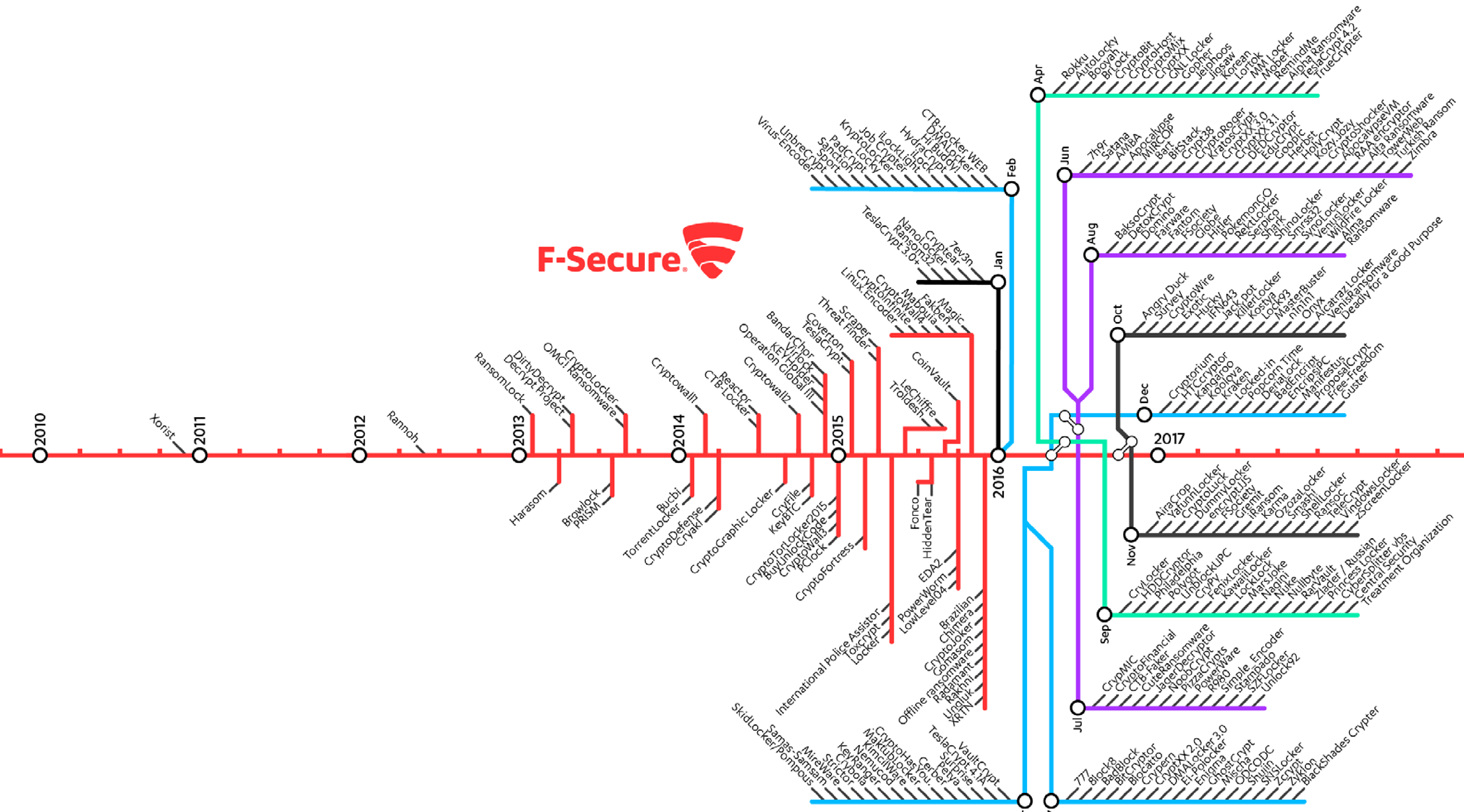
LEARN TO SECURE YOUR GREATEST ASSET (YOUR BUSINESS) FROM A CYBER-ATTACK

MAD DATA

Agenda:

- □ Current Cyber Landscape
- □ 5 Groups under Attack
- □ How to Protect your Business

