



The Current State of Ransomware

Andy Thompson
Allan Cox





Andy Thompson

Andy.Thompson@CyberArk.com

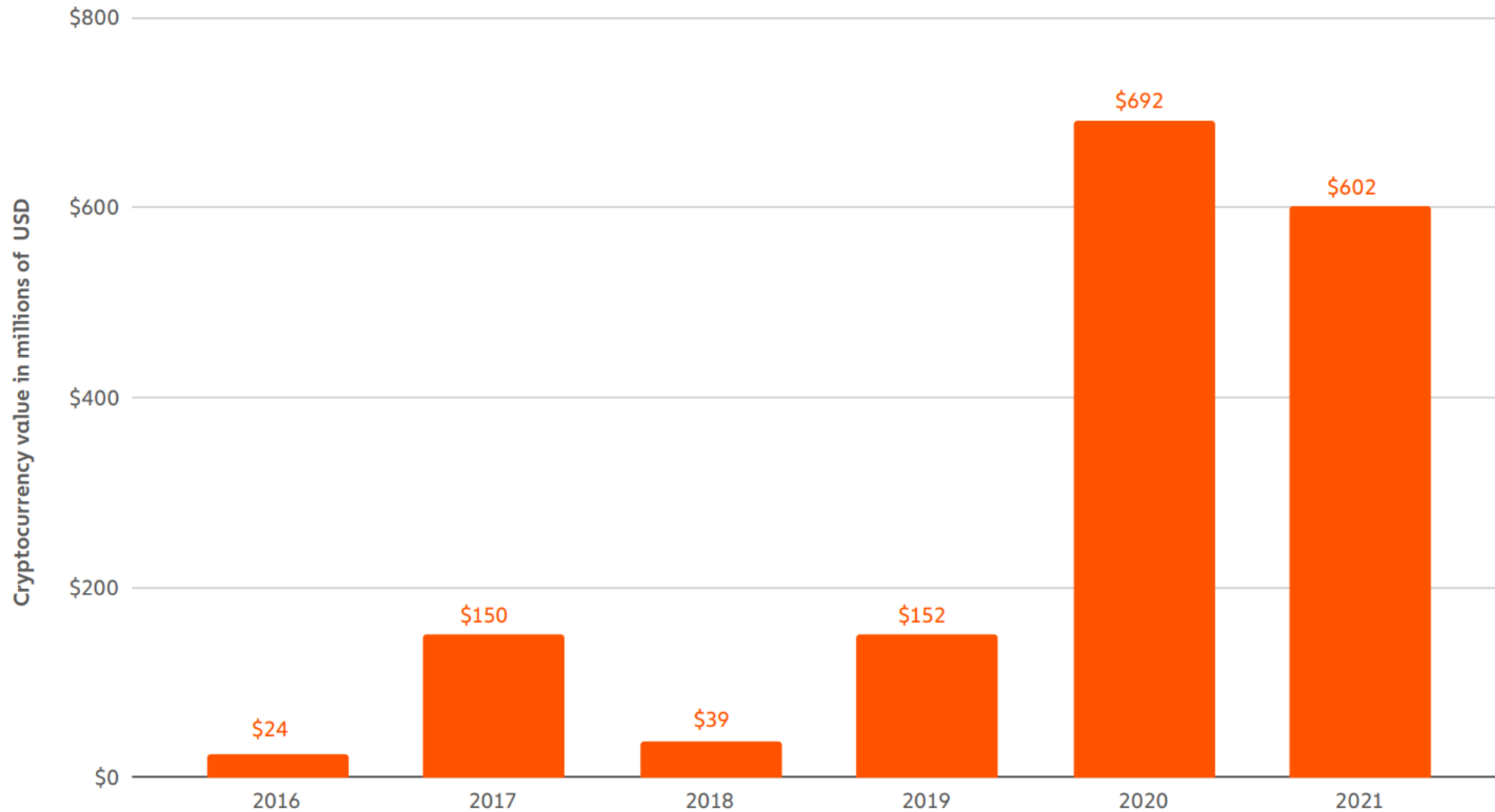
- Global Research Advisor/Evangelist
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hackers Association Organizer
- Travel-Hacker

-
- LinkedIn: [in/andythompsoninfosec](https://www.linkedin.com/in/andythompsoninfosec)
 - GitHub: github.com/binarywasp
 - Twitter: [@R41nMkr](https://twitter.com/R41nMkr)



