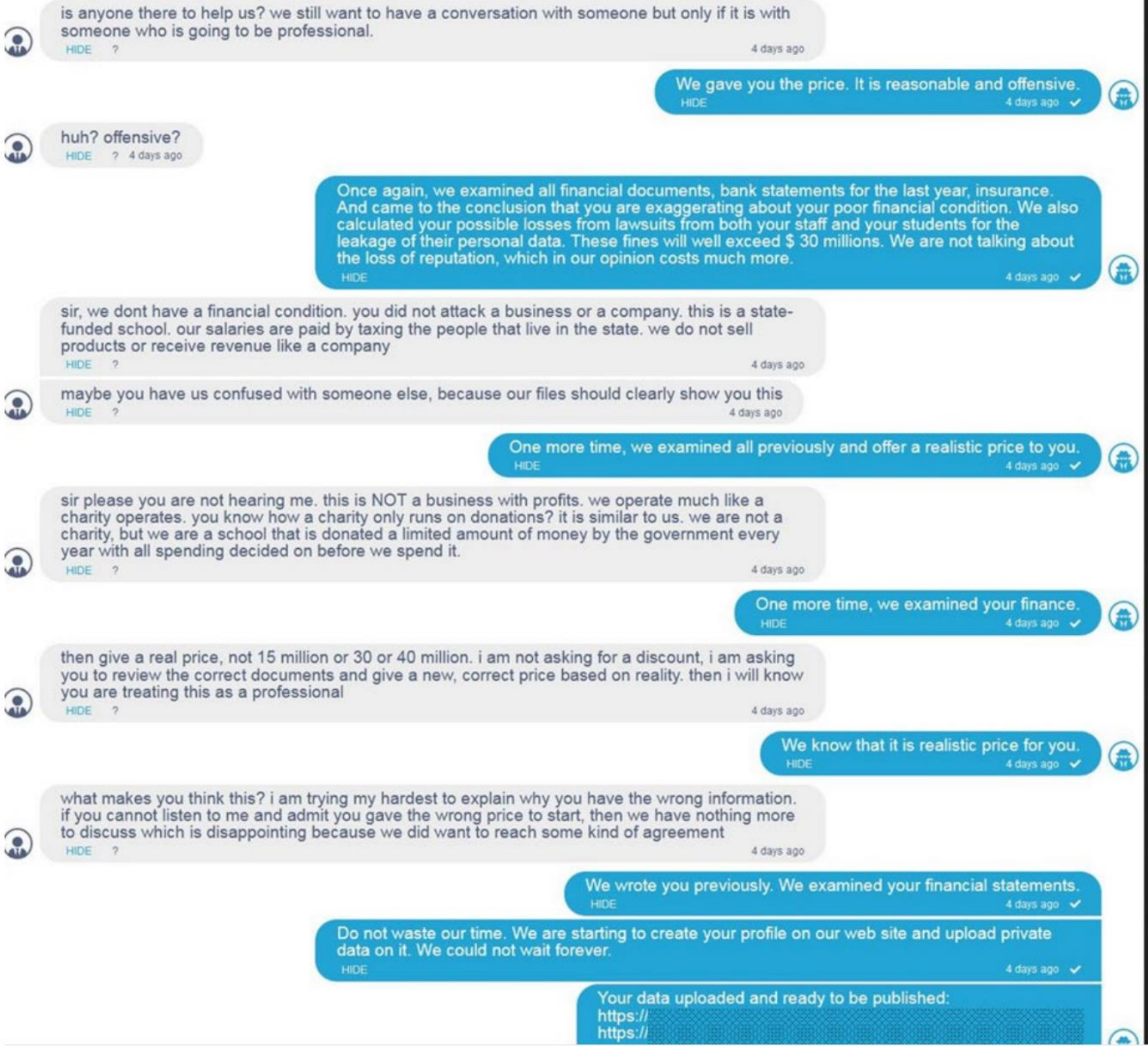


CYBER HOSPITALITY 2021

David Caswell, PhD

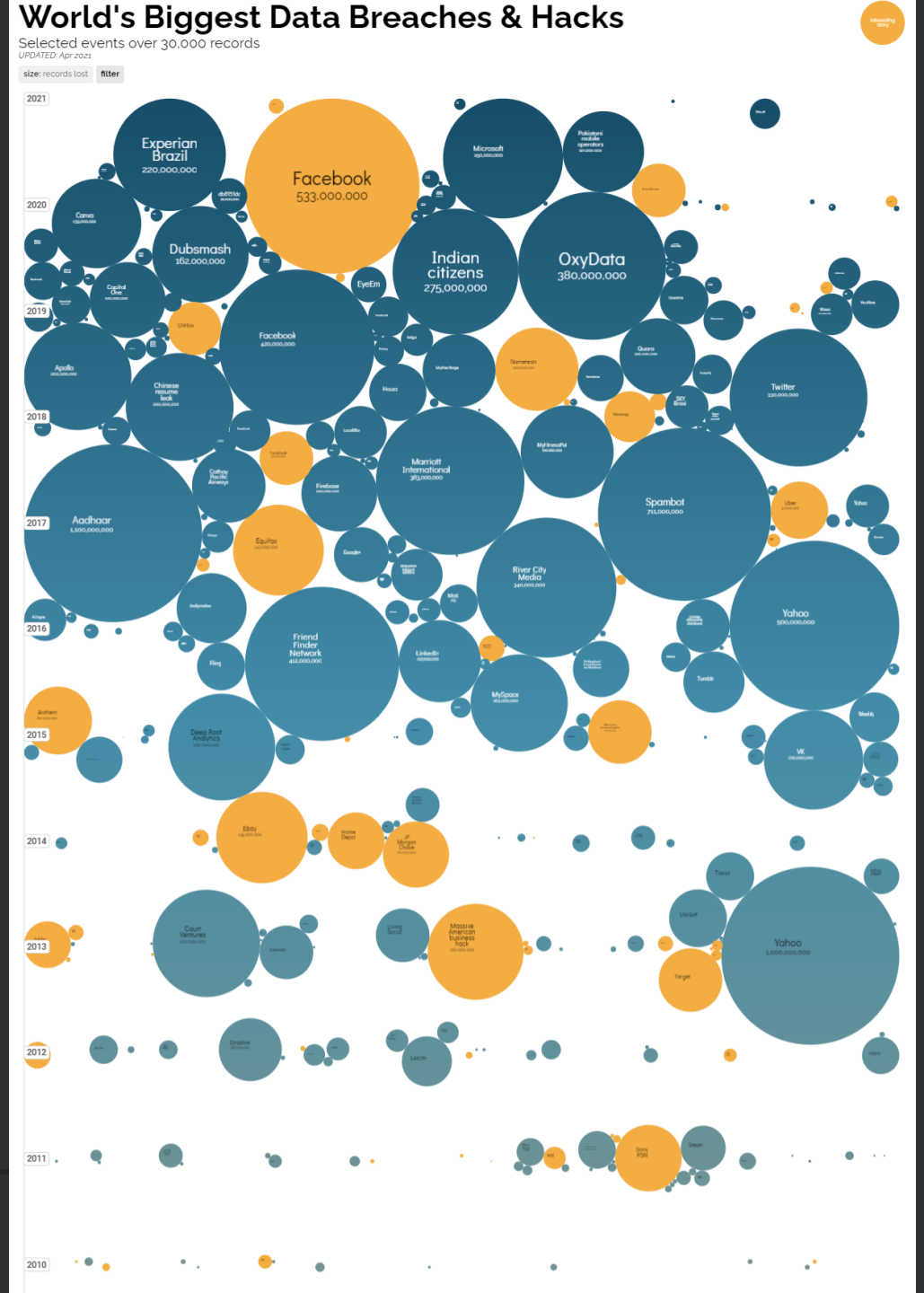
Microsoft, Critical Infrastructure and Cybersecurity