CURRENT CYBER LANDSCAPE


F-Secure
2010
Xorist
2011
2012
Rannoh
2013
RansomLock
DirtyDecrypt
Decrypt Project
OMG! Ransomware
CryptoLocker
Harasom
Browlock
PRISM
2014
Cryptowall1
Reactor
CTB-Locker
Cryptowall2
Operation Global III
KEYHolder
Virlock
BandarChor
Bucbi
TorrentLocker
CryptoDefense
Cryaki
CryptoGraphic Locker
CryFile
KeyBTC
CryptoTorLocker2015
BuyUnlockCode
CryptoWall3
PClock
2015
TeslaCrypt
Coverton
Threat Finder
Scraper
Linux.Encoder
CryptoInfinite
CryptoWall4
Mabouia
Fakben
Magic
CoinVault
LeChiffre
Troldesh
CryptoFortress
International Police Assistor
Toxcrypt
Locker
Fonco
HiddenTear
EDA2
PowerWorm
LowLevel04
Brazilian
Chimera
CryptoJoker
Gomasom
Offline ransomware
Radamant
Rakhni
Unqluk
XRTN
2016
Jan
TeslaCrypt 3.0+
Ransom32
NanoLocker
Cryptear
7ev3n
Feb
Virus-Encoder
UnbreCrypt
Sport
Sanction
PadCrypt
Locky
KryptoLocker
Job Crypter
iLockLight
iLock
HydraCrypt
Hi Buddy!
DMALocker
CTB-Locker WEB
SkidLocker/Pompous
Samas-Samsam
MireWare
Strictor
Cryptobia
KeyRanger
Nemucod
KimcilWare
Maktub Locker
CryptoHasYou.
Cerber
Petya
Surprise
TeslaCrypt 4.1A
VaultCrypt
Apr
Rokku
AutoLocky
Booyah
BrLock
CryptoBit
CryptoHost
CryptoMix
CryptXXX
GNL Locker
Gopher
Jeiphoos
Jigsaw
Korean
Lortok
MM Locker
Mobef
RemindMe
Alpha Ransomware
TeslaCrypt 4.2
TrueCrypter
777
8lock8
BadBlock
BitCryptor
Blocatto
Crypern
CryptXXX 2.0
DMALocker 3.0
El-Polocker
Enigma
GhostCrypt
Mischa
ODCODC
Shujin
SNSLocker
Zcrypt
ZyKlon
BlackShades Crypter
Jun
7h9r
Satana
AMBA
Apocalypse
MIRCOP
Bart
BitStack
Crypt38
CryptoRoger
KratosCrypt
CryptXXX 3.0
CryptXXX 3.1
DEDCryptor
EduCrypt
Goopic
Herbst
HolyCrypt
Kozy.Jozy
CryptoShocker
ApocalypseVM
RAA encryptor
Alfa Ransomware
TowerWeb
Turkish Ransom
Zimbra
Jul
CrypMIC
CryptoFinancial
CTB-Faker
CuteRansomware
JagerDecryptor
NoobCrypt
PizzaCrypts
PowerWare
R980
Simple_Encoder
Stampado
SZFLocker
Unlock92
Aug
BaksoCrypt
DetoxCrypt
Domino
Fairware
Fantom
FSociety
Globe
Hitler
PokemonGO
RektLocker
Serpico
Shark
ShinoLocker
Smrss32
SynoLocker
VenusLocker
WildFire Locker
Alma
Ransomware
Sep
CryLocker
HDDCryptor
Philadelphia
Polyglot
UnblockUPC
CryPy
FenixLocker
KawaiiLocker
LockLock
MarsJoke
Nagini
Nuke
Nullbyte
RarVault
Zlader / Russian
Princess Locker
CyberSplitter vbs
Central Security
Treatment Organization
Oct
Angry Duck
Survey
CryptoWire
Exotic
Hucky
IFN643
Jack.pot
KillerLocker
Kostya
Lock93
MasterBuster
n1n1n1
Onyx
Alcatraz Locker
VenisRansomware
Deadly for a Good Purpose
Nov
AiraCrop
YafunnLocker
CryptoLuck
DummyLocker
encryptJJS
FSociety
Gremit
iRansom
Karma
OzozaLocker
Smash!
ShellLocker
Ransoc
TeleCrypt
VindowsLocker
zScreenLocker
Dec
Cryptorium
HTCcryptor
Kangaroo
Koolova
Kraken
Locked-in
Popcorn Time
DerialLock
BadEncript
EncripsiPC
Manifestus
ProposalCrypt
Free-Freedom
Guster
2017

Common Cyber Misconceptions

I'm not in a compliance business …

Hackers wouldn't go after a small company like me…

I don't collect sensitive data…

5 REASONS HACKERS TARGET SMALL-MID SIZED BUSINESSES

- They are low-hanging fruit
- They are more vulnerable to social engineering
- They often feel they must pay ransoms
- They are the ‘gateway” to larger organizations
- They are sometimes not targeted at all, but simply collateral damage

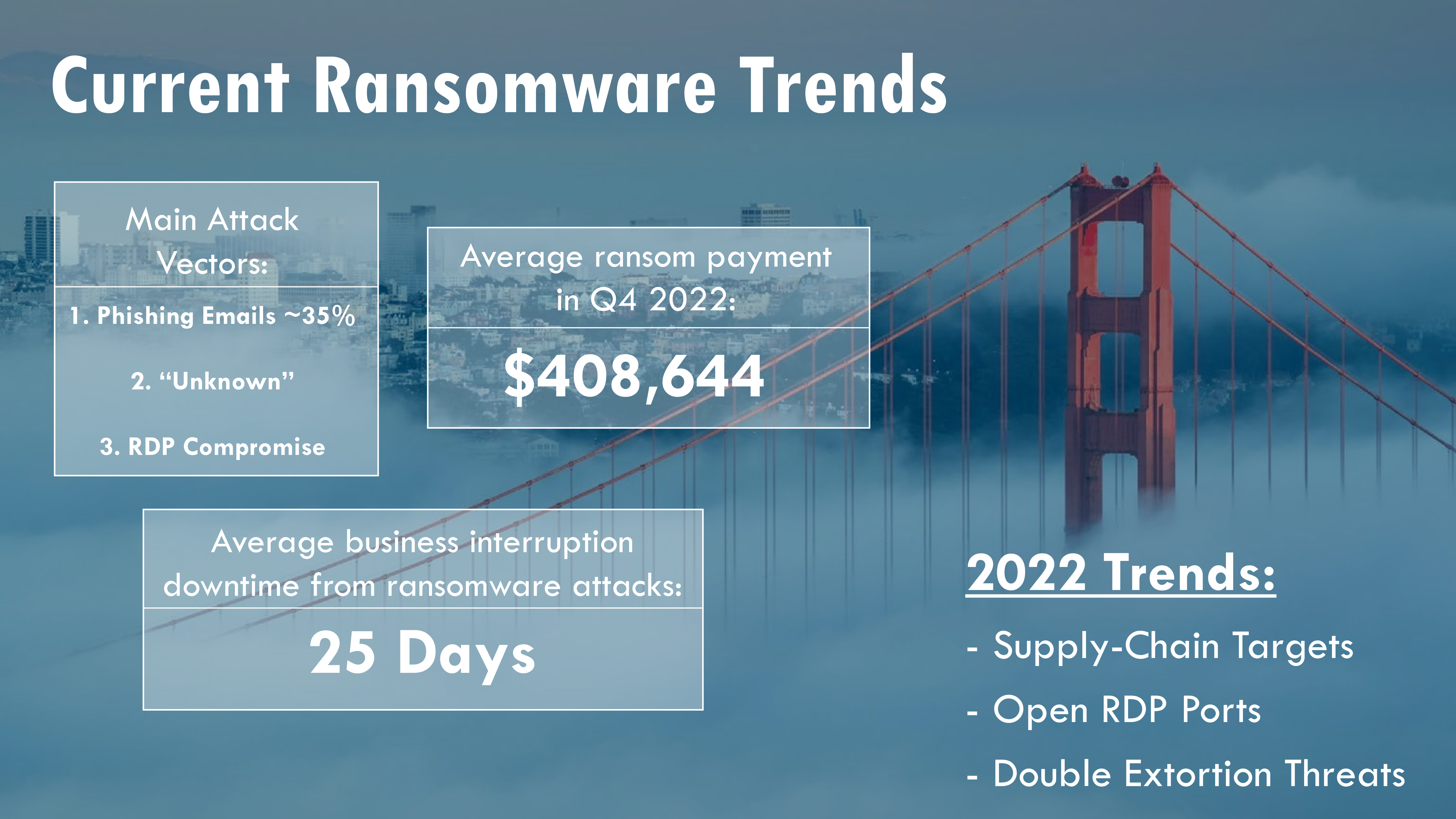
Why Do Businesses Get Hacked?