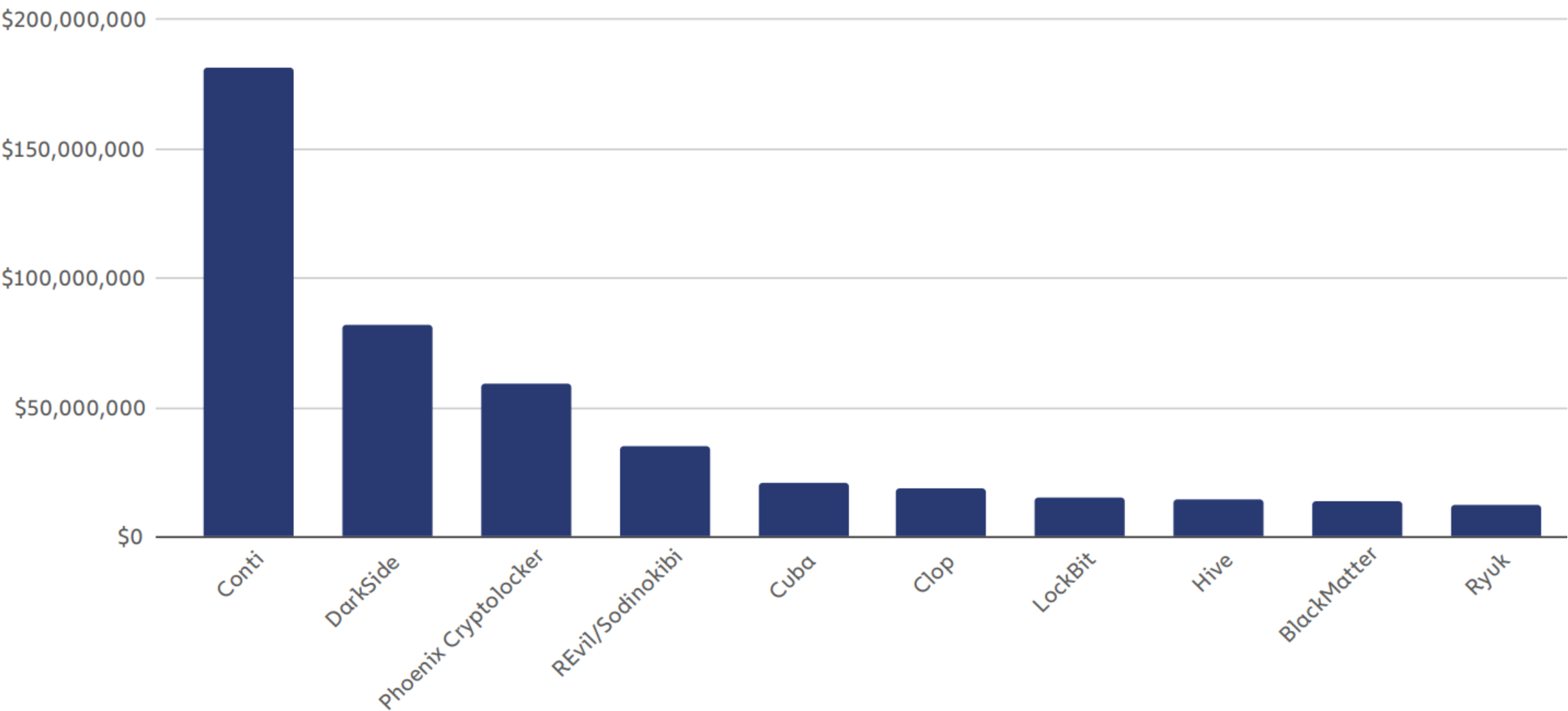
Current Statistics

Total cryptocurrency value received by ransomware addresses | 2016–2021



Current Statistics

