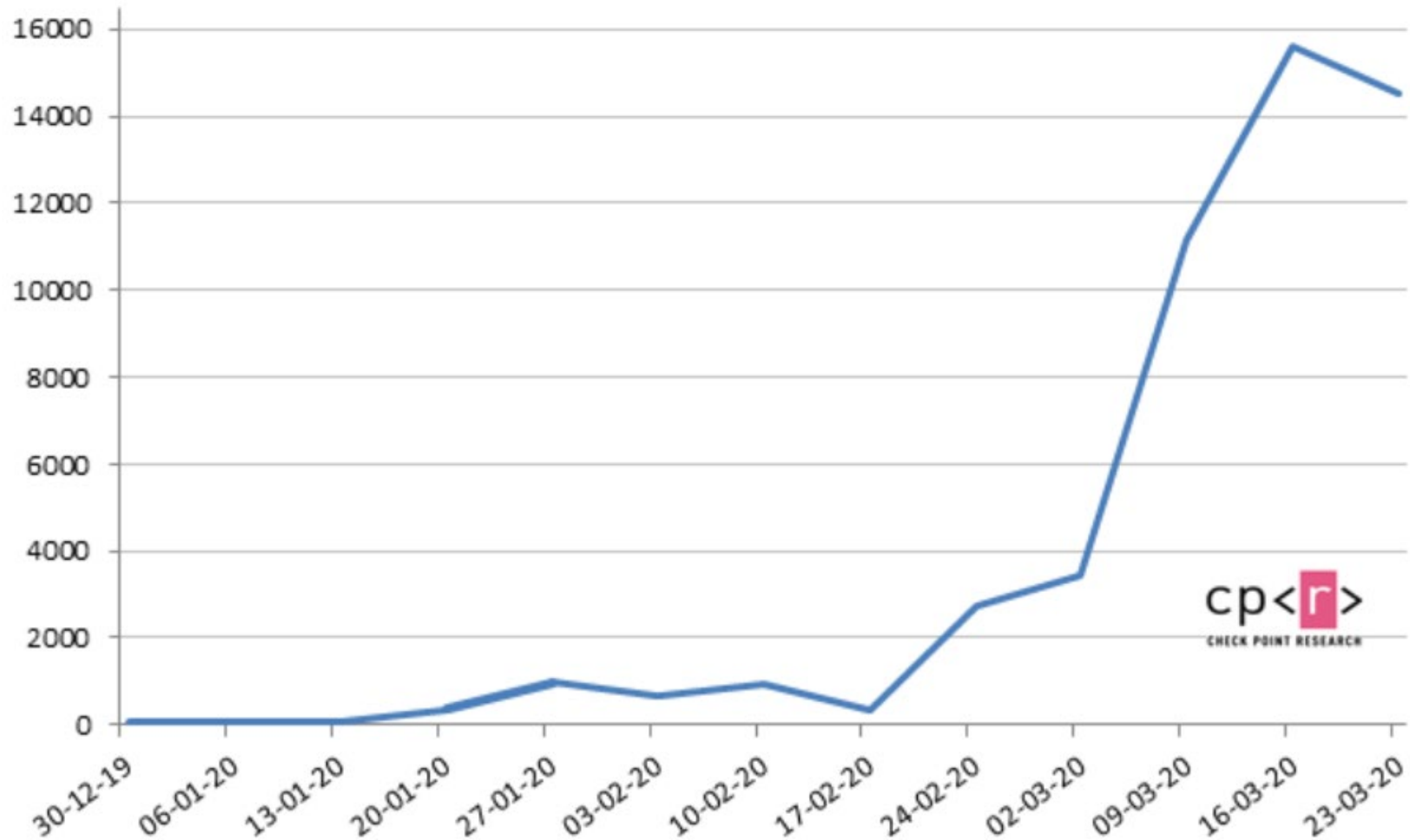
On 2015-08-26 16:42, Debbie [REDACTED] wrote:

I can go to the bank and see.