Every industry…

#1 Cause of Cyber Attacks is Human Error

- Collects Sensitive Data
- Relies On Technology
- Performs Financial Transactions
- Has a Human Workforce

Current Ransomware Trends



Main Attack Vectors:

1. **Phishing Emails ~35%**
2. **“Unknown”**
3. **RDP Compromise**

Average ransom payment in Q4 2022:

$408,644

Average business interruption downtime from ransomware attacks:

25 Days

2022 Trends:

- Supply-Chain Targets
- Open RDP Ports
- Double Extortion Threats

Hacking Profitability

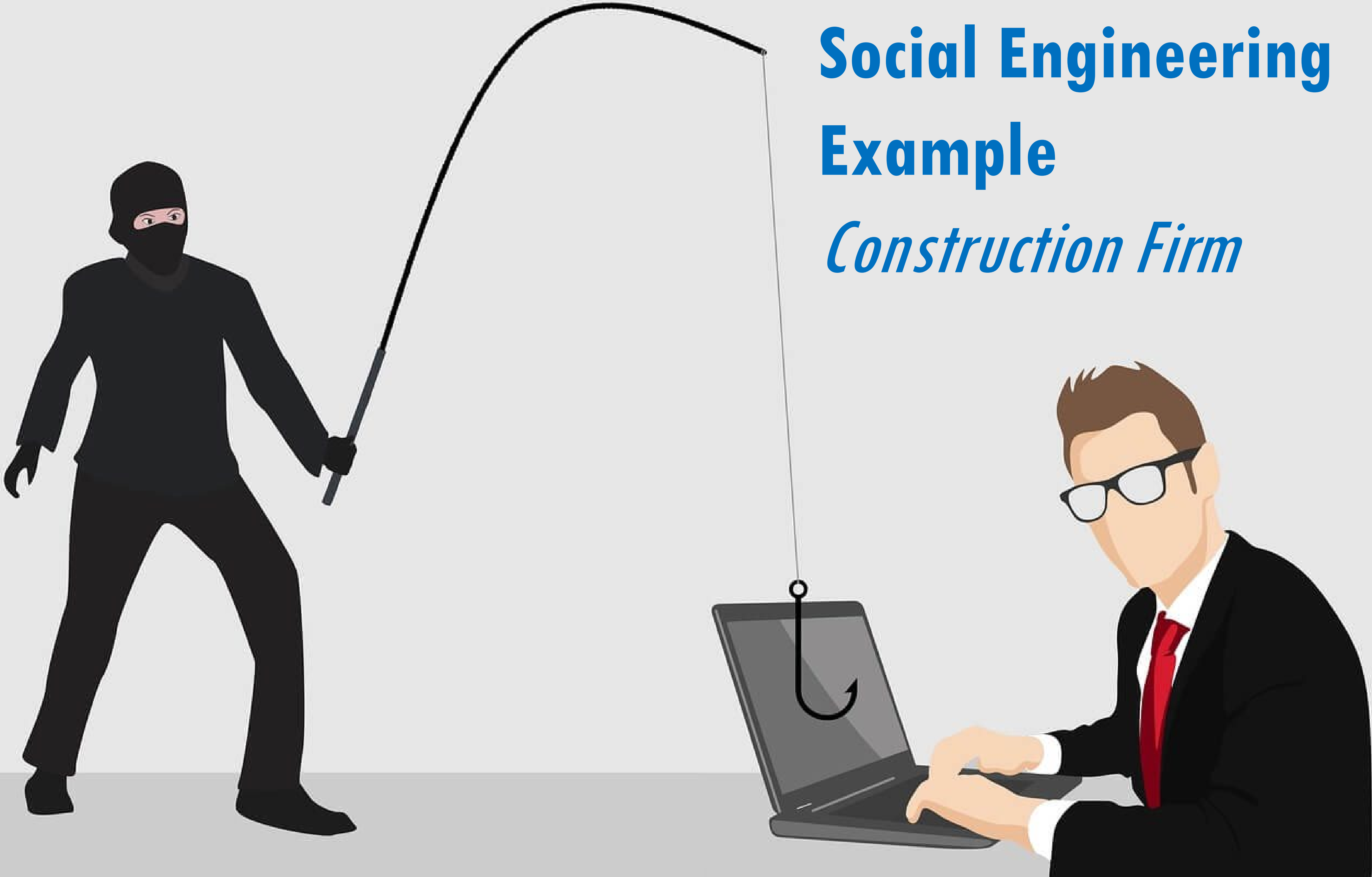
Coveware Stats	Ransomware	Drug Trafficking in 1992
Revenue/Unit	$140,000/attack	$60,000/kilo
Operating Costs/Unit	$2,500/attack*	$5,000/kilo
Profit Margin	98%	91%
Arrests/Unit	.0008*	.50
Deaths/Unit	0	.25
Barriers to Entry	None	Very High