Top 10 ransomware strains by revenue | 2021



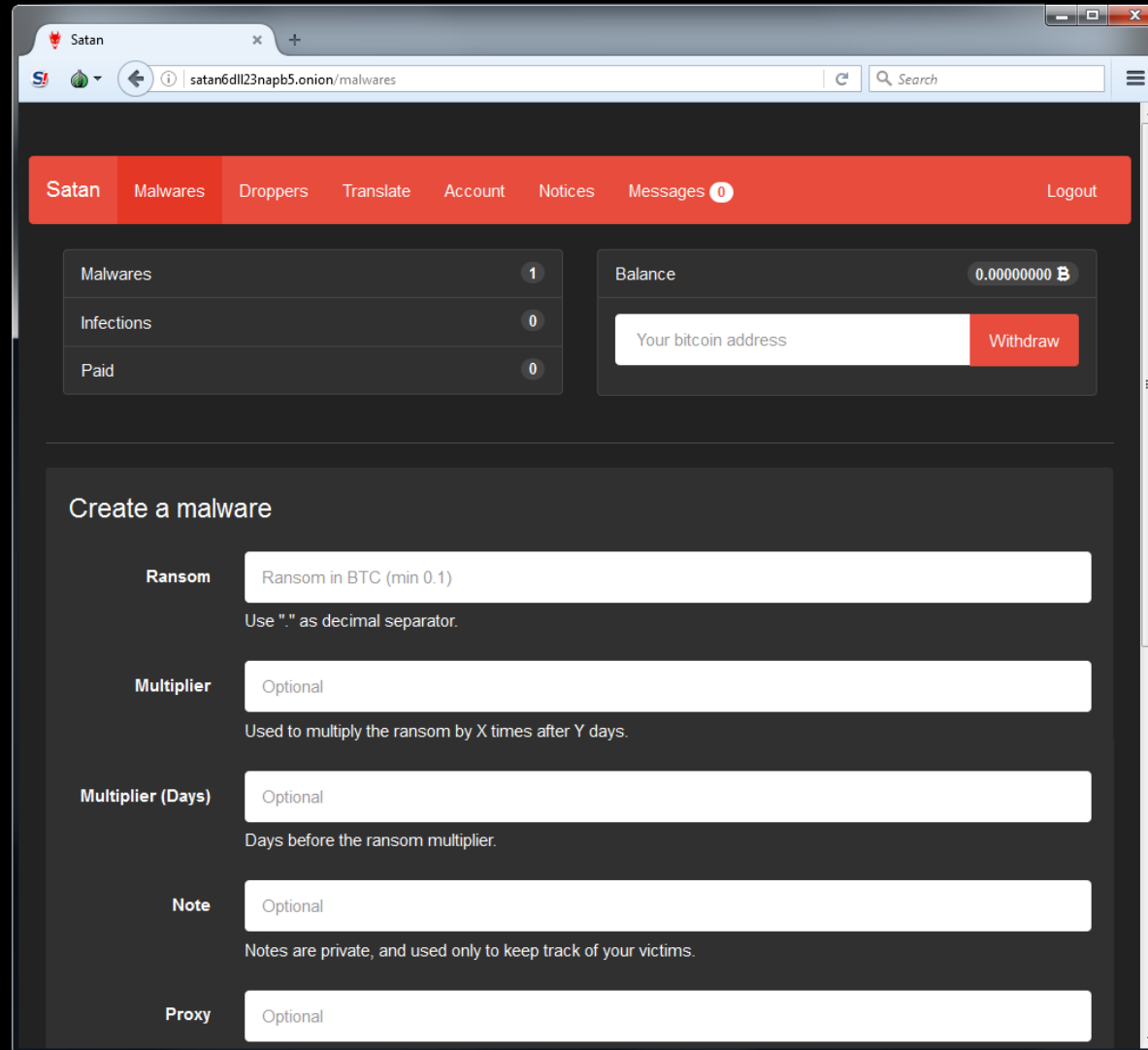
Source: Chainalysis: "The 2022 Crypto Crime Report" February 2022



