

Ransomware: Protect Your Data or Pay the Price

July 27, 2021

Sponsored By:





- LegalFuel connects Florida Bar members with strategic tools designed to help you fuel your law practice with increased efficiencies & profitability.
- We're your go-to resource for learning how to start a new law firm or manage an existing one. Looking for specific topics on marketing, trust accounting or technology? We've got you covered.
- Plus, we know that earning Continuing Legal Education (CLE) credits is a priority for you. So, we've curated a library of free webinars, podcasts and more for you to access whenever it's most convenient.



Today's Speakers



Joelle Dvir, McDonald Hopkins, National Data Privacy and Cybersecurity Group

Joelle advises organizations on data privacy and cybersecurity risks, including proactive compliance with state and federal data breach notification laws and incident response strategies and management. Joelle has counseled clients through hundreds of data breaches and privacy incidents, working closely with forensic investigators, third party vendors, and local, state, and federal law enforcement, while minimizing exposure to her clients.



Esteban Farao, Director, ERMPProtect Cybersecurity

During 25 years in cybersecurity, Esteban has investigated hundreds of data breach incidents, identifying the cause of attacks and assisting clients to contain them. An expert in IT Security, he advises clients on how to fortify defenses and secure IT infrastructure. He has two master's degrees and 11 IT Security certifications, including certification by the Payment Card Industry Security Council to assess compliance with payment card security requirements (PCI QSA) and to investigate credit card breaches (PCI PFI).





Agenda



- Latest Trends in Ransomware Attacks
- Legal & Practical Considerations of Paying Ransom
- What to Do if You Get Hit
- Steps Law Firms Can Take to Protect Themselves





Disclaimer



- The information in this presentation is not legal advice and should not be considered as such.
- This presentation represents only the personal views of the presenters.
- This presentation is offered for informational and educational uses only.



The 2020 Story

\$3.86 million

Average total cost

+\$137,000

Remote work impact on
avg. total cost

Ransomware and destructive malware breaches cost more than the average malicious attack.

Malicious attacks that destroyed data in destructive/wiper-style attacks (average cost of \$4.52 million) and ransomware attacks (\$4.44 million) were more expensive than the average malicious breach (\$4.27 million) or the average data breach (\$3.86 million)