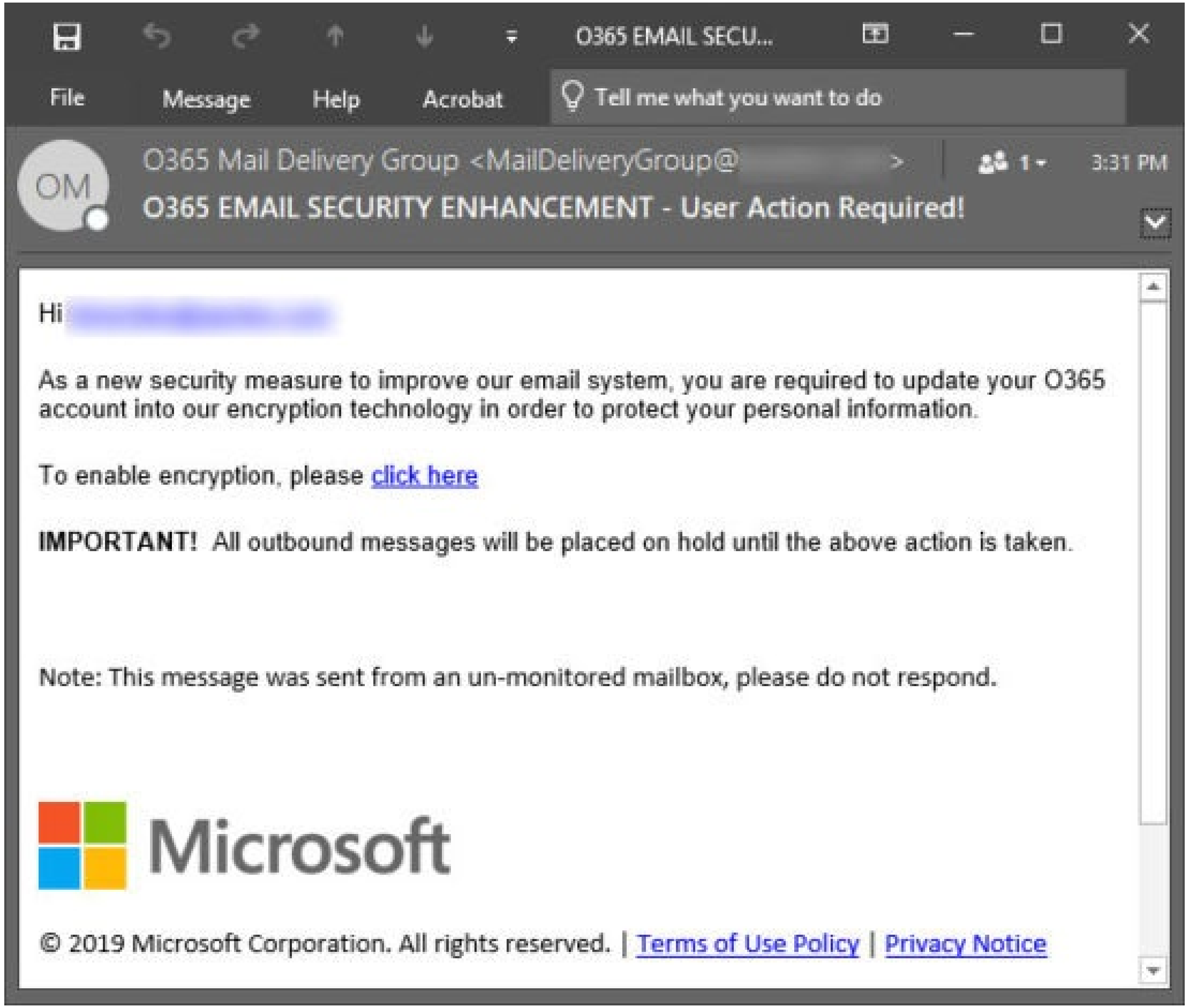
**Estimate based on reported costs of network access credentials, and amount of hours a threat actor expends on the average attack*

***Estimated roughly 25,000 ransomware attacks of impact in 2020. Research found evidence of less than 20 total arrests globally.*

Social Engineering Example

Construction Firm





O365 Mail Delivery Group <MailDeliveryGroup@[redacted]>

O365 EMAIL SECURITY ENHANCEMENT - User Action Required!

Hi [redacted]

As a new security measure to improve our email system, you are required to update your O365 account into our encryption technology in order to protect your personal information.