CYBERSECURITY LANDSCAPE - 2021

2020

2018

2010

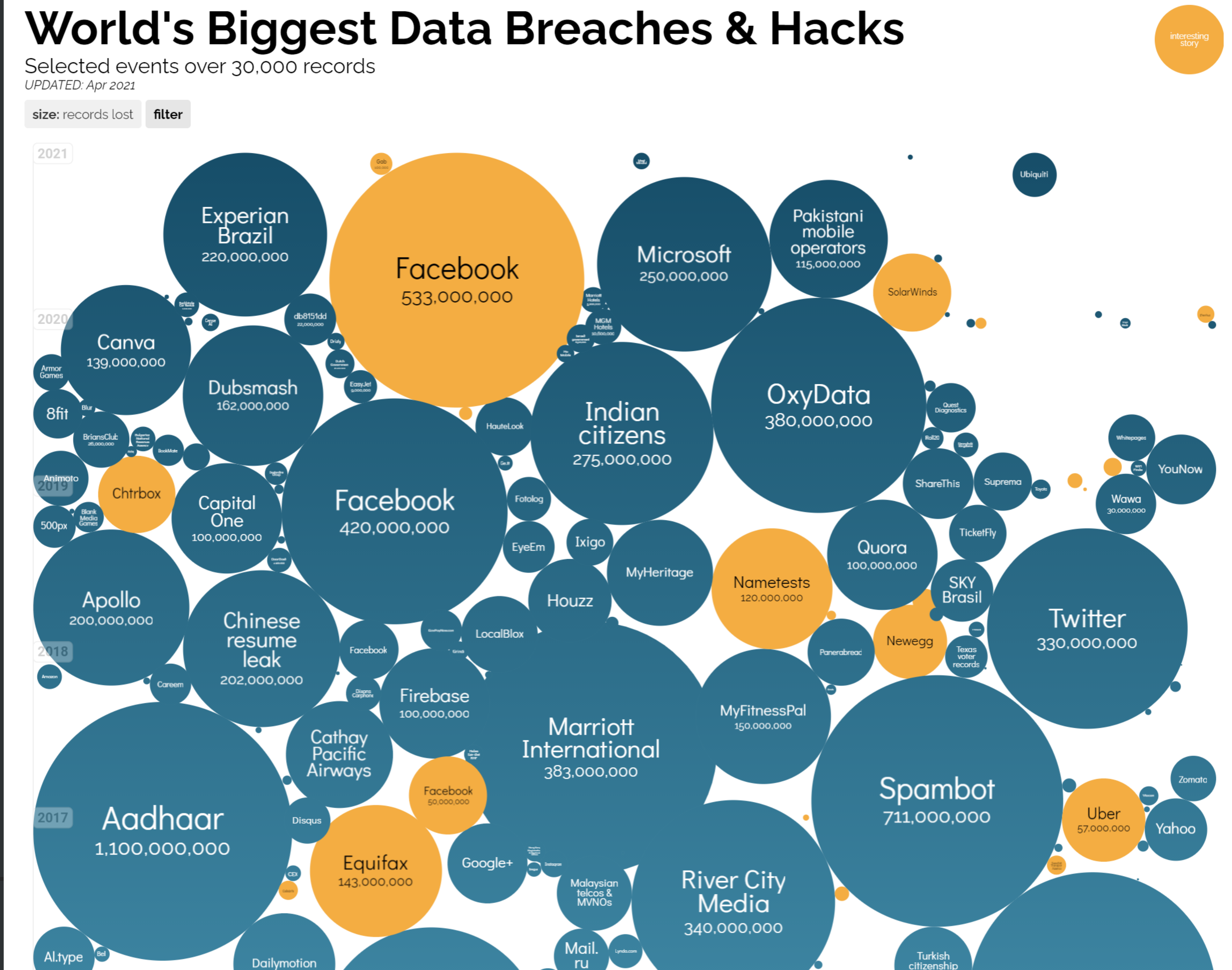


[World's Biggest Data Breaches & Hacks — Information is Beautiful]

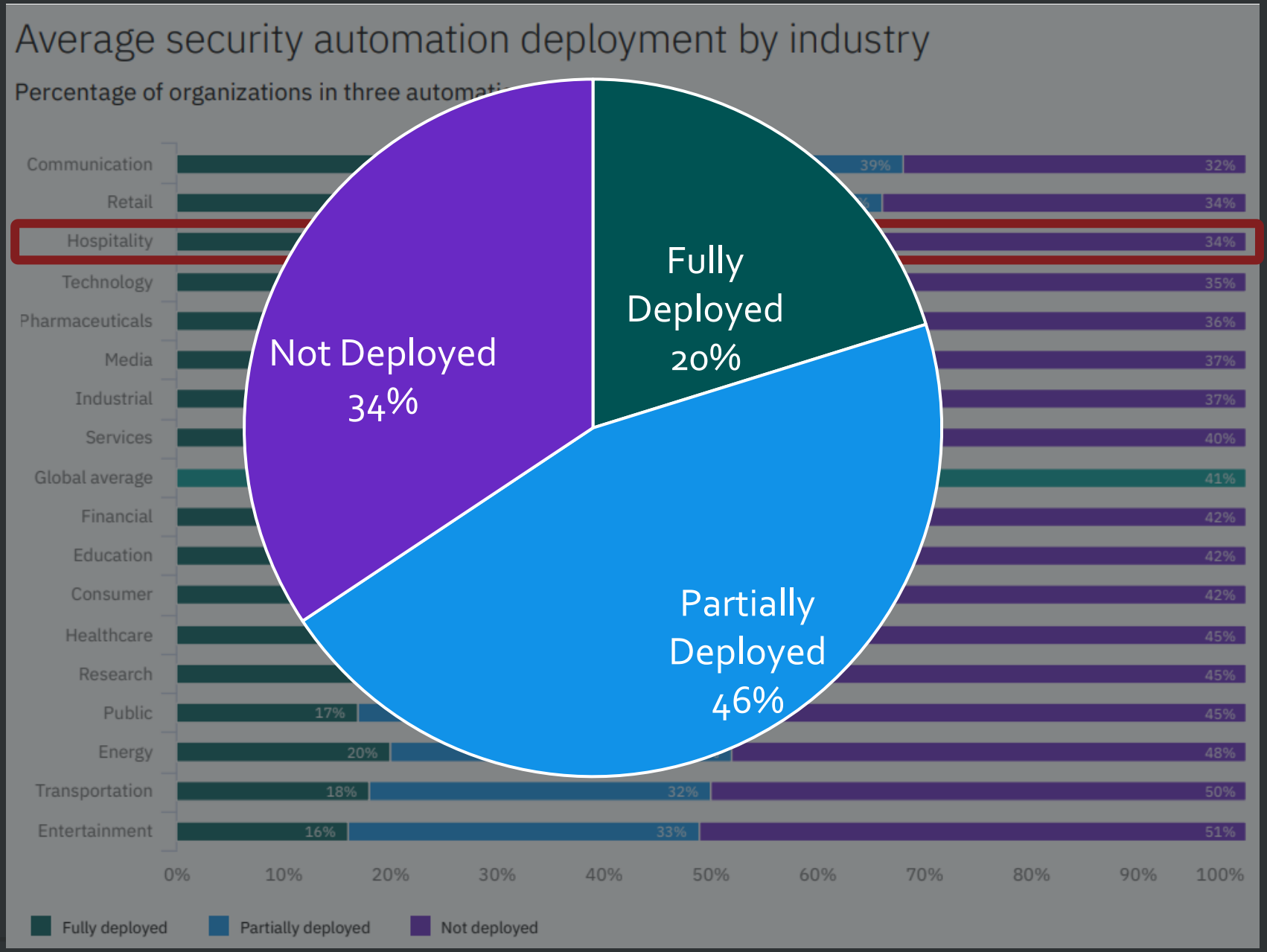
2020

2019

2018



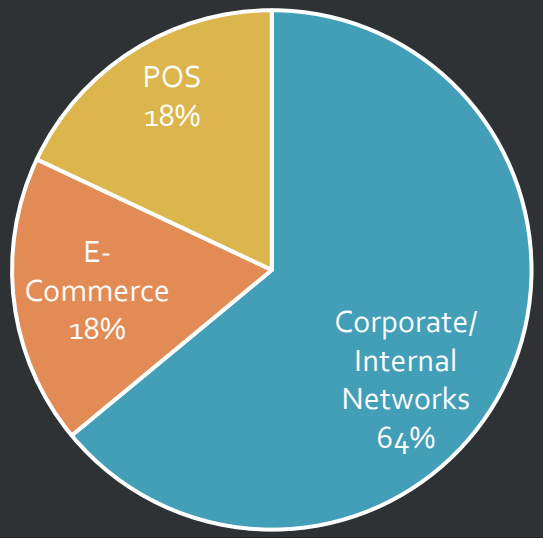
[World's Biggest Data Breaches & Hacks — Information is Beautiful](#)