\$150

Customer PII avg. cost
per record

280 days

Average time to identify
and contain



Source: IBM Cost of a Data Breach Report 2020

Biggest Attacks

 **software** AG



Cognizant



GARMIN®



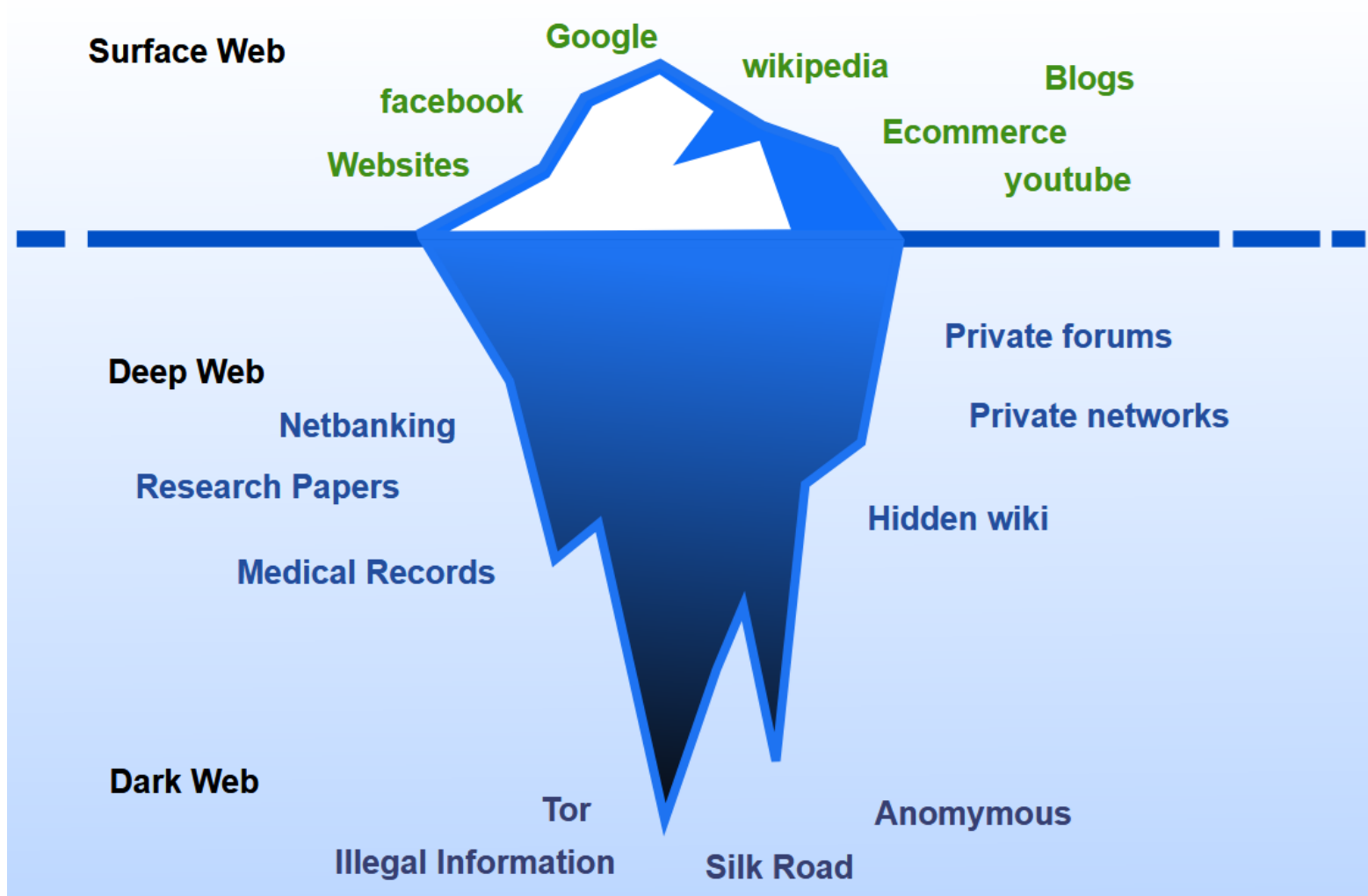

Kaseya®



Why?