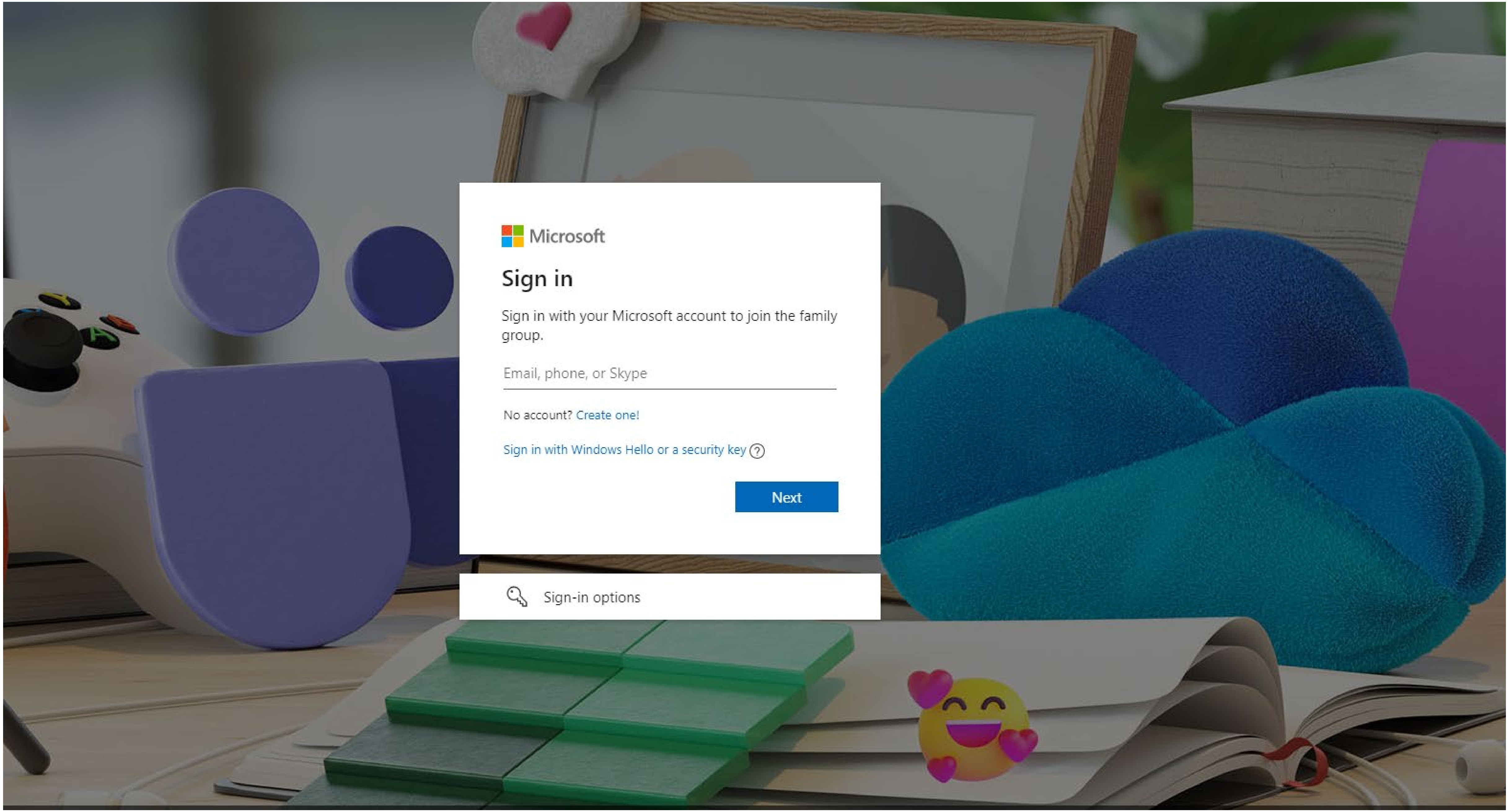
To enable encryption, please click here

IMPORTANT! All outbound messages will be placed on hold until the above action is taken.

Note: This message was sent from an un-monitored mailbox, please do not respond.

Microsoft

© 2019 Microsoft Corporation. All rights reserved. | Terms of Use Policy | Privacy Notice



Microsoft

Sign in

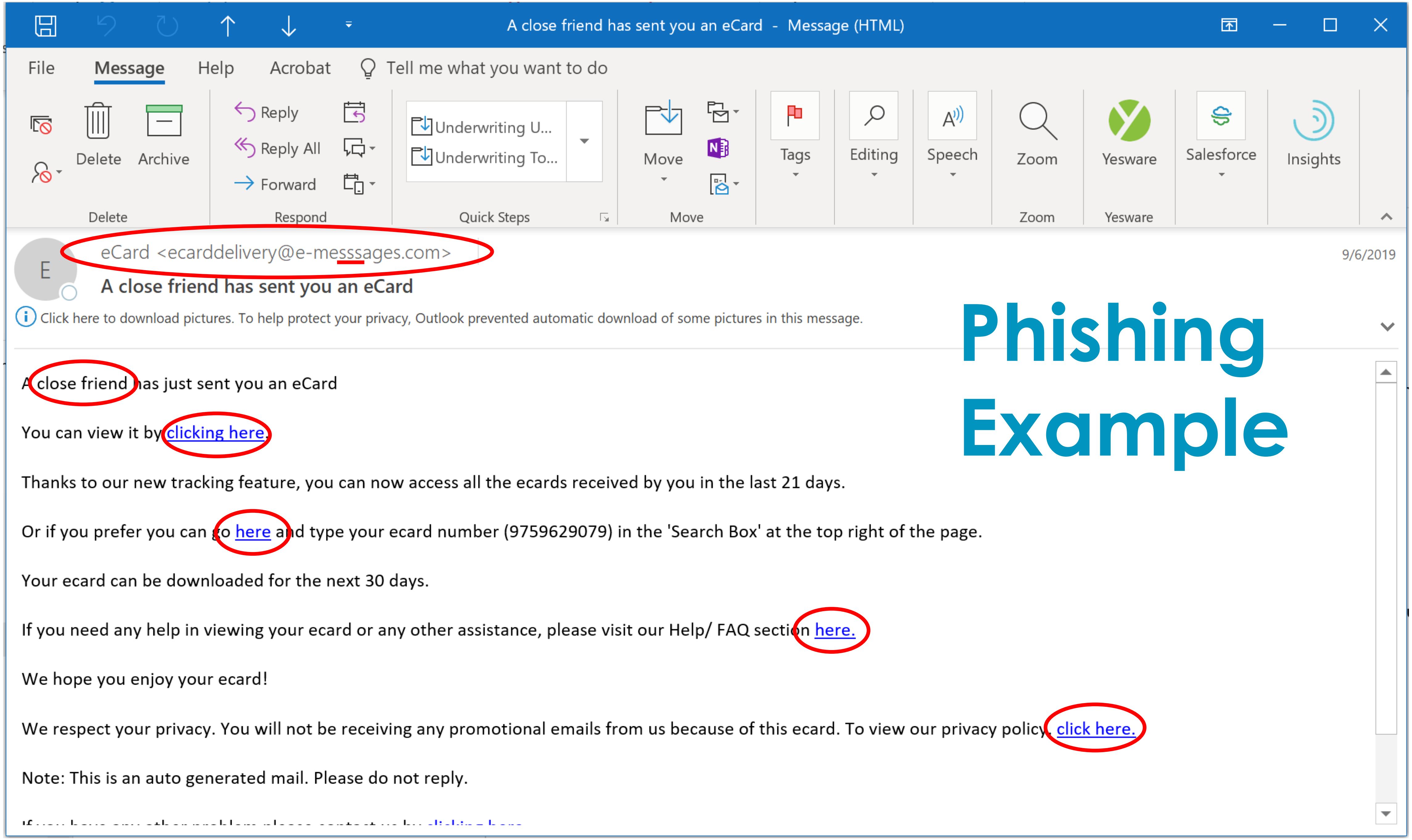
Sign in with your Microsoft account to join the family group.