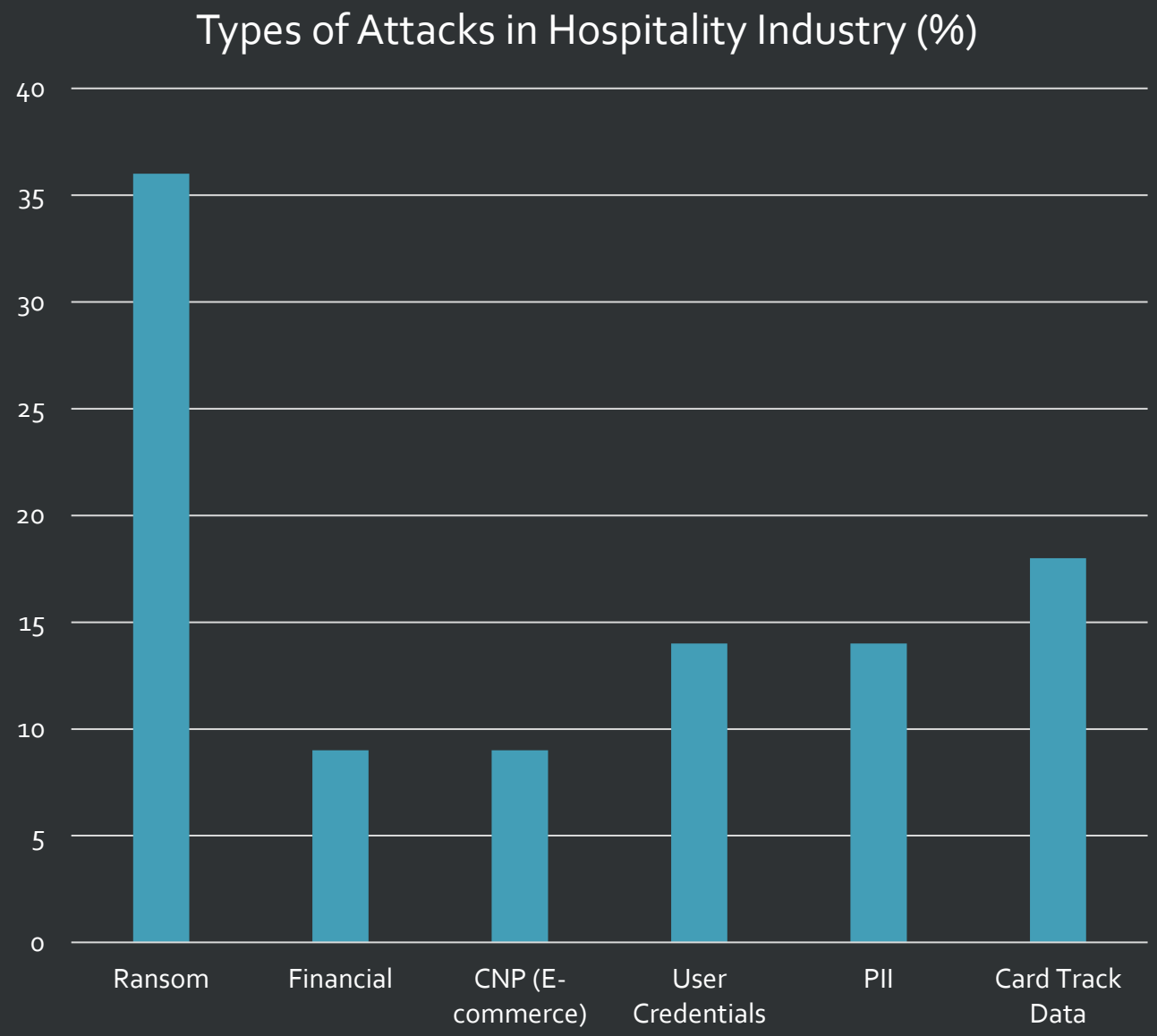


IBM Ponemon, Global Cost of Data Breach Study 2020

Attacks on the Hospitality Industry (2020)

Hospitality Industry Environments Compromised

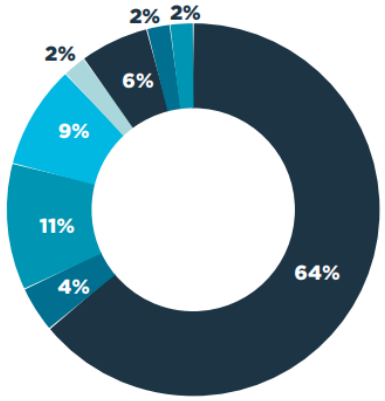




[2020 Trustwave Global Security Report | Trustwave]

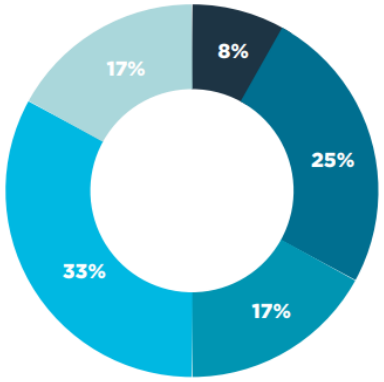
Sources of Compromise

Corporate/Internal Network



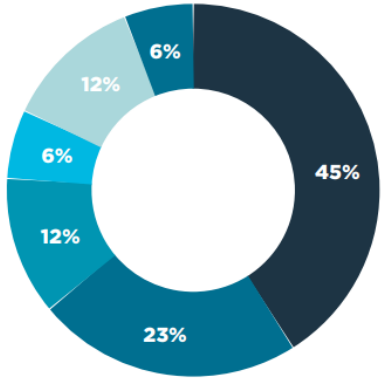
64% Phishing/SE
4% Application Exploit
11% Malicious Insider
9% Weak password
2% Code Injection
6% Service Provider
2% Credential Stuffing
2% Other

E-Commerce



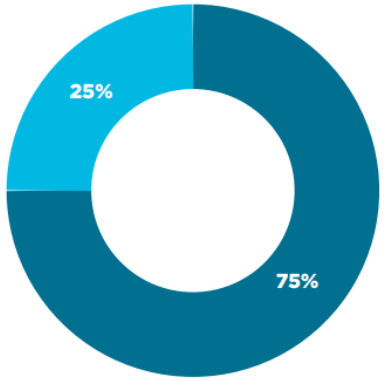
8% Phishing/SE
25% Application Exploit
17% Malicious Insider
33% Code Injection
17% Other

Cloud



45% Phishing/SE
23% Application Exploit
12% Malicious Insider
6% Weak password
12% Credential Stuffing
6% Other

POS



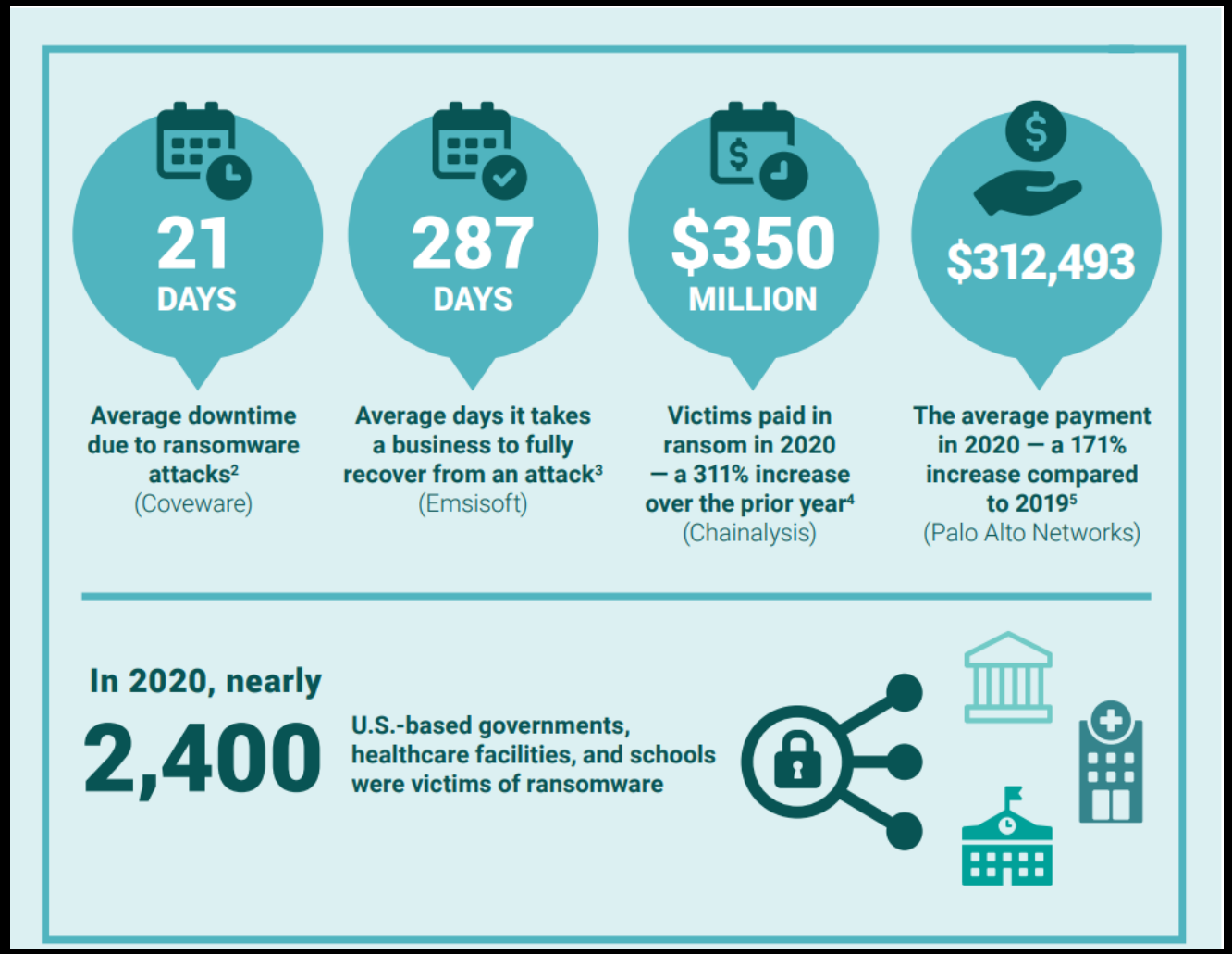
75% Phishing/SE
25% Service Provider

[2020 Trustwave Global Security Report | Trustwave]


CONTI recovery service
HOW I GOT HERE?
If you are looking at this page right now, that means that your network was succesfully breached by CONTI team.
All of your files, databases, application files etc were encrypted with military-grade algorithms.
If you are looking for a free decryption tool right now - there's none.
Antivirus labs, researches, security solution providers, law agencies won't help you to decrypt the data.

RANSOMWARE

By the numbers (Q1 2021)



Institute for Security and Technology (IST) » Ransomware Task Force (RTF)

Terms

- **Ransomware**
  - A cyber attack whereby a victim's data is encrypted and/or stolen with the intent of holding said data hostage for financial or other blackmail purposes
  - Short-term for the ransomware encryptor software

- **Ransomware Encryptor** – the software used to encrypt/decrypt and/or extract data from a victim

- **Ransomware as a Service (RaaS)** – the business service of ransomware whereby different groups are responsible for different components of a ransomware attack thereby significantly reducing the barrier to entry for criminals

What is a Ransomware Attack?

1) Files are encrypted and held for ransom
2) Backups are deleted

Attention!

| What happened?