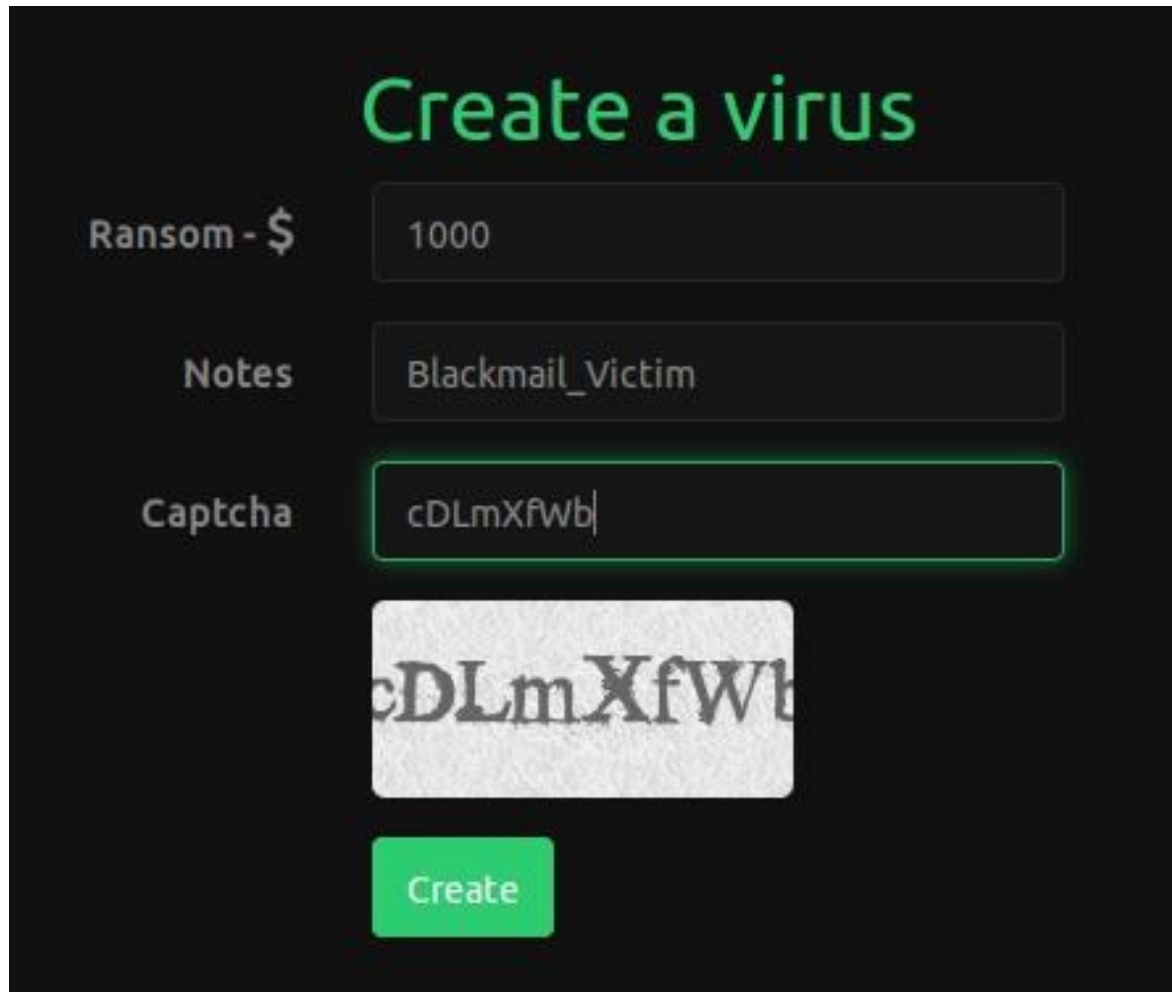


The Dark Web



Source: Wikimedia Commons

30% Profit Sharing Model



The image shows a dark-themed web interface titled "Create a virus" in green text. It contains three input fields: "Ransom - \$" with the value "1000", "Notes" with the value "Blackmail_Victim", and "Captcha" with the value "cDLmXfWb|". Below the captcha field is a small image of a captcha with the text "cDLmXfWb". At the bottom of the form is a green "Create" button.

Create a virus

Ransom - \$

Notes

Captcha



RaaS – Ransomware as a Service

The image shows a dashboard for a Ransomware as a Service (RaaS) platform. The dashboard is titled "Dashboard Statistics Overview" and features a sidebar with navigation options: "Dashboard", "Clients", and "Settings". The main content area displays four key statistics:

- Clients:** 1 (represented by a server icon)
- Payments:** 0 (represented by a shopping cart icon)
- Earned:** 0 (represented by a Bitcoin icon)
- Bitcoin Price:** 1284\$ (represented by a Bitcoin icon)

Below the statistics, there are two main sections:

- Updates:** A list of recent updates with dates:
 - New Design + Bug fix (22 feb)
 - Critical bug fixed (20 feb)
 - New programm design (20 feb)
 - Fix programm bug (18 feb)
 - Release new version (15 feb)
 - Test new version (14 feb)
- Infos:** A section containing information about the current version (2.4) and instructions for users, such as "Price to unlock", "Don't forget", "Contact jabbe", and "Contact Tele".