Email, phone, or Skype

No account? Create one!

Sign in with Windows Hello or a security key ?

Phishing Example



eCard <ecarddelivery@e-messsages.com>

9/6/2019

A close friend has sent you an eCard

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

A close friend has just sent you an eCard

You can view it by clicking here.

Thanks to our new tracking feature, you can now access all the ecards received by you in the last 21 days.

Or if you prefer you can go here and type your ecard number (9759629079) in the 'Search Box' at the top right of the page.

Your ecard can be downloaded for the next 30 days.

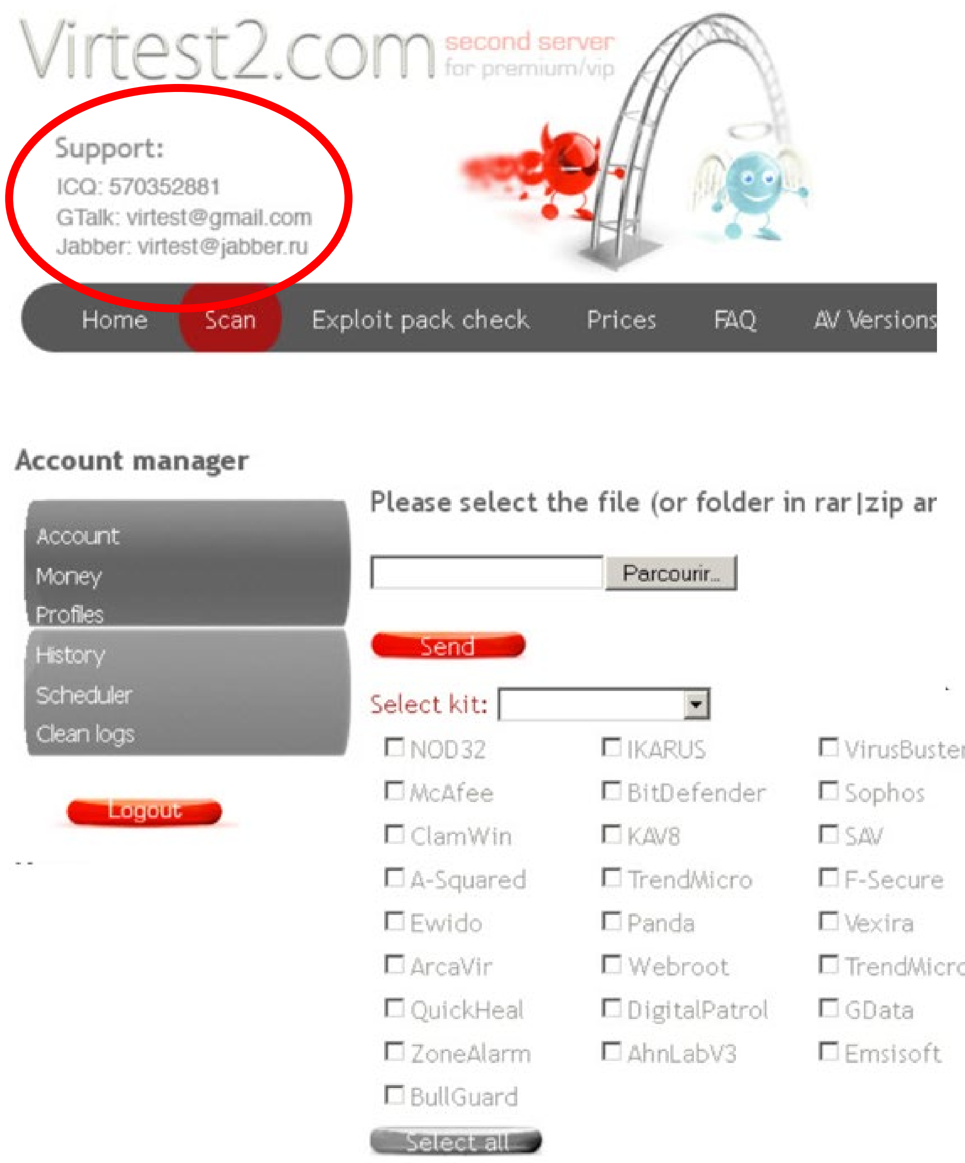
If you need any help in viewing your ecard or any other assistance, please visit our Help/ FAQ section here.

We hope you enjoy your ecard!

We respect your privacy. You will not be receiving any promotional emails from us because of this ecard. To view our privacy policy, click here.

Note: This is an auto generated mail. Please do not reply.