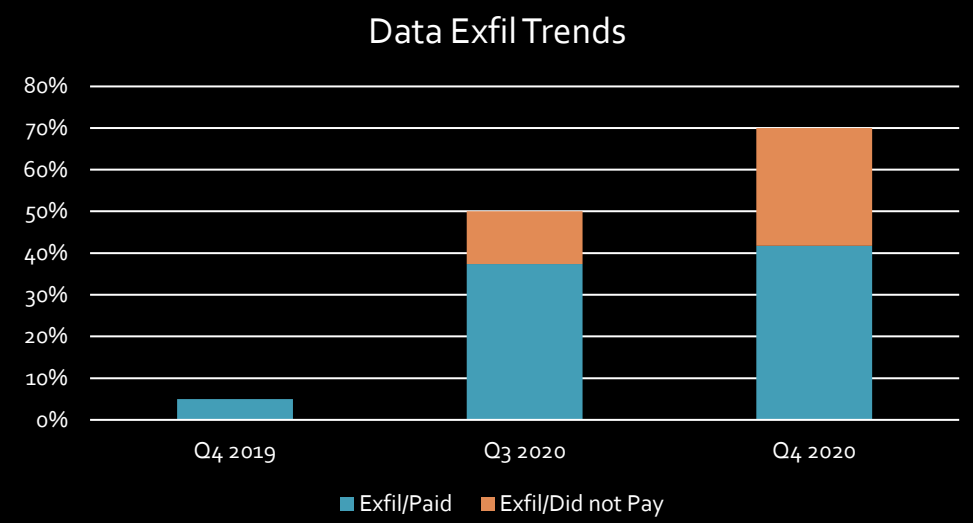
We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

We have also downloaded a lot of data from your network, so in case of not paying this data will be released.
If you dont believe we have any data you can contact us and ask a proof, also you can google [redacted]

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

| How to contact us and get my files back?

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored on our servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.



What is a Ransomware Attack?

1) Files are encrypted and held for ransom
2) Backups are deleted
3) Files are exfiltrated and held hostage

The message displayed at the top of the Maze Ransomware public shaming site.

[Ransomware Payments Decline in Q4 2020 (coveware.com)]
[The Marriage of Data Exfiltration and Ransomware (coveware.com)]
[Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up – Krebs on Security]

If you get Attacked…

Direct Costs

2013 - ~$1K to decrypt
2015 - ~$20K
2021- $100K to $10M

Average Ransom Payment

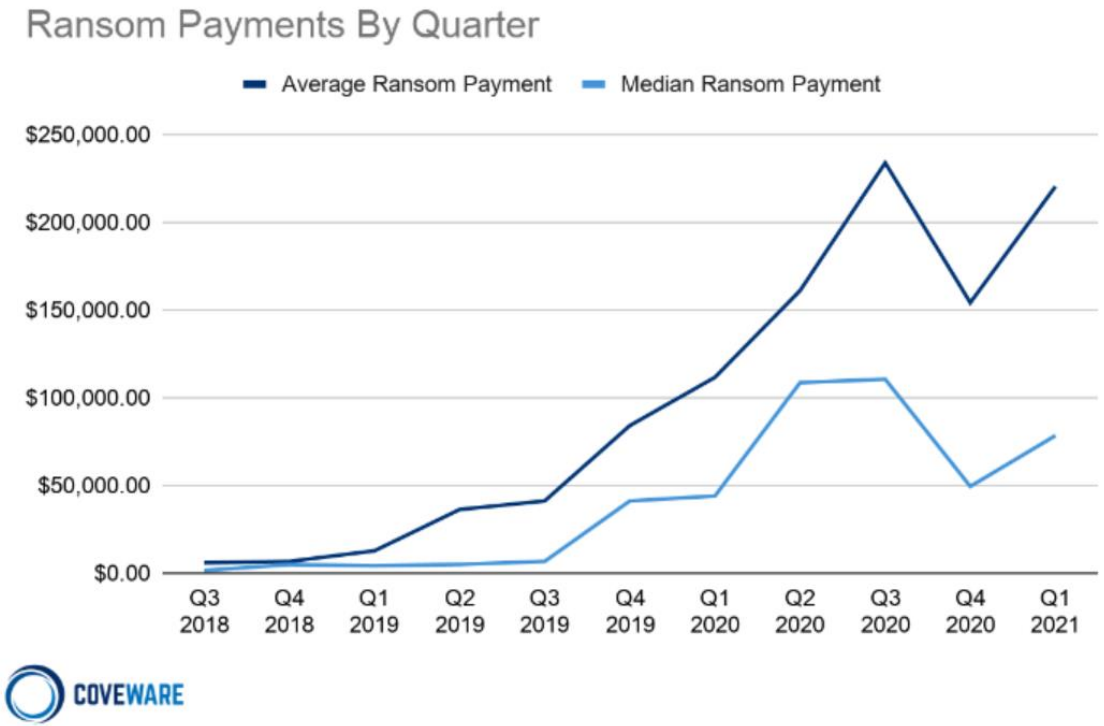
$220,298

+43% from Q4 2020

Median Ransom Payment

$78,398

+59% from Q4 2020

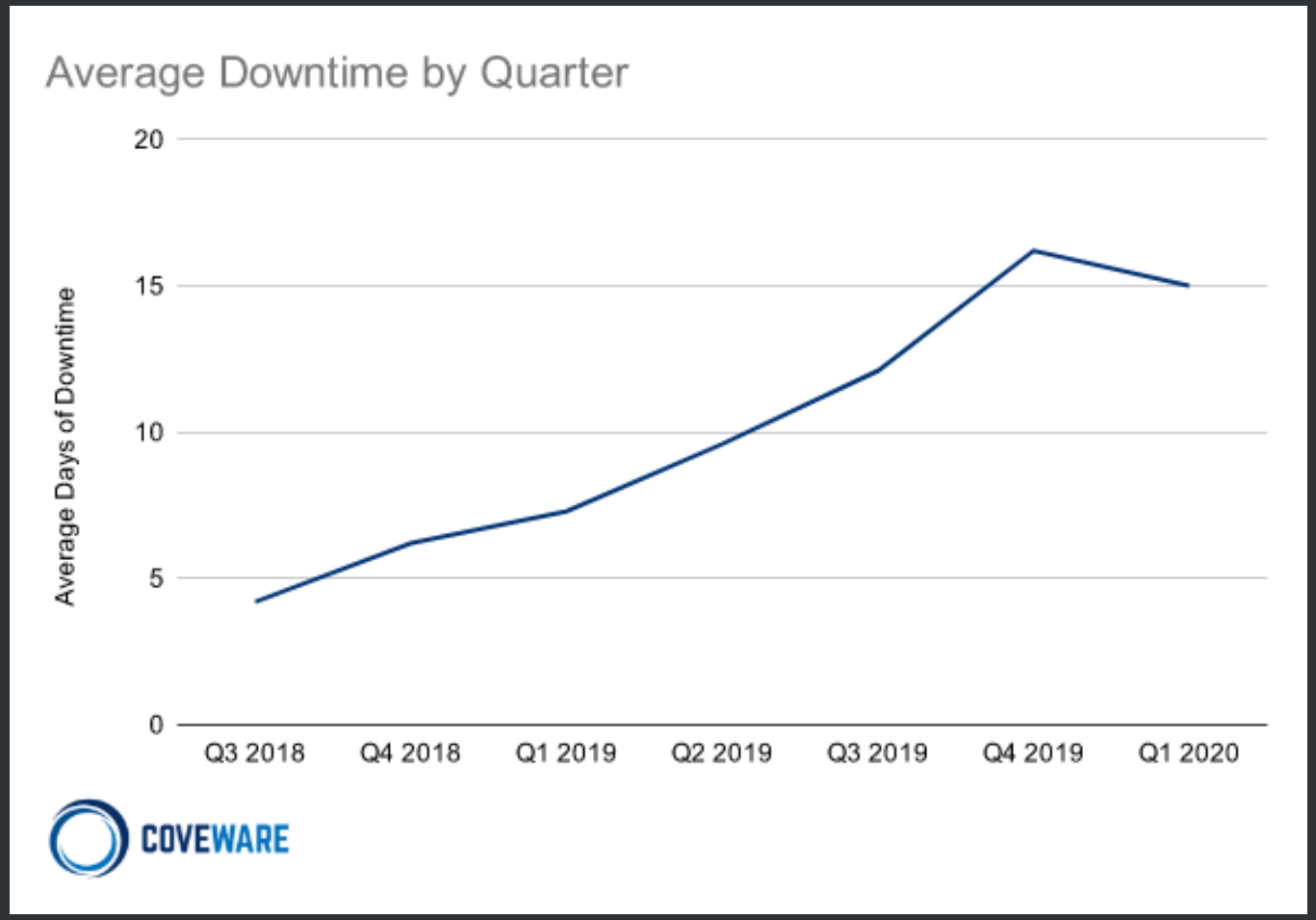


[Ransomware Attack Vectors shift as New Software Vulnerability Exploits Abound (coveware.com)]

If you get Attacked…

Indirect Costs

Q4 2020 – **21** days average downtime



[Ransomware Amounts Rise Threefold (coveware.com)]
[Ransomware Payments Decline in Q4 2020 (coveware.com)]