A prominent notification window is overlaid on the dashboard, titled "Files encrypted". The message reads:

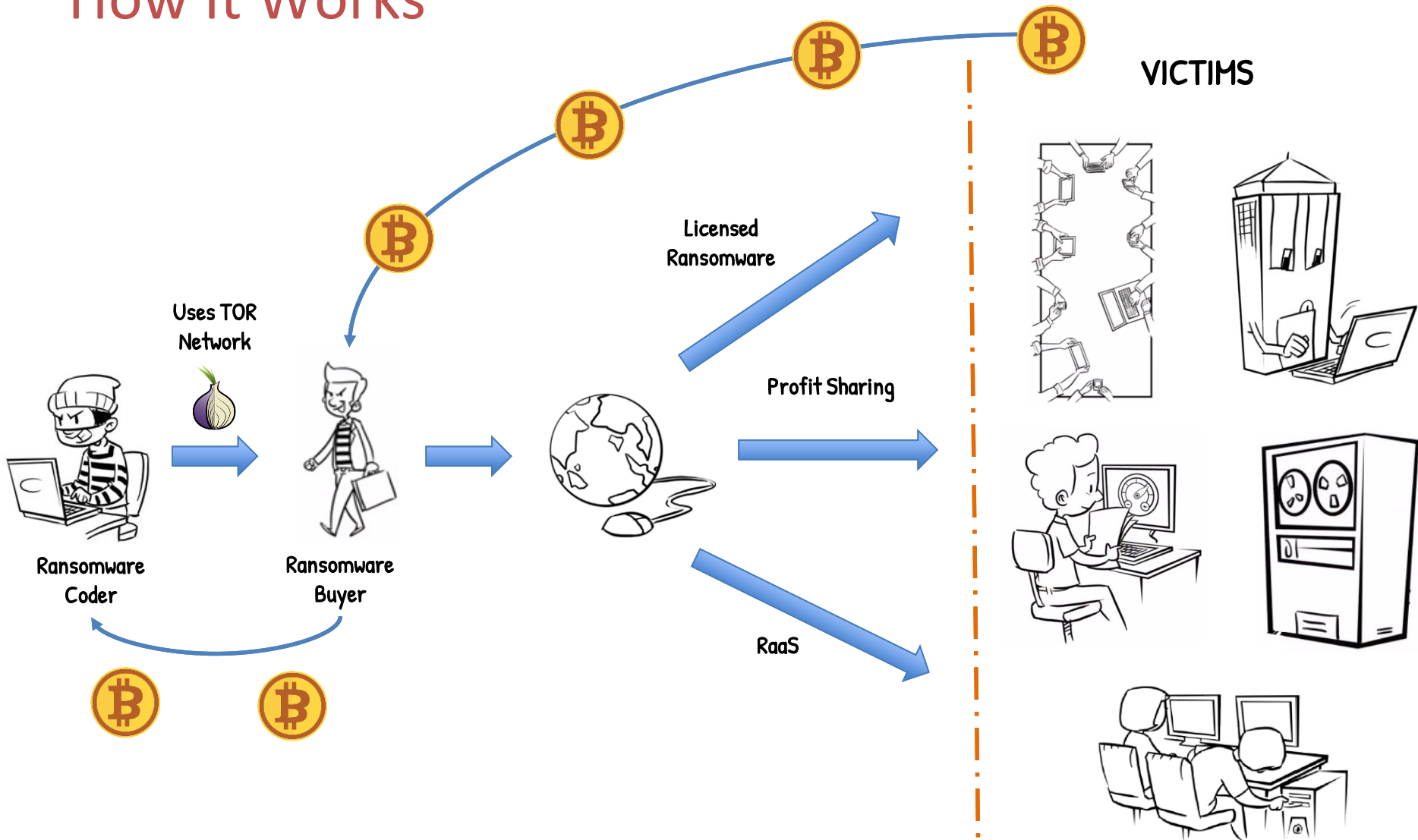
Files encrypted

All files are encrypted! Please follow the mind. In order to get the key to decrypt send this amount to our wallet Bitcoin. Decrypt files automatically.

Interference with the program - can leave you without files.

The notification window includes language selection buttons for "DEU" and "ENG" and a Bitcoin address field showing "0.00000000 to".