- Globally, there were 304.7 million ransomware attacks in the first half of 2021, a 151% increase since 2020. (SonicWall)
- Ransomware attacks experienced annually by organizations have been on the rise since 2018, peaking at 68.5% in 2021. (Statista)
- 80% of organizations were hit by a ransomware attack in 2021. (Claroty x Forbes)
- There were 121 reported ransomware incidents reported in the first half of 2021, a 64% increase from 2020. (PurpleSec)
- The FBI's Internet Crime Complaint Center (IC3) received 2,084 ransomware complaints in the first half of 2021. (FBI and CISA)
- Experts estimated that a ransomware attack would take place every 11 seconds in 2021. (Cybersecurity Ventures)
- Ransomware attacks increased 148% from Q2 of 2020 to Q2 of 2021. (SonicWall)
- There were a record-breaking number of ransomware attacks in Q3 of 2021, totaling 190.4 million. (SonicWall)
- 127 new ransomware families were discovered in 2020, up 34% since 2019. (Statista)
- There were 304 million ransomware attacks globally in 2020. (Statista)
- The total number of ransomware attacks in 2020 increased by 62% compared to 2019. (Statista)
- December 2021 saw one of the highest volumes of ransomware attacks that year, with 33 publicly reported attacks. (Blackfog)
- Compromised remote desktop protocol connections were the most common attack vector in Q1 of 2021. (Coveware)
- VPN appliances, like Fortinet and Pulse Secure, were the most commonly exploited software vulnerabilities in Q1 of 2021. (Coveware)
- 571 different victims suffered a ransomware attack due to a data leak in Q3 of 2021. (Digital Shadows)
- At least one employee downloaded a malicious mobile application in 46% of organizations in 2021. (Check Point)
- The total cost of a ransomware breach was an average of \$4.62 million in 2021, not including a ransom. (IBM)
- Reported monetary losses to ransomware attacks increased 20% in the first half of 2021 compared to 2020. (FBI and CISA)
- Ransomware breach response costs took up 52% of the overall cost of a ransomware attack in 2020. (Corvus Insurance)
- Globally, no less than \$18 billion was paid in ransoms in 2020. (EmiSoft)
- The average ransom payment was \$220,298 in Q1 of 2021, up 43% from Q4 of 2020. (Coveware)
- The average ransom payment was \$136,576 in Q2 of 2021, 38% less than Q1 of 2021. (Coveware)
- The average ransom payment was \$139,739 in Q3 of 2021, up 2.3% from Q2 of 2021. (Coveware)
- In 2021, lost business represented the largest share of data breach costs, averaging \$1.59 million. (IBM)
- 68% of U.S. organizations paid the ransom for a ransomware attack in 2020. (Statista)
- Total ransom demands across all ransomware families averaged \$847,344 in 2020. (Bloomberg)
- 32% of ransomware victims paid the ransom in 2021. (Cloudwards)
- Of the 32% of ransomware victims who paid the ransom in 2021, only 65% of their data was ultimately recovered. (Cloudwards)
- Ransomware will cost victims over \$265 billion annually by 2031. (Cybersecurity Ventures)
- LockBit 2.0 was the most active ransomware group in Q3 of 2021. (Digital Shadows)
- 125 ransomware families were discovered between 2018 and 2020, and 32 new families were uncovered in 2021. (Ivanti)
- <https://www.pandasecurity.com/en/mediacenter/security/ransomware-statistics/>



Ransomware as a Service (RaaS)



The screenshot shows a web browser window with the address bar displaying 'satan6dll23napb5.onion/malwares'. The page has a dark theme with a red navigation bar at the top. The navigation bar contains links for 'Satan', 'Malwares', 'Droppers', 'Translate', 'Account', 'Notices', 'Messages' (with a notification badge), and 'Logout'. Below the navigation bar, there are two main sections. On the left, a table shows statistics: 'Malwares' (1), 'Infections' (0), and 'Paid' (0). On the right, there is a 'Balance' section showing '0.00000000 B' and a 'Withdraw' button next to a text input field for 'Your bitcoin address'. Below these sections is a 'Create a malware' form. The form has five fields: 'Ransom' (with a hint 'Ransom in BTC (min 0.1)' and a note 'Use "." as decimal separator.'), 'Multiplier' (with a hint 'Optional' and a note 'Used to multiply the ransom by X times after Y days.'), 'Multiplier (Days)' (with a hint 'Optional' and a note 'Days before the ransom multiplier.'), 'Note' (with a hint 'Optional' and a note 'Notes are private, and used only to keep track of your victims.'), and 'Proxy' (with a hint 'Optional').

Satan

Malwares Droppers Translate Account Notices Messages 0 Logout

Malwares	1
Infections	0
Paid	0

Balance 0.00000000 B

Your bitcoin address Withdraw

Create a malware

Ransom Ransom in BTC (min 0.1)
Use "." as decimal separator.

Multiplier Optional
Used to multiply the ransom by X times after Y days.