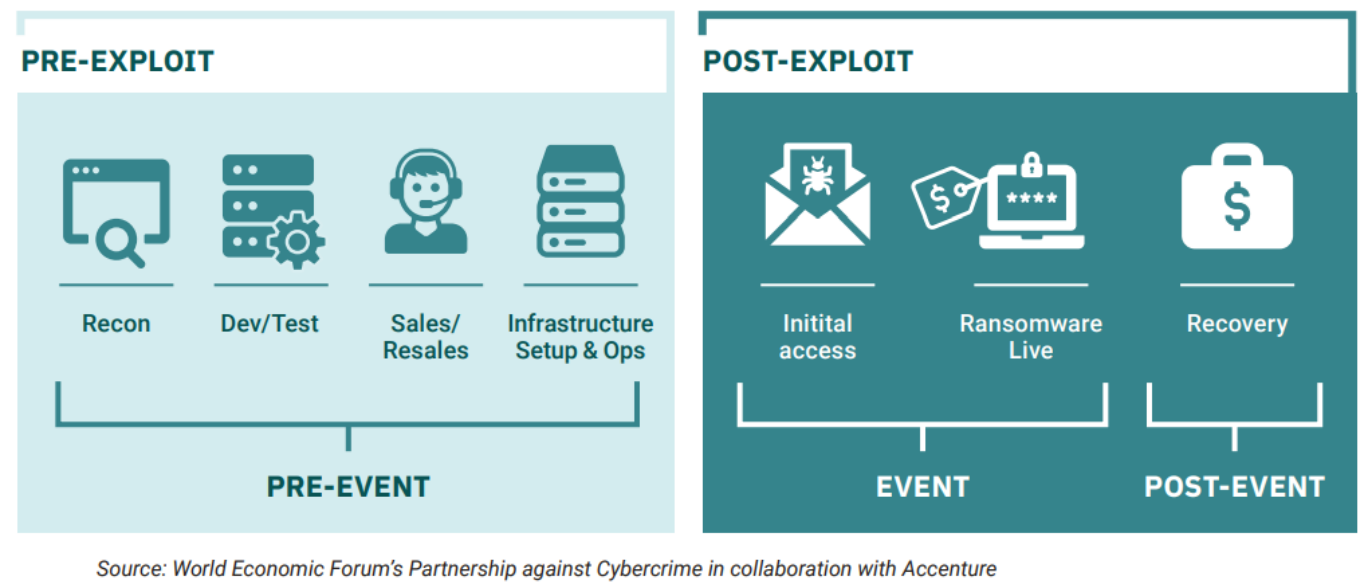
If you get Attacked…

Long Term Considerations

- If the attacker gained access to encrypt, you should assume:
  - They have access to the data on the encrypted machines and have stored an external copy (exfilled)
  - They have left additional backdoors to re-access your systems at will

- If the attacker has copied your data, you should assume:
  - They will continue to have a copy of the data (even if they state you will delete the data) and are able to blackmail you for the data any time in the future

Ransomware as a Service



Source: World Economic Forum's Partnership against Cybercrime in collaboration with Accenture

The Developer

Develops and licenses the malware for fixed fee/share of payment

The Affiliate

Executes the attack, collects the ransom, exploits the victim, brokers the funds

[Human-operated ransomware | Microsoft Docs]
[Institute for Security and Technology (IST) » Ransomware Task Force (RTF)]

ATT&CK Matrix for Enterprise

layout: side ▾ | show sub-techniques | hide sub-techniques

Reconnaissance
10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (7)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Internal Image
- Modify Authentication Process (4)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (7)
- Server Software Component (3)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (7)
- Valid Accounts (4)

Defense Evasion
39 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (7)
- Hijack Execution Flow (11)
- Impair Defenses (7)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (6)
- Modify Authentication Process (4)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (5)
- Pre-OS Boot (5)
- Process Injection (11)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11)
- Signed Script Proxy Execution (1)
- Subvert Trust Controls (6)
- Template Injection
- Traffic Signaling (1)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
15 techniques

- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Man-in-the-Middle (2)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (7)

Discovery
27 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Man in the Browser
- Man-in-the-Middle (2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

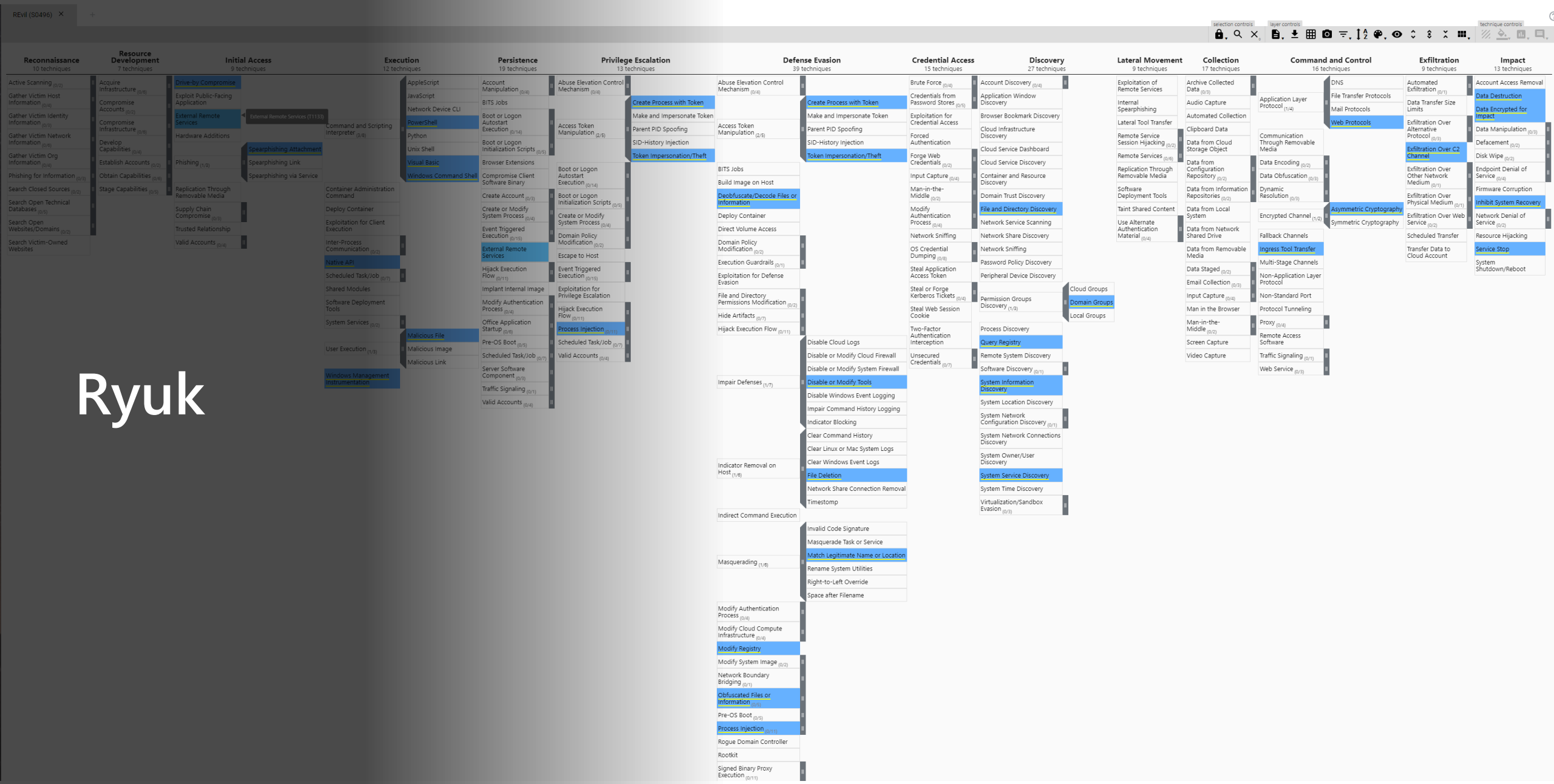
Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