How It Works

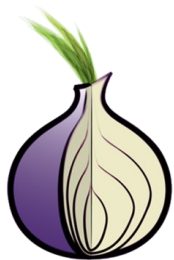


The TOR Network



2.4 Million directly connecting TOR users at a given time

6,500 relays and **1,800** bridges



175,000 .onion addresses

500,000 update requests over the past 3 months



Source: metrics.torproject.org



Ransomware: Protect Your Data or Pay the Price



Current Trends: Victims

- Significant increase in attacks in certain industries:
 - Healthcare
 - Managed Service Providers (MSPs)
 - Manufacturing
 - Municipalities
 - Professional Service Providers
 - Education (School districts, universities)
 - Financial Institutions
- Increase in attacks on small and mid-size businesses



Current Trends: Attack Vector, Variants

- Attack vector typically email phishing or RDP compromise
- New variants exfiltrate data prior to encryption and threaten to expose the data if ransom is not paid
 - Ex. Maze, Sodinokibi, Doppelpaymer
- Due to increase in exfiltration events, increase in “breaches” requiring notification
- Hasty threat actors are wiping data



Legality of Paying Ransomware

- No state or federal law prohibiting payment
- Breaking down the OFAC guidance (10/1/20)
 - Sanctions risk if paying forbidden entities/individuals on sanctions list
 - E.g., Evil Corp. (Dridex), Lazarus Group (WannaCry 2.0)
 - Possible strict liability
 - Entities making payment must be registered Money Services Businesses and need to file appropriate SARs
 - Disclose to and work with law enforcement to minimize risk



Considerations in Paying Ransom

- Cyber insurance
- Viability of backups
 - How long will it take to restore?
- Ability to rebuild
- Business interruption costs
 - Average of 21 days of downtime (source – Coveware)
 - Amount of ransom vs. lost revenue – may be financially advantageous to pay ransom
 - May be able to negotiate ransom down



Considerations in Paying Ransom

- Proof of stolen data
 - Sensitivity of same
 - Legal obligations
- Reputation/history of threat actor group
 - Statistics relating to TA group
 - Recovery
 - Reextortion
 - TA may still post data
- Threat to human life
 - Delayed treatment due to hospital computers being down caused death



Role of Cyber Insurance

- Helps protect organizations from cyberattack fallout from ransomware, business email compromise, etc.
- Potentially covers financial cost of some elements of dealing with the attack and recovering from it
- Know your coverage, exclusions, and limits
 - Business interruption, ransom payments
- Rates increasing 20-50% this year (source – Aon)



Ethics of Security Incidents

FL RPC 4-1.6 Comments – Confidentiality of Information

- Lawyer must competently safeguard client information
- Unauthorized access to information does not constitute a violation if lawyer has made reasonable efforts to prevent the access or disclosure
- Whether a lawyer may be required to take additional steps is beyond the scope of these rules



Ethics of Security Incidents

ABA Formal Opinion 483 – Lawyers’ Obligations After an Electronic Breach or Cyberattack

- Model Rule 1.4 – Keep clients “reasonably informed”
- Model Rules 1.1, 1.6, 5.1 and 5.3 – Duty to notify and take reasonable steps when data breach occurs involving or having a substantial likelihood of involving material client information