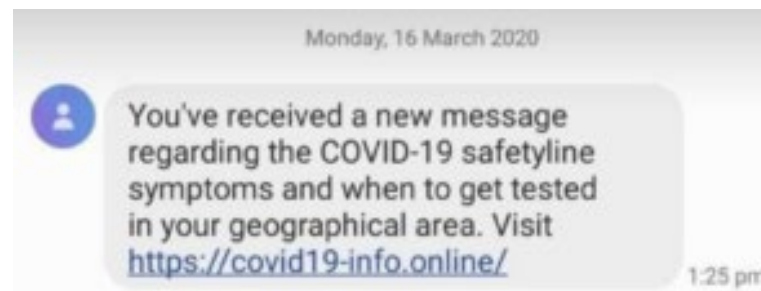
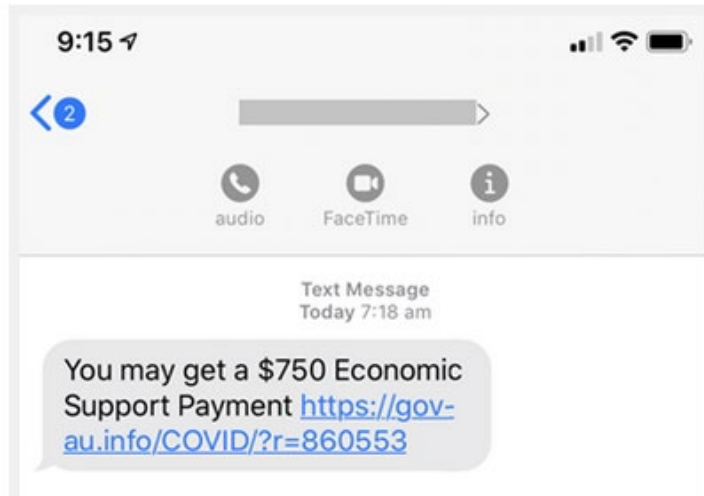
Debbie