Multiplier (Days) Optional
Days before the ransom multiplier.




Note Optional
Notes are private, and used only to keep track of your victims.

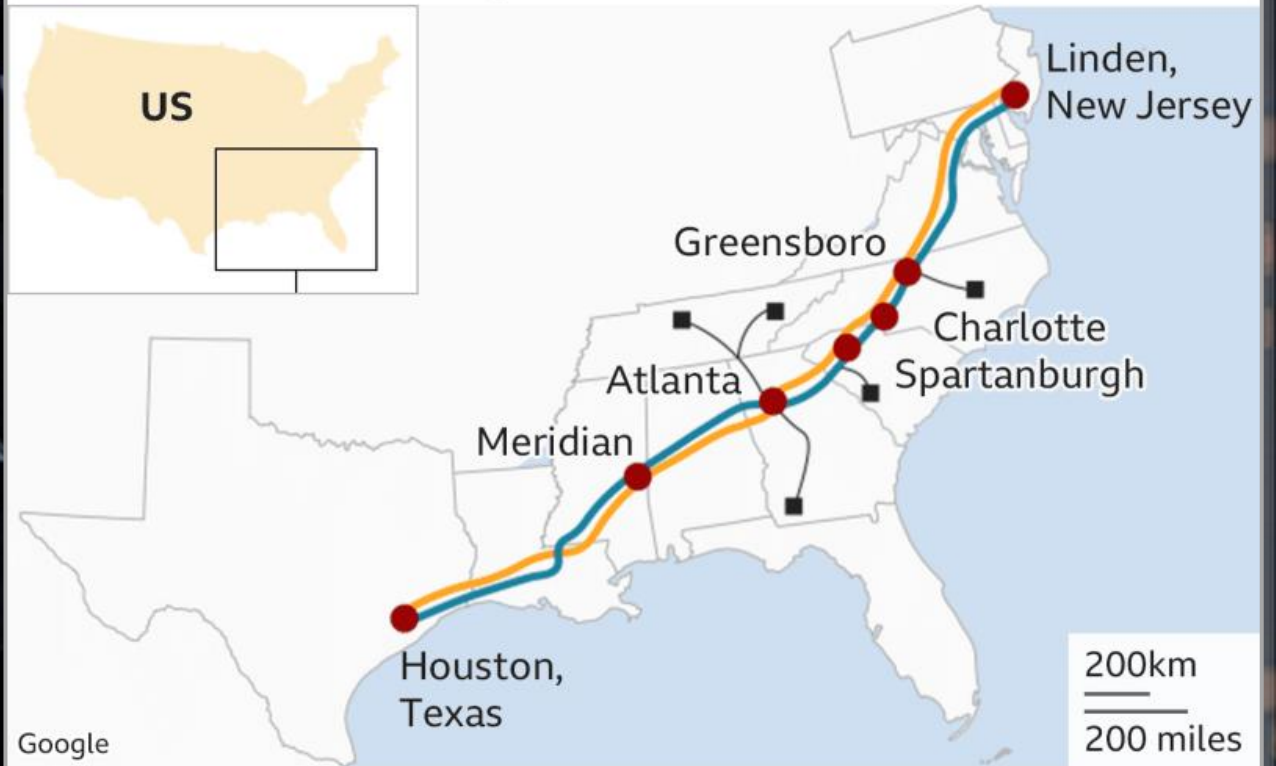
Proxy Optional



Darkside

Colonial Pipeline system map

-  Pipeline system
-  Sublines
-  Main weekend delivery locations



Google

Source: Colonial Pipeline Company

BBC





LOCK**BIT** 2.0



Ryuk



CONTI

A stylized world map is centered on a black background. The map is composed of a dense network of thin, light-colored lines connecting various points. These points are represented by small circles in red, orange, and yellow. The map itself is filled with a textured, brush-stroke-like pattern in shades of red, orange, and yellow. The word "REVIIL" is written in large, bold, white capital letters across the center of the map.