Ransomware: Protect Your Data or Pay the Price



Ransomware Attack Response

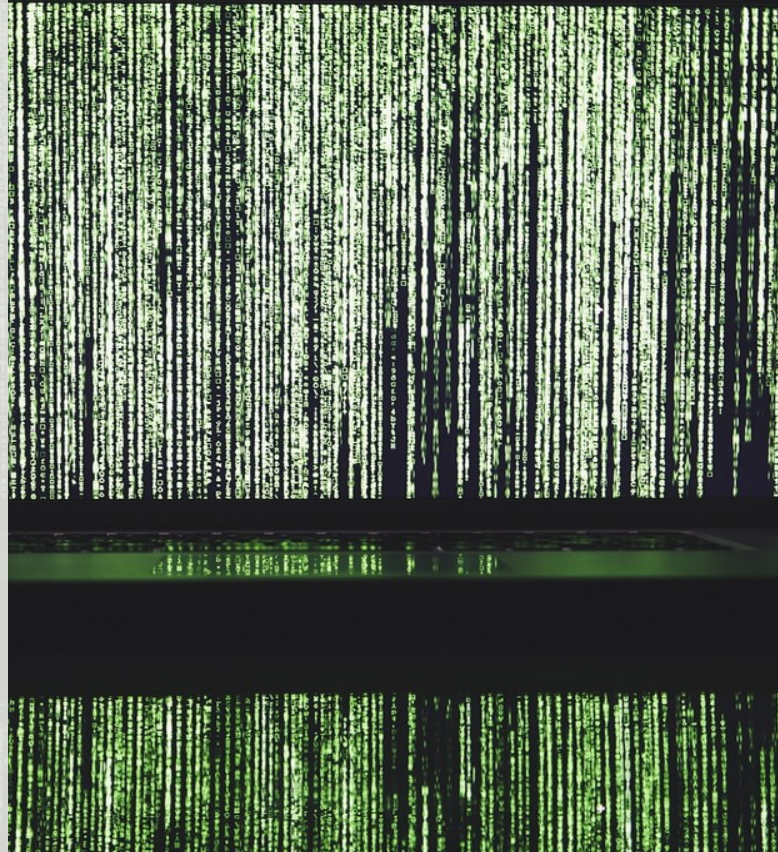
10 10 10 01 01 01 00 10 01 00 11 00
00 11 00 00 00 00 01 01 11 10 10 00
11 10 10 11 10 11 11 00 10 10 10 00
10 00 01 00 10 11 01 00 00 10 10 10
10 10 11 11 01 10 11 00 10 10 10 10
00 01 00 10 00 01 10 01 00 00 11 00
10 10 00 11 11 01 01 01 11 11 10
11 10 11 00 11 10 01 01 10 01 01 00
00 01 11 00 10 00 11 01 00 11 10 01 10
10 10 11 11 01 00 01 01 00 01 11 01
01 11 11 01 00 10 00 11 10 10 00 11
11 10 11 10 10 01 11 01 10 11 01 01
11 11 10 01 01 01 11 10 01 01 00 11
11 01 11 00 00 01 10 01 00 01 11
00 00 00 11 11 11 01 01 00 11
10 10 11 10 01 00 01 01 01 01 01
11 10 00 00 00 01 00 11 10 01 11 01
00 01 10 01 01 11 10 01 00 00 01
01 00 01 10 11 10 11 10 00 00 10
00 10 11 11 01 00 00 01
01 11 11 00 10 11 10 10 11 01 11 11
11 11 01 10 11 00 00 01 01 10 11 00
10 00 00 10 01 00 11 00 10 01 10 11
01 00 10 11 01 10 10 11 10 01 01 01
11 01 01 11 11 01 10 01 01 10 01 11
11 00 00 11 00 11 11 11 10 00 01
01 10 10 01 00 10 10 01 10 11 11
00 01 10 11 10 11 11 10 00 11
00 11 00 01 10 00 10 11 11 01 00 00
11 10 11 10 10 00 11 01 11 11 01 10
10 01 00 11 11 01 11 11 10 11 11 00
01 01 00 00 00 00 11 11 10 10 01 00
11 01 01 11 00 10 01 11 10 00 00 01
11 11 00 00 11 01 00 01 10 01 01 01