Phishing

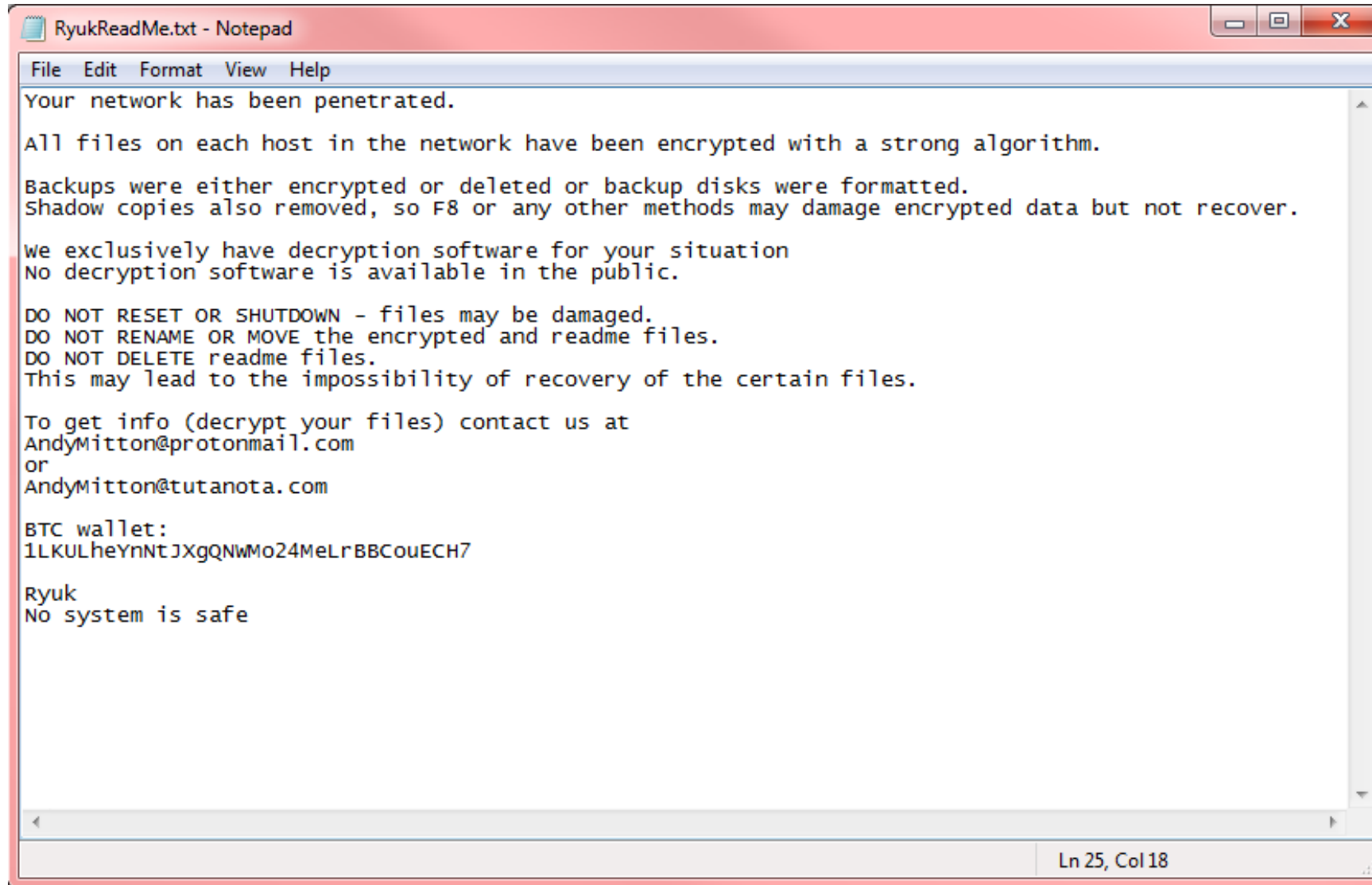
Coronavirus Domains Registered Weekly



Phishing



Malware/Ransomware



```
File Edit Format View Help
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

we exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com

BTC wallet:
1LKULheYnNtJXgQNwMo24MeLrBBCouECH7

Ryuk
No system is safe

Ln 25, Col 18
```

Malware/Ransomware



In 2021, roughly **67%** of malware victims were small to mid-size businesses with 1,000 employees or less.

There are an estimated **350,000** new malware variants identified every day.

Credential Theft/Account Takeover



Password reuse by age group

87%

of respondents
ages 18-30

81%

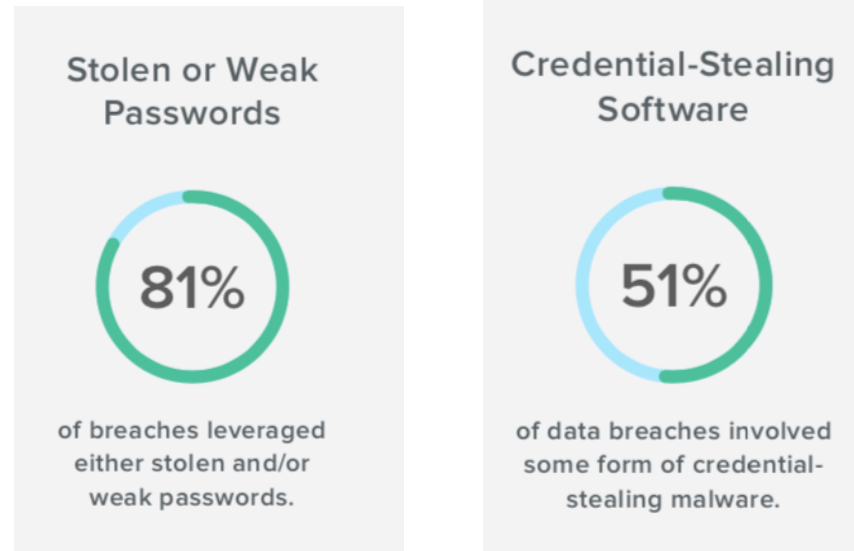
of respondents
ages 31 and up

Credential Theft/Account Takeover

3. Phishing and Credential Theft Are Rampant in the Work-from-Home Era

According to the report, phishing remains the top form of social-driven breach and “schemes are increasingly sophisticated and malicious” as remote work surges. Meanwhile, the use of stolen credentials by external actors is on a meteoric rise. More than 80% of breaches tied to hacking (the number one threat action) involve the use of lost or stolen credentials or brute force.