REVIIL

RaaS Business Model



**SUBSCRIPTION
BASED**



**AFFILIATE
BASED**



**LIFETIME
LICENSING**



PARTNERSHIPS




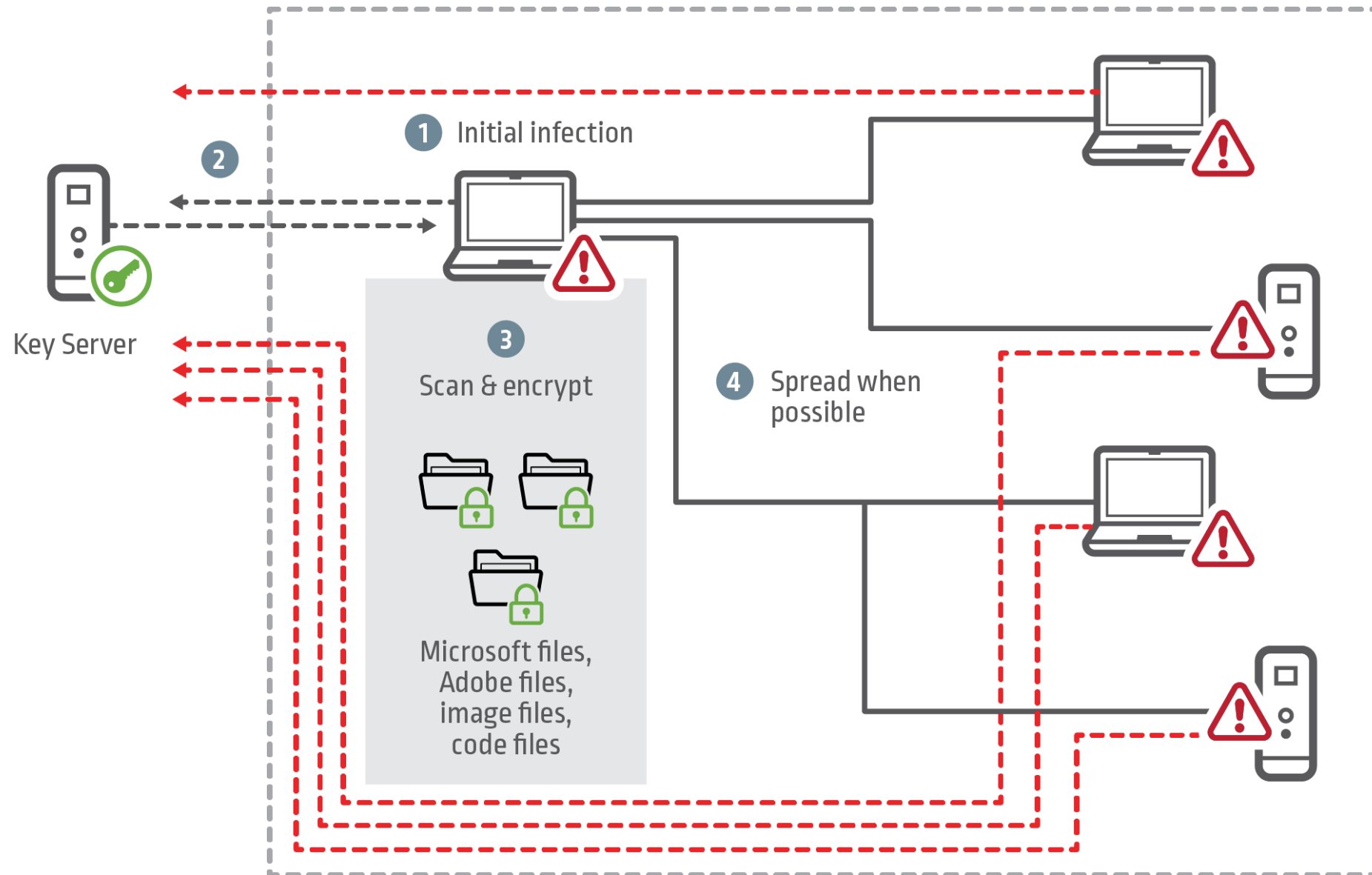
Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

⌚ The price will be doubled in:

6 days 13 hours 43 minutes 10 seconds

 Start the decryption process



Evolution of Extortion Payments



CHECKS



GIFT CARDS



MONEY ORDERS



BITCOIN



MONERO



Attacker Evolution



Targets

- Education
- Retail
- Business, Professional, & Legal Services
- Central Government
- IT
- Manufacturing
- Healthcare
- Local Government
- Financial Services