- Isolate
- Kill Communications
- Block IPs
- Find Decryption Keys

1 01 10 01 10 00 10 11 11 11 01 10 01 11 01 00 11 01 01 10 11 01 11 00 01 01 01 01 01 01
1 01 11 00 00 01 00 11 11 00 11 11 01 10 00 10 00 11 00 01 11 01 10 10 10 01 00 11
0 10 00 10 00 01 10 00 00 11 00 11 00 10 10 11 10 10 01 00 00 01 00 00 11 01 10 01 01 10
1 10 01 10 01 10 11 00 01 11 00 10 01 11 11 11 11 10 11 01 01 10 00 11 00 11 10 10 00
0 10 10 00 11 00 10 00 01 11 10 01 10 01 00 10 11 01 00 01 01 01 01 01 11 00 11 01 00 11
1 10 00 10 10 00 11 00 11 00 10 11 01 11 01 10 11 00 00 11 10 00 00 01 10 01 10 11 00
0 01 00 11 10 11 01 11 10 10 00 10 10 00 00 11 10 00 00 01 00 11 10 10 01 01 10 11 11
0 11 11 00 11 01 00 10 10 00 00 00 11 11 10 10 11 01 00 01 11 10 11 10 11 01 01 11 10 00
0 00 11 00 10 00 11 01 10 00 10 01 11 11 01 01 01 11 11 10 11 11 01 11 11 01 11 11 11
0 01 11 10 11 10 10 00 10 10 00 10 01 11 01 11 01 11 10 00 11 01 10 01 00 10 01 11 00 10
1 10 10 01 01 01 10 01 00 10 01 00 11 11 10 11 00 00 11 10 00 11 10 01 00 01 00 00 10 11 10
0 00 10 11 10 10 01 01 11 11 11 11 11 01 00 11 01 11 00 11 01 10 00 00 01 10 11 00 00 11 01
1 01 01 10 00 00 01 00 01 01 00 01 10 01 11 01 11 01 11 00 11 01 10 00 10 10 11 01 01 01
1 01 11 00 10 11 00 11 01 10 00 10 01 10 00 01 10 11 10 01 00 00 11 00 11 01 00 01 01
0 11 10 11 10 00 00 11 00 10 11 01 11 11 01 11 01 00 10 01 11 10 00 01 10 00 00 01 11 00
1 10 11 11 10 00 10 00 10 00 01 11 10 11 00 01 00 11 00 11 01 00 11 10 10 10 10 00 10 11
0 10 10 01 00 00 11 11 10 11 11 10 11 01 01 10 11 10 11 01 00 10 11 01 00 10 11 00 00 10
1 01 01 10 11 01 10 00 10 10 11 11 10 01 01 00 11 10 00 10 10 01 01 11 10 01 10 00 01 01 00
1 01 01 01 11 00 01 10 01 10 01 11 00 11 10 10 00 10 01 10 00 10 01 10 10 00 01 10 11 01 11
0 10 11 10 10 00 00 01 10 01 01 01 00 10 10 10 00 01 10 10 00 01 10 10 00 10 10 11 11 01 11
1 11 11 00 10 11 01 HACKED 10 01 00 01 10 00 10 10 10 11 11 00 00 11 01 11 11 01 01 00
0 01 00 11 10 00 11 01 00 10 01 01 10 10 01 10 00 10 10 10 10 10 00 11 11 10 10 00 10 11
1 11 01 10 00 01 00 11 00 01 11 00 10 01 11 00 00 11 10 00 11 00 00 10 00 00 11 01 10 11
0 00 11 10 10 00 01 00 01 01 10 10 00 11 11 00 11 11 10 01 10 11 00 00 01 01 10 10 00
1 10 00 01 00 01 01 11 00 10 00 11 10 01 10 01 11 10 11 00 10 11 00 01 01 00 01 10 00 01
1 10 01 01 10 10 11 11 00 01 10 01 10 11 10 10 11 00 10 01 11 01 01 00 01 01 00 00 01 01
0 00 01 10 00 10 01 11 00 10 01 10 01 01 00 10 00 11 01 01 10 00 01 01 00 01 00 10 01 11
1 10 01 10 01 00 01 10 00 01 10 00 11 01 01 01 00 11 01 00 01 10 11 11 01 11 00 10 01 10
0 10 11 10 10 01 00 11 01 10 11 00 11 00 10 10 00 00 00 11 10 11 01 11 00 10 00 10 00 00 11
0 00 00 11 11 10 10 00 00 00 01 11 11 00 01 11 10 00 01 10 01 11 10 00 01 10 00 11 00 00
1 01 00 11 00 00 10 10 00 01 10 10 00 10 10 10 10 11 11 11 01 01 11 00 01 01 10 11 00
0 11 11 10 11 10 00 01 11 01 10 00 10 10 01 01 00 11 00 01 00 00 01 00 11 11 01 00 10 00
1 10 00 01 10 11 11 11 00 01 11 00 11 11 00 11 11 00 10 10 00 11 11 10 10 01 10 01 11 10
1 00 11 00 00 01 01 11 00 11 11 11 00 00 10 10 00 00 00 10 00 11 01 10 00 01 00 11 01
0 10 11 00 01 11 00 11 10 11 01 00 00 10 01 00 10 01 10 00 01 01 01 00 11 01 11 00 00 11
0 00 01 00 10 00 00 11 00 00 01 10 10 11 01 11 11 10 10 10 00 01 00 11 10 10 01 10 01 11
0 01 11 00 10 00 00 10 10 11 11 01 11 01 01 10 11 01 01 10 11 01 01 10 00 11 00 00 11 11
0 11 01 01 11 01 01 11 11 00 10 11 10 11 01 01 00 00 01 01 01 10 00 01 11 01 11 01 11 11
1 01 10 10 00 01 01 10 11 01 00 10 01 10 01 10 01 10 11 00 00 01 01 01 11 11 11 10 01 10
0 10 11 10 00 10 11 01 11 11 01 11 00 11 10 01 00 00 11 11 10 11 11 11 00 11 00 10 00 10
0 10 01 00 01 10 11 11 10 10 11 11 11 01 01 10 11 01 01 10 10 10 01 00 10 10 01 00 11 01 11
1 01 11 11 10 00 00 01 01 00 00 01 10 10 11 01 01 11 01 01 11 01 01 11 11 11 01 01 01 11 10 11
0 00 00 11 11 11 01 00 01 01 01 00 10 11 00 10 10 11 00 00 11 10 01 10 01 10 00 01 01
1 10 01 00 10 00 11 01 01 00 11 11 00 11 01 01 01 11 00 10 01 01 01 11 00 01 11 11 11 11