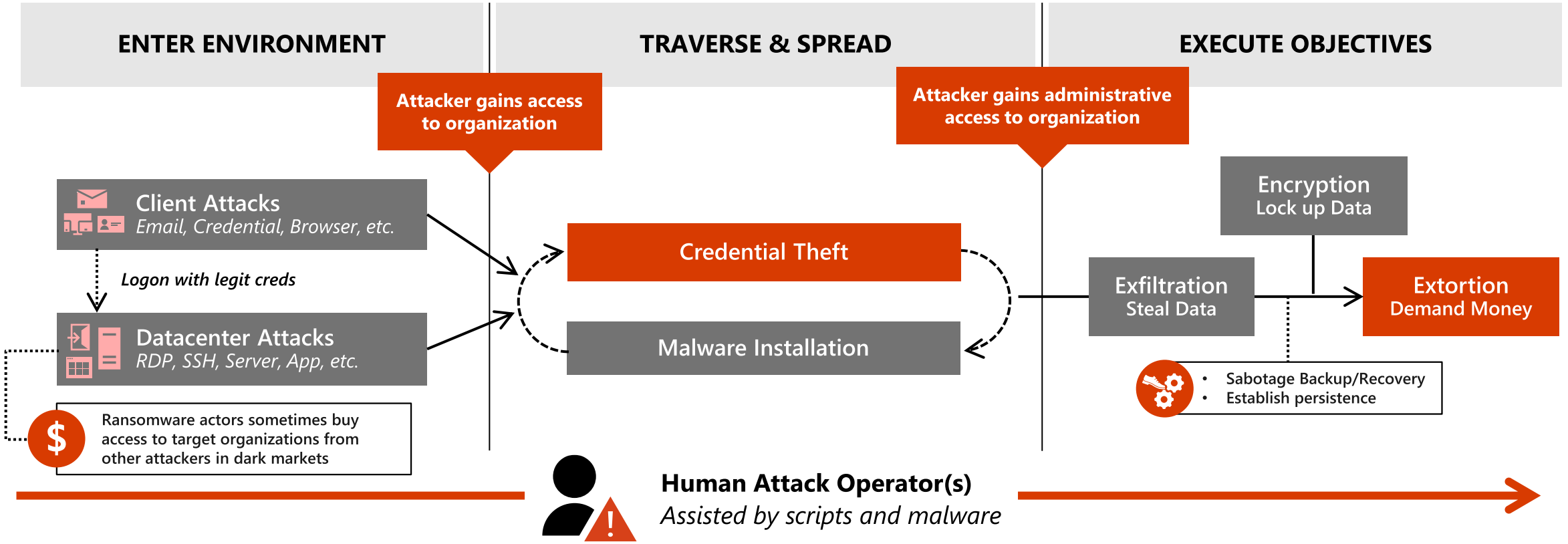
MITRE ATT&CK®



Ryuk

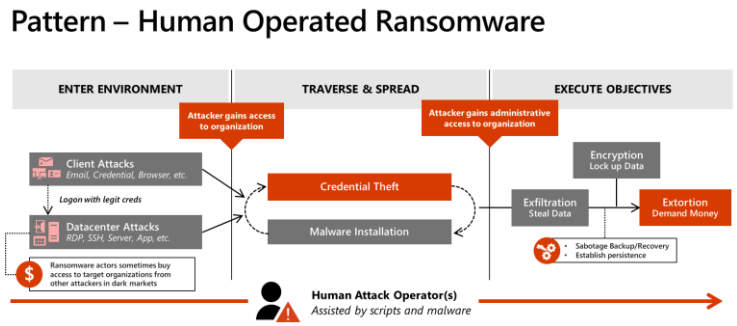
REvil, Software S0496 | MITRE ATT&CK®

Pattern – Human Operated Ransomware

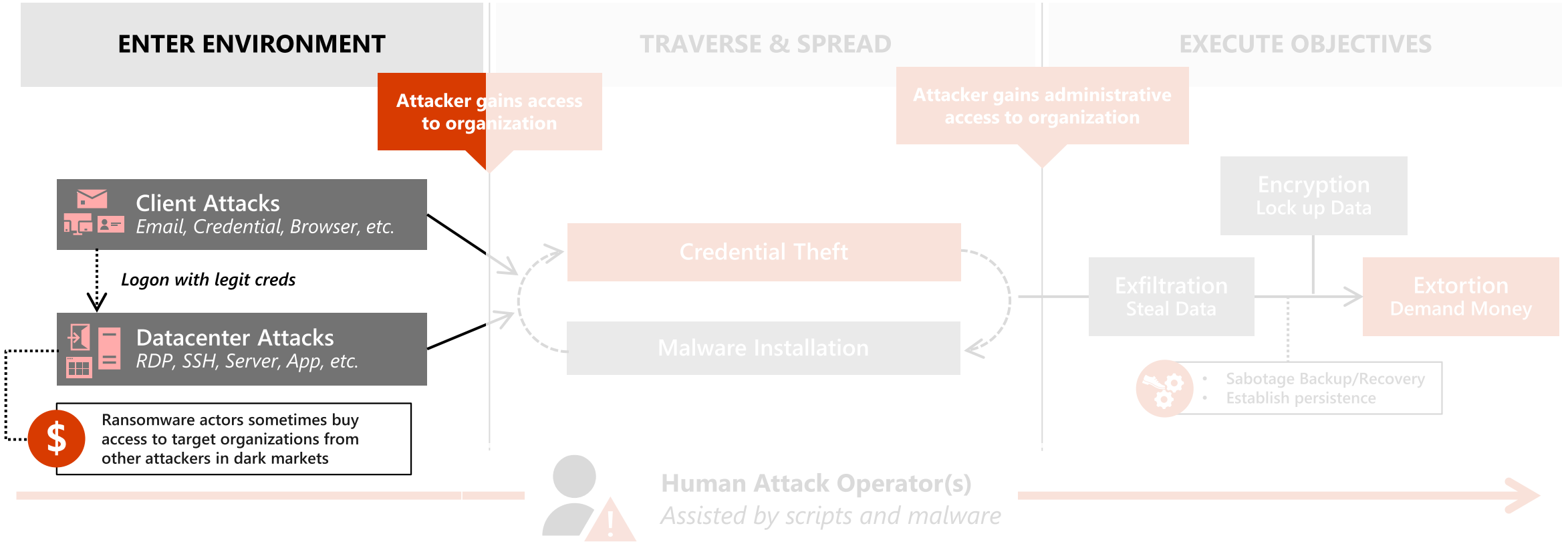


[Human-operated ransomware | Microsoft Docs]

DEFENSE IN DEPTH



Pattern – Human Operated Ransomware



[Human-operated ransomware | Microsoft Docs]

Phishing Attacks

BEC Type	Typical Subject Lines	Description
Vendor Payment or Invoice	Urgent Assistance needed Are you at your desk? Request Available? Invoice payment	Scammer impersonates the CEO or CFO and asks someone in Finance to urgently send a payment to a vendor or other party.
Gift Cards	Need your help Quick Task Favor	Scammer impersonates the CEO, CFO or other manager and asks an employee to purchase gift cards (iTunes for example), scratch them, take a photo and send the image. Scammer then redeems the cards.
Payroll Change	Payroll Update DD Update Direct Deposit Change Change Bank Info	Scammer impersonates an employee and asks HR staff to change the bank account for salary deposits.
BEC Type	**Typical Subject Lines**	**Description**
Phone Number	Hello [person] Quick Request	Scammer impersonates the CEO, CFO or other manager and asks an employee for cell phone number, from where a text message conversation occurs.
Altered Invoice	Varies according to actual email correspondence	Scammer obtains access to real email accounts through credential phishing and monitors email looking for suitable invoices or transactions about to happen. Scammer then injects themselves in the middle of the email conversation and supplies an altered invoice, closely resembling the original, except for the bank account details.

2020 Trustwave Global Security Report

- Be wary of emails from external addresses (Gmail.com, Aol.com, RR.Com, Lycos.com, etc)

- Email Defenses:
  - Lock down inbound traffic – particularly with attachments (.vbs, .js, .cpl, .chm, .lnk, etc)
  - Block/flag Macros from executing
  - Ensure anti-spoofing technologies deployed
  - Educate your employees!

Have a Defense Mindset

- Emails from "management" on policies (e.g., with pdfs containing malware, links, or files with macros)
- Photos of complaint evidence (with a link or embedded malware)
- "Please can I use the computer, I lost my passport and phone…"

Be Wary of Links

http://www.ThisAppearsToBeGood.com/

This appears to be a good site

Protect your Accounts

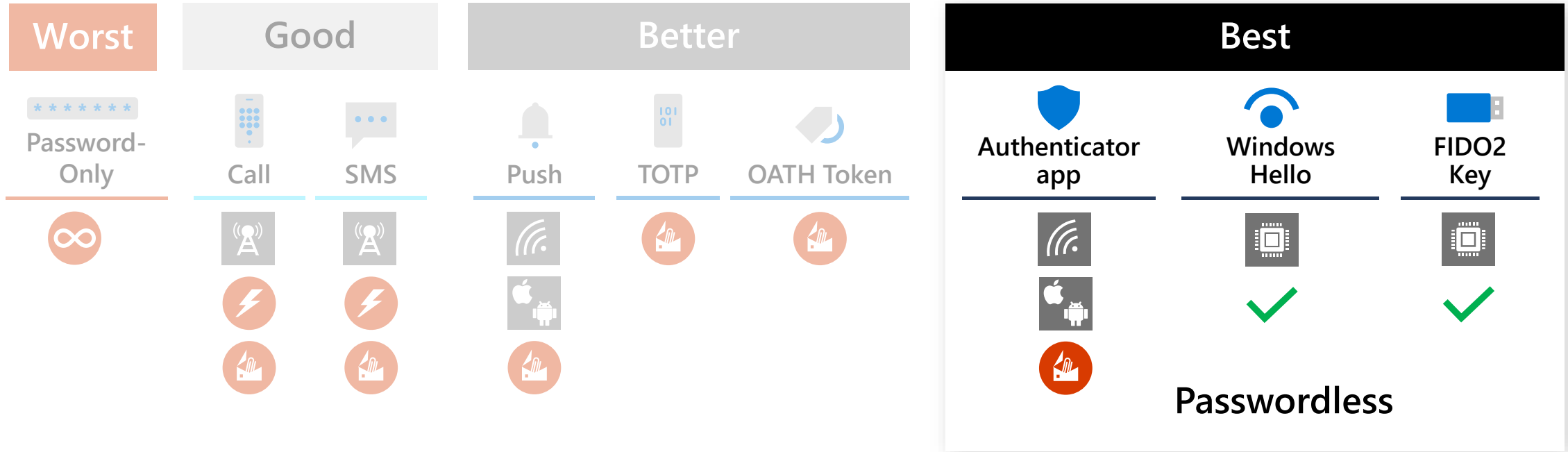
- Use multi-factor authentication on all accounts– particularly administrators
- NEVER share accounts
- Apply least-privilege policy to all accounts

"Coveware has NEVER seen a ransomware attack, where domain administrator credentials were compromised after multifactor authentication (mobile, not token based) was overcome. 100% of ransomware attack victims LACK true multi factor authentication for the domain administration accounts."