Tactics



Tools



Attacker Evolution



Targets



Tactics

- Phishing
(old, but still relevant)
 - Spray and pray
 - Spearphishing
- Malicious insiders
- RDP brute force
- Vulnerable internet facing systems

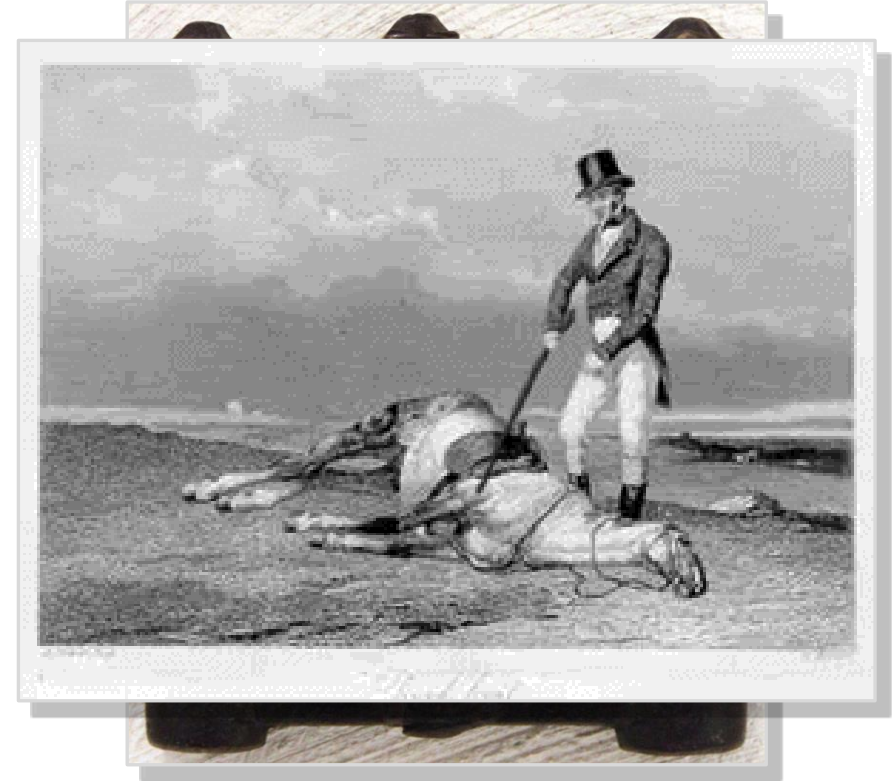


Tools



Additional Tactics

- Backup destruction
- Extortion multiple times over
 - Single Extortion - Encrypt data
 - Double Extortion - Leak and publish data
 - Triple Extortion – DDoS & Downstream risk



Encryption is no longer required!!!



Attacker Evolution



Targets



Tactics



Tools

- Avaddon
- Lockbit 2.0
- Blackcat
- STOP





AVaddon
RANSOMWARE

The logo features the word "AVaddon" in a stylized, italicized font. The "A" is a large, red, 3D block letter. The "V" and "addon" are in white with black outlines. Below this, the word "RANSOMWARE" is written in a smaller, bold, black, sans-serif font with a white outline. The entire logo is set against a dark background with horizontal streaks of red and blue light, and numerous small, glowing circular particles.



LOCKBIT 2.0

ALL YOUR **IMPORTANT FILES** ARE **STOLEN AND ENCRYPTED!**

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.

You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.

Open our letter at your email. Launch the provided virus on any computer in your company.

Companies pay us the foreclosure for the decryption of files and prevention of data leak.

You can communicate with us through the Tox messenger

[\[Redacted Tox ID\]](#)

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, use ToxID:

[\[Redacted Tox ID\]](#)

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser

[\[Redacted Website URL\]](#)



STP

Why Ransomware Works

- Failure to practice good hygiene
- Implementation of inadequate & ineffective processes



Mitigation Strategies



Mitigation Strategies

- Cyber Insurance

Trends

- Past 24 Months – Industry transformative
- Rise of ransomware led to increased claims
- Stricter underwriting and higher prices

Top 5 Controls

- MFA
- EDR
- Administrative account control
- Security awareness training
- Tested backups

For More information, including a detailed whitepaper available on our website:

<https://www.cyberark.com/cyber-insurance/>



Mitigation Strategies

- Cyber Insurance
- Patching

Patching

- One of the top priorities of successful security programs
- Log4
 - Actively exploited
 - Patches TBD



PATCH

Mitigation Strategies

- Cyber Insurance
- Patching
- **Backup & Recovery**

Backup & Recovery

Does not prevent ransomware attacks.