If you have any other problem please contact us by clicking here



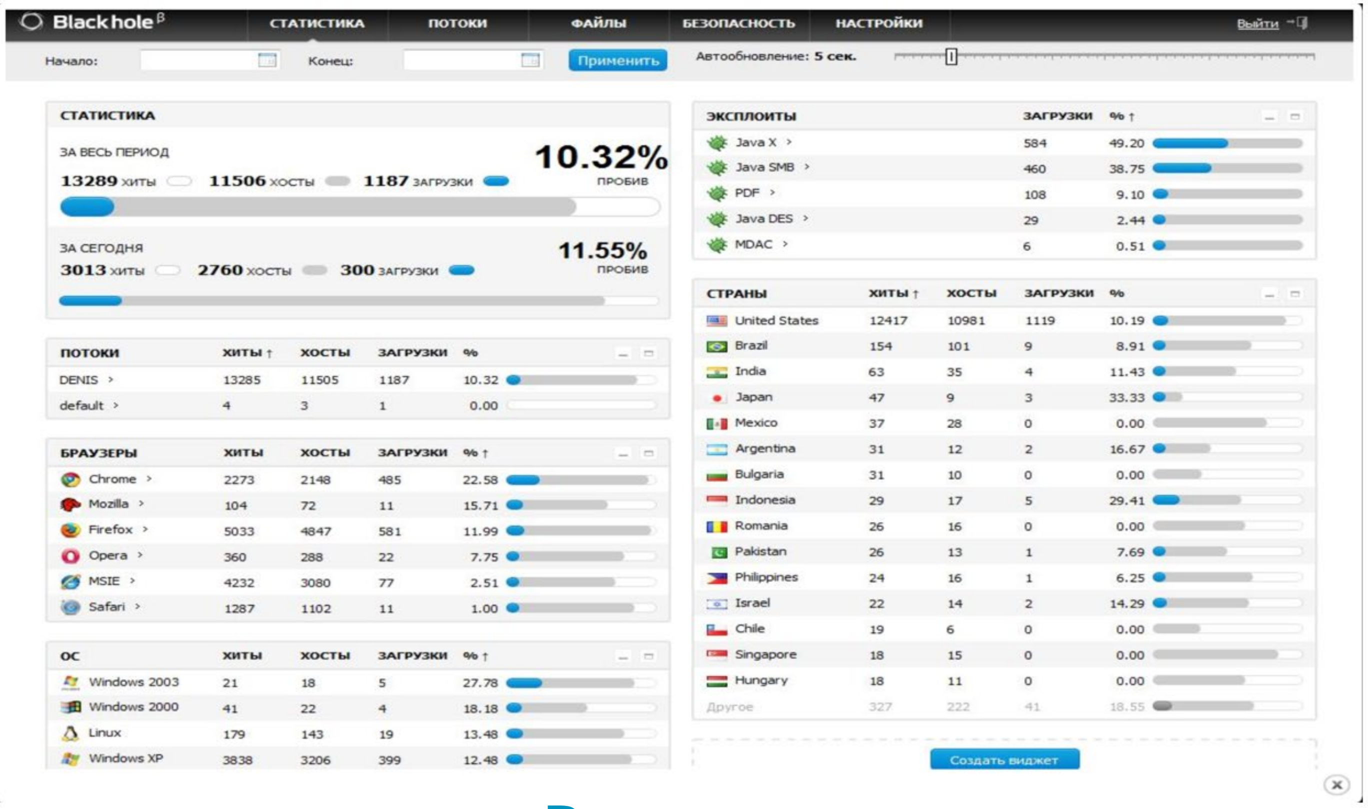
Support:
ICQ: 570352881
GTalk: virtest@gmail.com
Jabber: virtest@jabber.ru

Account manager

Please select the file (or folder in rar|zip ar

Select kit:

☐ NOD32
☐ McAfee
☐ ClamWin
☐ A-Squared
☐ Ewido
☐ ArcaVir
☐ QuickHeal
☐ ZoneAlarm
☐ BullGuard
☐ IKARUS
☐ BitDefender
☐ KAV8
☐ TrendMicro
☐ Panda
☐ Webroot
☐ DigitalPatrol
☐ AhnLabV3
☐ VirusBuster
☐ Sophos
☐ SAV
☐ F-Secure
☐ Vexira
☐ TrendMicro2010
☐ GData
☐ Emsisoft
☐ DrWeb
☐ eTrust
☐ Vba32
☐ OneCare
☐ Norman
☐ Comodo
☐ AVL
☐ SAS
☐ Avast
☐ AVG8
☐ F-Prot
☐ Avira
☐ Solo
☐ Rising
☐ IkarusT3
☐ ViRobot



Начало: Конец: Автообновление: 5 сек.

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД
13289 ХИТЫ 11506 ХОСТЫ 1187 ЗАГРУЗКИ
10.32% ПРОБИВ

ЗА СЕГОДНЯ
3013 ХИТЫ 2760 ХОСТЫ 300 ЗАГРУЗКИ
11.55% ПРОБИВ

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58
Mozilla ›	104	72	11	15.71
Firefox ›	5033	4847	581	11.99
Opera ›	360	288	22	7.75
MSIE ›	4232	3080	77	2.51
Safari ›	1287	1102	11	1.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78
Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
Java DES ›	29	2.44
MDAC ›	6	0.51

СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29
Chile	19	6	0	0.00
Singapore	18	15	0	0.00
Hungary	18	11	0	0.00
Другое	327	222	41	18.55

Ransomware as a Service (RaaS) Platforms

- **Commercialized Exploit Packets**
- **Help Hotlines**
- **Management System**

GROUPS UNDER ATTACK

5 TARGETS OF RANSOMWARE

By Industry:

- Unknown : 5434
- Public administration : 2792
- Finance : 2527
- Professional Services: 3566
- **Manufacturing : 2337**

5 TARGETS OF RANSOMWARE

By Company Size:

3 to 1
Small vs Medium to Large Business

Why Manufacturing ??