Take the Advice of Ransomware Actors: Prevent Escalation and Lateral Movement (coveware.com)

Strong Multi-Factor Authentication

The best options aren't that difficult



[Human-operated ransomware | Microsoft Docs]

Step 1 – get the app

(as a note: this can be used for both your business and personal accounts)

Cyber Hygiene

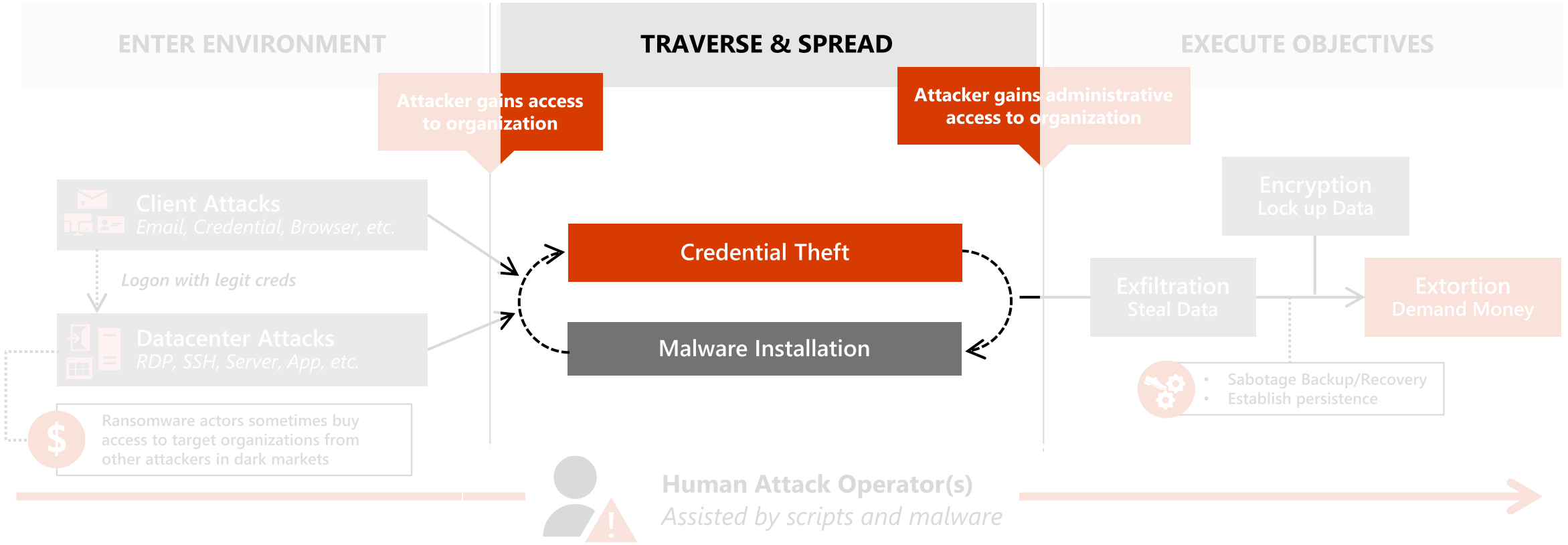
- Patch operating system and software
- Ensure security features are active and up-to-date
  - Antivirus or better
  - Secure network access
    - Wifi WPA3 encryption
    - MAC Address White-Listing
- Lock down unnecessary comms including disabling/securing:
  - Remote Desktop Protocol (RDP)
  - Internal Server Message Block (SMB) v1/v2
  - Block all external SMB

CVE	Description
CVE-2018-0802	Equation Editor - Microsoft Office Memory Corruption Vulnerability
CVE-2017-1882	Equation Editor - Microsoft Office Memory Corruption Vulnerability
CVE-2014-6352	OLE Remote Code Execution Vulnerability
CVE-2017-0199	Microsoft Office/WordPad Remote Code Execution Vulnerability
CVE-2015-1641	Microsoft Office Memory Corruption Vulnerability
CVE-2012-0158	MSCOMCTL.OCX RCE Vulnerability

Top email malware exploits in 2019 (Trustwave, 2020)

[CISA MS-ISAC Ransomware Guide]
[Good Security Habits | CISA]
[Securing Wireless Networks | CISA]

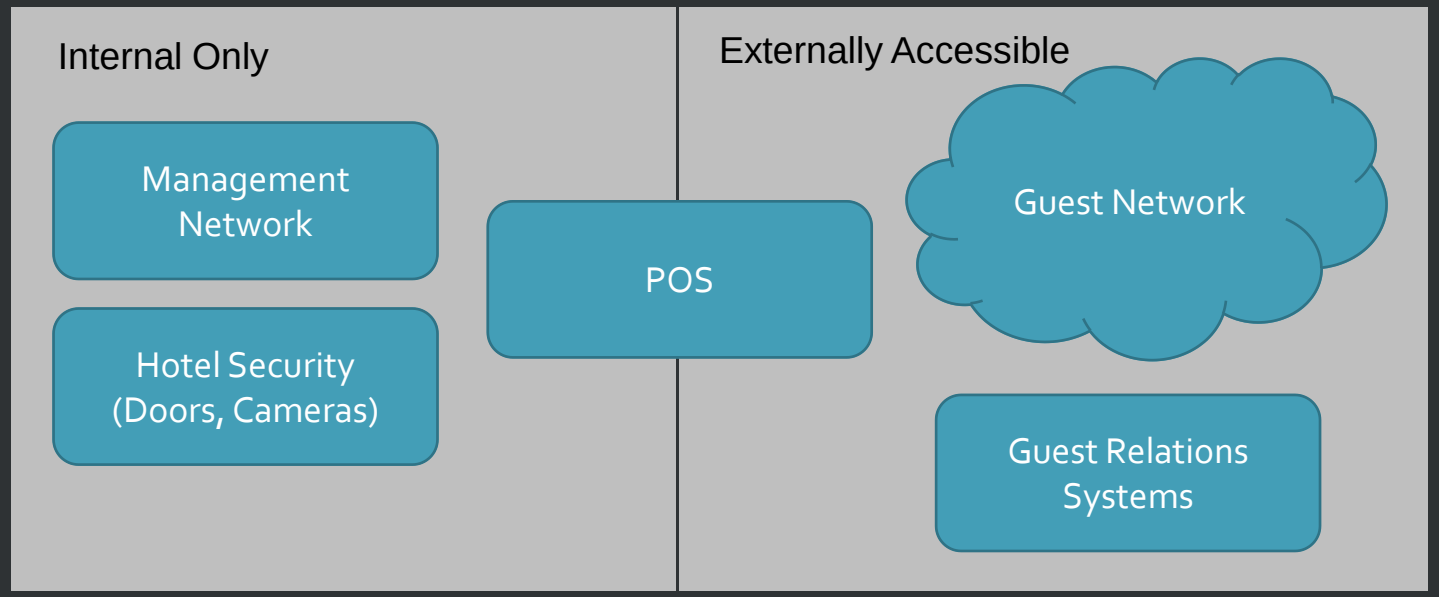
Pattern – Human Operated Ransomware



[Human-operated ransomware | Microsoft Docs]

Prevent Lateral movement and privilege escalation

- Minimize administrator access to devices
- Minimize number of administrators
- Disable command-line and scripting from systems
- Secure domain controllers
- Segment your network logically and physically



The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks

Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Keep up to date

Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

Utilize antimalware

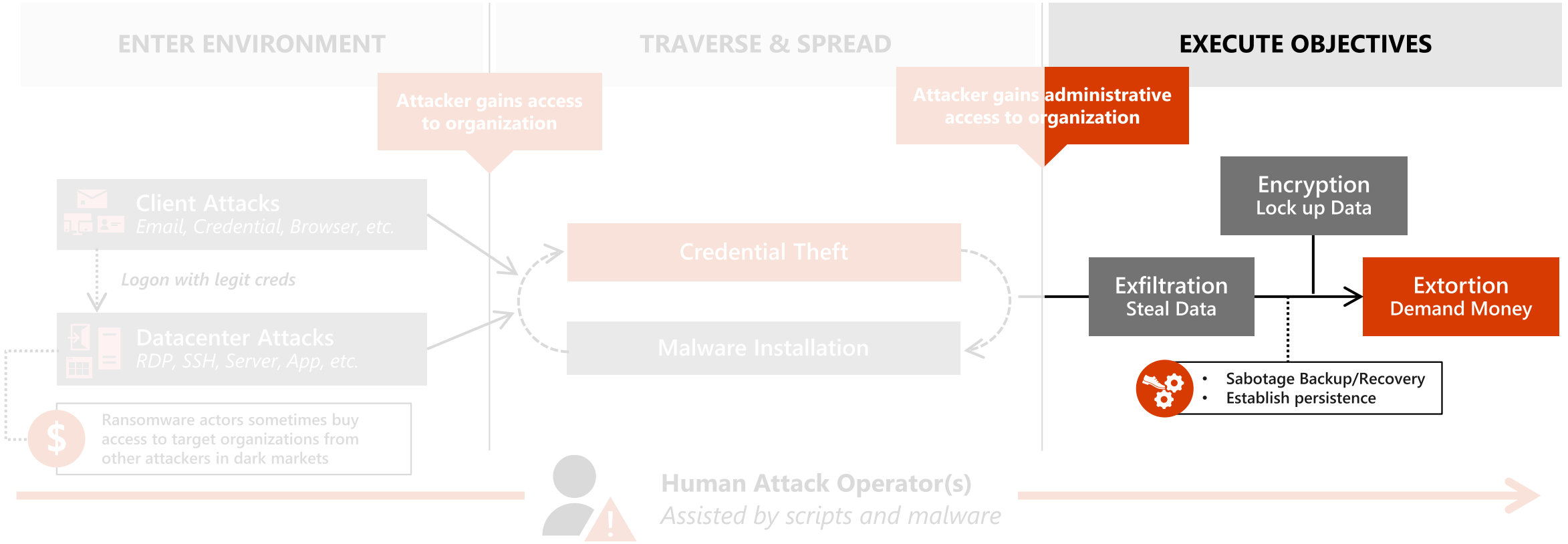
Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.