Allows recovery without payment

Part of every Disaster Recovery strategy

Data may still be lost.

Costs of storage and data loss should be considered.



Mitigation Strategies

- Cyber Insurance
- Patching
- Backup & Recovery
- **Endpoint Protection**

Block Applications

- Prevents KNOWN malware
- Ineffective against new & polymorphic malware



Mitigation Strategies

- Cyber Insurance
- Patching
- Backup & Recovery
- **Endpoint Protection**

Allow Applications

- Extremely effective against ransomware
- Difficult to execute effectively
- Easier implemented on servers
 - More difficult on user endpoints



Mitigation Strategies

- Cyber Insurance
- Patching
- Backup & Recovery
- **Endpoint Protection**

Application Control

- Allows more flexibility
- Restricts
 - Internet access (geo-callbacks & key exchanges)
 - Read, Write, & Modify file permissions
 - Restricts access to file shares and, other applications, and child processes.
- Extremely effective



Mitigation Strategies

- Cyber Insurance
- Patching
- Backup & Recovery
- **Endpoint Protection**

Least Privilege

- Part of Microsoft's "Ten Immutable Laws of Security"
- Should be implemented along with other controls



The Principle of
Least Privilege

Mitigation Strategies

- Cyber Insurance
- Patching
- Backup & Recovery
- Endpoint Protection
- PAM Controls
- **Multifactor**

Multi-Factor Authentication

- Mandatory for ingress.
- LP & MFA

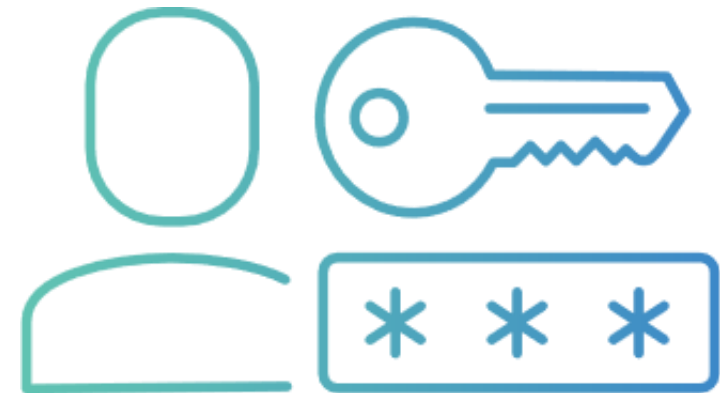


Mitigation Strategies

- Cyber Insurance
- Patching
- Backup & Recovery
- Endpoint Protection
- **PAM Controls**

Privileged Account Management

- Create isolation layers
- Remove direct access to Tier 0 systems
- Eliminate credential exposure



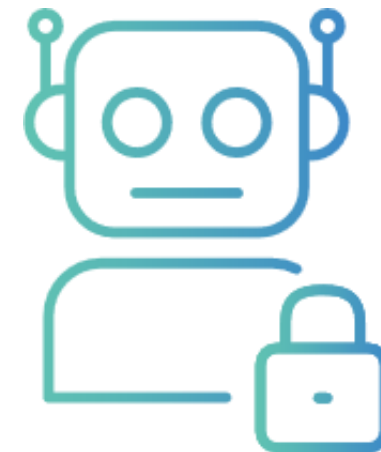
Mitigation Strategies

- Cyber Insurance
- Patching
- Backup & Recovery
- Endpoint Protection
- PAM Controls
- Multifactor
- **Non-Human Access**

Secure Non-human access

Prevent compromise of the application secrets/Service Accounts.

Used to access Tier 0 assets and CI/CD pipelines with CyberArk Secrets Manager.



Recommendations

- Locate all sensitive information and critical files
- Allow listing on servers
- Grey listing on workstations
- Remove local admin rights from endpoints
- Elevate privileges only for specific tasks
- Use AV tools to protect against known malware
- Air-gapped data protection strategy





Learn More:

[Cyberark.com/ransomware](https://cyberark.com/ransomware)

[Cyberark.com/cyber-insurance/](https://cyberark.com/cyber-insurance/)

Request Demo