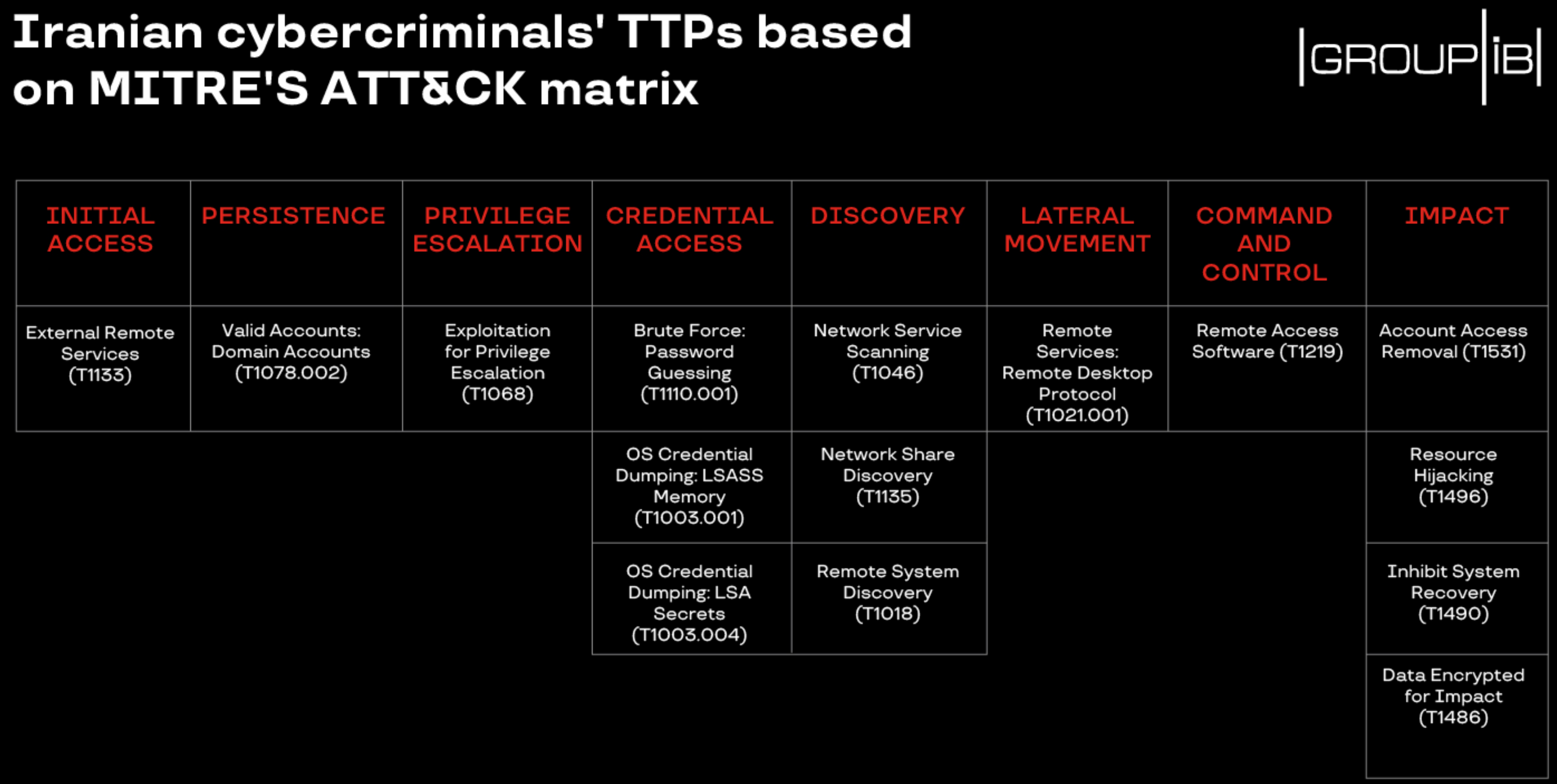
1. Legacy Equipment with software that is outdated (PLC, CNC's are using windows xp still
2. Networks were setup quickly and security was being considered
3. Open sharing which makes it easy for an attack
4. Some ERP software providers tell manufacturers you don't need security
5. Proper network backups are not in place
6. Still using Hotmail, yahoo or gmail for business communications
7. Nobody knows who I am
8. Tend to deal with things when they absolutely have to

HOW TO PROTECT YOUR BUSINESS

Network Risk Assessment is a Must

- Anti-Virus that is SOC monitored

- Anti-Virus that is SOC monitored
- MDR Solution (managed detection and response)



Iranian cybercriminals' TTPs based on MITRE'S ATT&CK matrix

INITIAL ACCESS	PERSISTENCE	PRIVILEGE ESCALATION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COMMAND AND CONTROL	IMPACT
External Remote Services (T1133)	Valid Accounts: Domain Accounts (T1078.002)	Exploitation for Privilege Escalation (T1068)	Brute Force: Password Guessing (T1110.001)	Network Service Scanning (T1046)	Remote Services: Remote Desktop Protocol (T1021.001)	Remote Access Software (T1219)	Account Access Removal (T1531)
			OS Credential Dumping: LSASS Memory (T1003.001)	Network Share Discovery (T1135)			Resource Hijacking (T1496)
			OS Credential Dumping: LSA Secrets (T1003.004)	Remote System Discovery (T1018)			Inhibit System Recovery (T1490)
							Data Encrypted for Impact (T1486)

- Anti-Virus that is SOC monitored
- MDR Solution (managed detection and response)
- Access Controls

Examples: Azure AD, JumpCloud or a Server

- Anti-Virus that is SOC monitored
- MDR Solution (managed detection and response)
- Access Controls
- Email filtering and using a business .com

- Anti-Virus that is SOC monitored
- MDR Solution (managed detection and response)
- Access Controls
- Email filtering and using a business .com

- Anti-Virus that is SOC monitored
- MDR Solution (managed detection and response)
- Access Controls
- Email filtering and using a business .com
- MFA on Email and online business solutions

- Anti-Virus that is SOC monitored
- MDR Solution (managed detection and response)
- Access Controls
- Email filtering and using a business .com
- MFA on Email and online business solutions
- Backups on Data that's in house

- Anti-Virus that is SOC monitored
- MDR Solution (managed detection and response)
- Access Controls
- Email filtering and using a business .com
- MFA on Email and online business solutions
- Backups on Data that's in house
- Firewall monitoring or a Follow-Me-Firewall

We will provide 30 assessments for free for AWFS Members

We will provide Run a Dark Web Scan to see if any company information out there for Free www.maddata.io/network-assessment/

MAD DATA

Brian.Hamilton@maddata.io

5404885752

linkedin.com/in/brian-hamilton-8474bb166