FY21 Microsoft Digital Defense Report

Pattern – Human Operated Ransomware



[Human-operated ransomware | Microsoft Docs]

Recovery

- Secure Backups
  - MFA for any backup modification/deletion
  - Offline but accessible
  - Immutable storage if possible

- Ensure you have a strong backup recovery plan
  - Ensure the backup recovery key is not on the network
  - How long will it take you to access and recover if needed?

Note from a non-affiliated Ransomware Attacker

How we penetrated your network

First carried out a phishing attack
The input machine was [redacted]\[redacted]
then we get information from it:

Vnc: [IP and port redacted], [redacted]
OS: Windo
Browser: M
Socks: [IP

having thes
go up to the
domain adr
having dom
enterprise a
[domain rec
[domain rec
[domain rec

then we sw
and got the
[domain rec
[domain rec
[domain rec

coincided

Our wishes:
Allocate all important servers to workgroups
buy normal antivirus, Carbon Black
not only on [domains redacted], etc. but also on [domain redacted]
All external connections only through 2-factor authentification
Close SMBv2
Organize data exchange through closed FTP
Reduce the number of domain admins
change passwords every 2 weeks
they will not light up in mimikatz and password hashes will not be bruted

Take the Advice of Ransomware Actors: Prevent Escalation and Lateral Movement (coveware.com)

SOME GOOD NEWS

Aug 2021 - Ragnarok, Ziggy, Avaddon, SynAck, Fonix
All released their decryption tools and neutralized their attacks

[Russia excluded from 30-country meeting to fight ransomware and cyber crime | Reuters]

October 13, 2021
4:24 PM MDT
Last Updated 3 days ago

World

Russia excluded from 30-country meeting to fight ransomware and cyber crime

3 minute read

By Nandita Bose

THE DAILY BEAST

+ Follow

Diabolical Ransomware Gang Calls it Quits

Shannon Vavra · 8/28/2021

Like · 7 Comments · 23

Just as in the Marvel Universe, a ransomware group that goes by the name "Ragnarok" caused catastrophic harm and ended in a snap.

© Provided by The Daily Beast Photo Illustration by The Daily Beast / Photos Getty

Summary

- Ransomware is and will continue to be a major threat to the world
- The attacks are becoming more sophisticated, but so are the defenses
- Proactive defense is significantly more cost-effective than extortion

Additional References

- FY21 Microsoft Digital Defense Report
- 2020 Trustwave Global Security Report
- Use passwordless authentication to improve security - Microsoft Security
- 2021-06-09-HRG-Testimony Carmakal.pdf (house.gov)
- Uncensored Interview with REvil / Sodinokibi Ransomware Operators — Cyble
- Latest Ransomware News and Trends (coveware.com)
- Parents were at the end of their chain — then ransomware hit (nbcnews.com)

TO PAY OR NOT TO PAY?

Considerations on whether to pay?

- How quickly can you recover your systems and data on your own?
- How reliable is the threat actor?
- Did the threat actor steal data before they deployed their encryptors? How sensitive is the data that they stole?
- Does the threat actor still have active access to your network?
- Will cybersecurity insurance cover the claim?
- Is the threat actor sanctioned by the US Department of Treasury?

Charles Carmakal, SVP & CTO, Fireye/Mandiant
Congressional Testimony July 20, 2021
2021-06-09-HRG-Testimony Carmakal.pdf (house.gov)

What happens if you pay?

- Many times, but not always:
  - Threat actors usually deploy multiple backdoors within victim environment
  - Many threat actors provide working decryption tools when they are paid
  - Many threat actors do not publish stolen data when they are paid
  - Many threat actors don't recompromise entities that paid them

- BUT… you MUST assume they have continued access to your environment and that they retained the data they stole…

Charles Carmakal, SVP & CTO, Fireye/Mandiant
Congressional Testimony July 20, 2021
2021-06-09-HRG-Testimony Carmakal.pdf (house.gov)

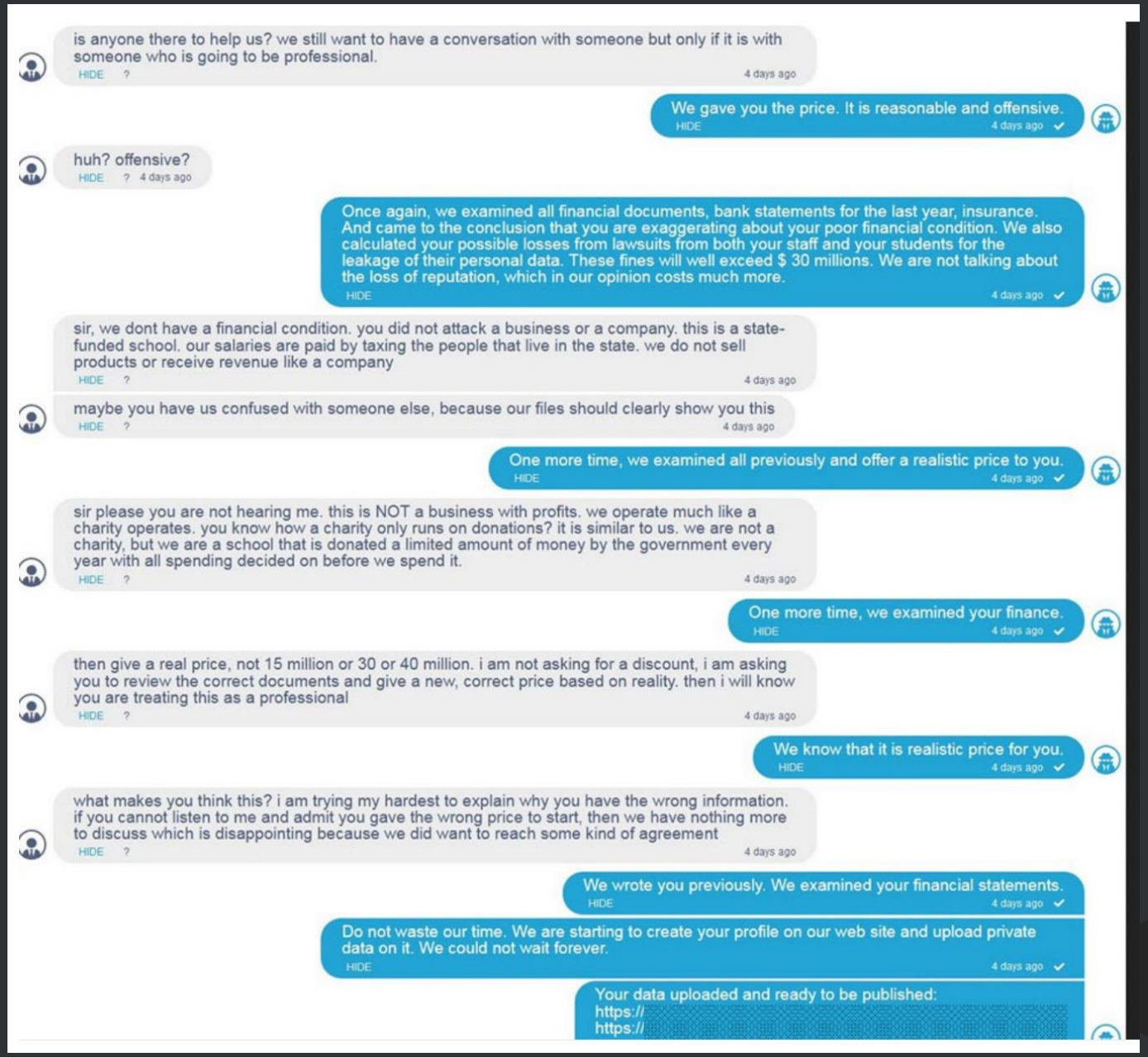
Overview

- Cybersecurity Landscape - 2021
- Ransomware in-depth
  - Purpose
  - Actors
  - How an attack occurs
- How to protect your business

Cyber-Readiness and Ransomware - Risk Management, Preparation, and Critical Actions for Disruption in the lodging industry: Learn about the cyber and ransomware threats relevant to your hotel or resort and how to be ready if your hotel is breached. Learn the latest insights about the importance of assessing risk from ransomware and cyber-attacks, how to be ready if your business is disrupted, and how cyber security readiness touches everyone.

- Trends in the cyber security environment and how this impacts the commercial marketplace particularly focusing on Ransomware
- What is the broader definition of Cyber and Ransomware?
- Learn about the importance of assessing risk at your hotel from ransomware and cyber-attacks, how to be ready if your business is disrupted, and how cyber – ransomware security readiness touches everyone and the steps to create your own hotel Cyber-Ransomware Readiness plan.
- Learn about best practices for securing your hotel and your customers and get resources

Chat between Ransomware Attackers and a School District



[Parents were at the end of their chain — then ransomware hit (nbcnews.com)]