While these findings are not new or surprising, the DBIR reminds us that attackers nearly always take the path of least resistance by using this tried-and-true approach: start with a phishing scam (96% arrive by email) targeting a user’s endpoint, then easily crack weak passwords or steal credentials stored on the device. Using these credentials, the attacker can move from workstation to workstation in search of sensitive data to steal and privileged credentials (such as [local admin rights](#)) that enable [escalation](#) to higher-value assets and information.



Credential Theft/Account Takeover

';--have i been pwned?

Check if your email or phone is in a data breach

ngravel@gravoc.com

pwned?

Oh no — pwned!

Pwned in 10 [data breaches](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)



ParkMobile: In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.

Compromised data: Email addresses, Licence plates, Names, Passwords, Phone numbers

Mitigation Measures: Our Advice to All Clients



- Perform Risk Assessment/Gap Analysis
 - Assess Security Operations (People, Process, Technology)
 - Assess Administrative, Physical, & Technical Controls
- Perform Vulnerability Assessment/Penetration Testing
 - Internal/External Network
 - Cloud Services (Office 365, etc.)
- Perform Social Engineering Exercise
 - Simulated Phishing
 - Simulated Spear Phishing

Mitigation Measures: Our Advice to All Clients



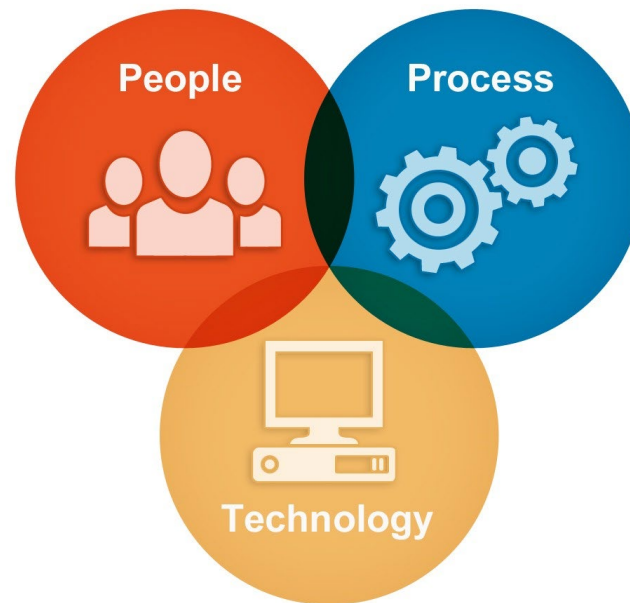
1. Train/educate
2. Invest in all 3 core components of security posture: protection, detection, response
3. Test (retest) and don't be afraid to fail

Question & Answer



Closing Remarks

Information security is **people**, **process**, and **technology**, not firewalls, encryption, and antivirus.



All You Need to Succeed



CONSULTING

- Cybersecurity & IT Consulting
- Government Grants & Contracts Consulting
- Outsourced Accounting & Advisory Services
- Royalty Examinations
- Sage Intacct Accounting Software
- Strategic Business Planning
- Succession Planning
- Transaction Advisory Services

TAX

- Estate & Gift Taxation
- State & Local Tax Services
- Tax Strategy & Compliance

AUDIT & ASSURANCE

- Auditing & Accounting
- Employee Benefit Plan Audits
- Financial Reporting Consulting
- Overhead Rate Audits

PRIVATE WEALTH

- Private Wealth Management

Thank you



Hank Wolfson
Partner & Chief Operating Officer
Gray, Gray & Gray, LLP
hwolfson@gggllp.com



Nate Gravel, CISA, CISM, CRISC
Cybersecurity Consultant
Gray, Gray & Gray, LLP
ngravel@gggllp.com

Contact Us



g³ gray
THE POWER OF MORE



Gray, Gray & Gray, LLP
150 Royall Street, Suite 102
Canton, MA 02021
www.gggllp.com
781.407.0300