Ransomware Attack Response

- **Secure Backups**
- **Preserve Locked Files**
- **Virtual Machines**



Ransomware Attack Response

- **Attempt To Restore**
- **Check For Infections**



Fortifying Your Defenses

- **Security Awareness Training**
- **VPN/Remote Access**
- **Strong Authentication**
- **Access Controls**
- **Vulnerability Scans**



Fortifying Your Defenses

- **Patches / Updates**
- **Antivirus / Anti-Malware**
- **Backups**
- **Incident Response Plan**



References

Security awareness training

- Cybrary - (<https://www.cybrary.it/>)
- KnowBe4 - (<https://www.knowbe4.com/>)
- ERMPProtect – (<https://erm.bridgeapp.com/>)

VPN/Remote Access

- Wireguard - (<https://www.wireguard.com/>)
- OpenVPN - (<https://openvpn.net/>)
- Check current firewall solution to determine if VPN functionality is present.

Multi-factor Authentication

- Duo - (<https://duo.com/>)
- Yubico - (<https://www.yubico.com/>)



References

Vulnerability Scans

- Qualys - (<https://www.qualys.com/>)
- Nessus Tenable - (<https://www.tenable.com/>)
- OpenVas - (<https://www.openvas.org/>)

Other References

- <https://us-cert.cisa.gov/ncas/alerts/aa20-073a>
- <https://www.cisa.gov/publication/ransomware-guide>
- <https://www.cisa.gov/publication/cisa-cyber-essentials>
- <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>
- <https://github.com/cisagov/cset/releases/tag/v10.3.0.0>
- <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>



Questions



For More Information



jdvir@mcdonaldhopkins.com

305.704.3986



efarao@ermprotect.com

305-447-6750

