



# The State of Ransomware and Enhanced Controls

Thomas L. Tyler, Jr.  
6.23.21



1

*The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.*

2



3



4

## Governmental Agencies

---

- Metro Police, Washington, D.C.
- Azusa Police, Azusa, California
- City of Tulsa, Oklahoma
- Santa Clara Valley Transportation Authority
- Illinois Attorney General's Office
- 78% of states have had at least one municipality attacked

5

## Health Care

---



6

## Education



7



Colonial Pipeline Company

May 2021

- Operator of one of nation's largest pipelines
- Shut down for six days as a precaution
- 2.5 million barrels daily – 45% of East Coast fuel supply
- Ransomware on corporate systems
  - Billing platform

*"Our goal is to make money and not creating problems for society." – DarkSide*

8



May 2021

- One of world's largest food companies
- Affected all U.S. meatpacking facilities
- Likely carried out by Russian-based criminal organization
- Systems were brought back online within a few days
  - "Remarkably fast"

9

## Executive Order

- Notify government of breaches against U.S. networks
- Standardized playbook
- Upgrade to secure cloud services and infrastructure
- Improves security of software
- Cybersecurity Safety Review Board
- Improves information sharing within government entities

10



11



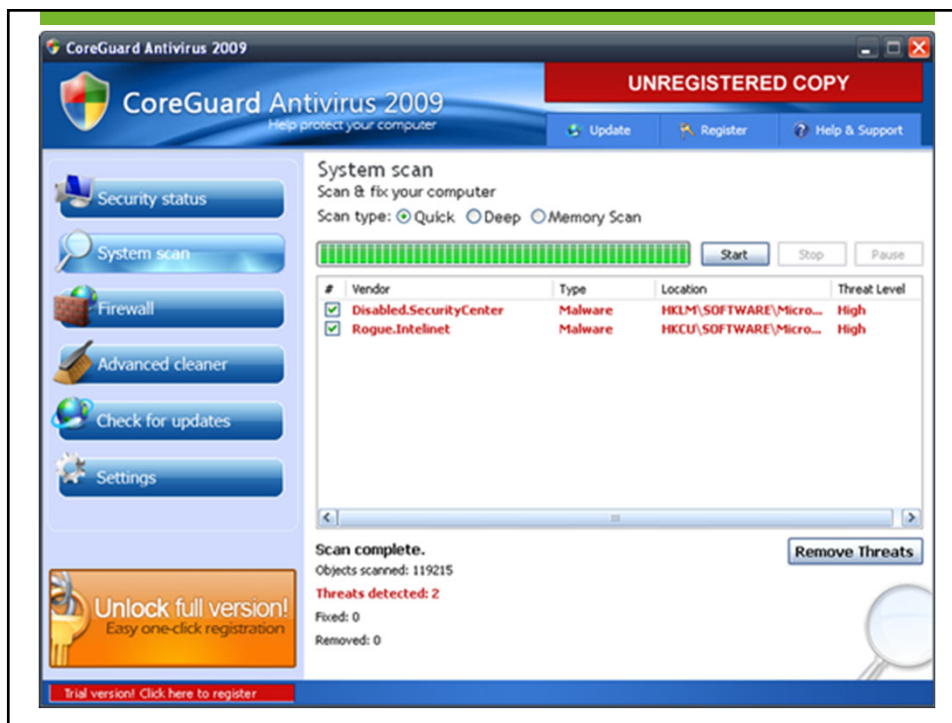
12



## Ransomware Proof of Concept

- IEEE Security & Privacy Conference – May 1996
- Program using public key algorithms could extort users
- Laid foundation for basis of ransomware we see today

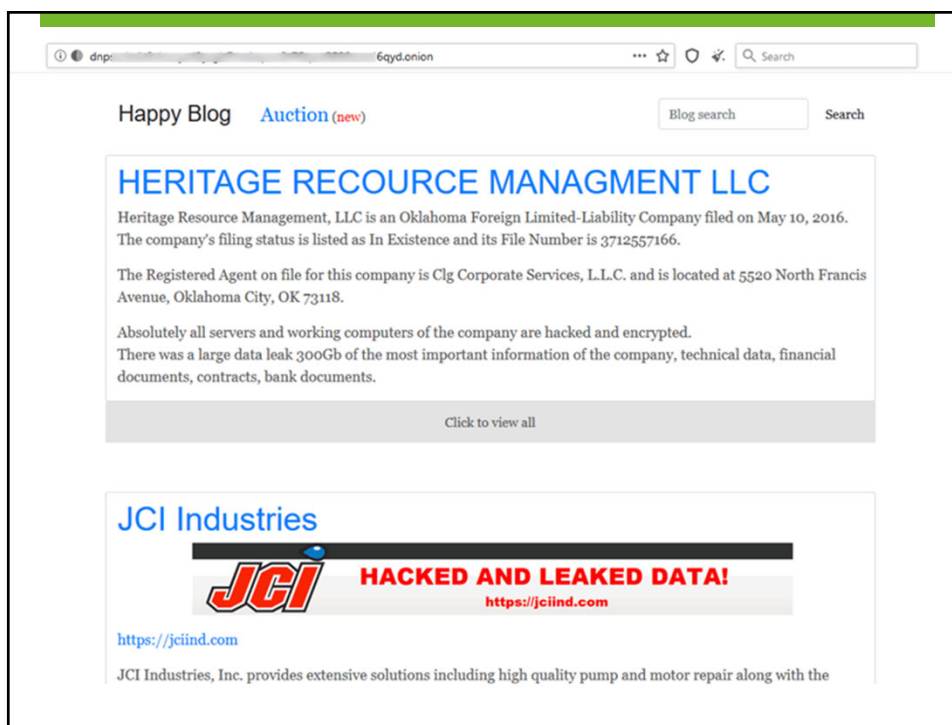
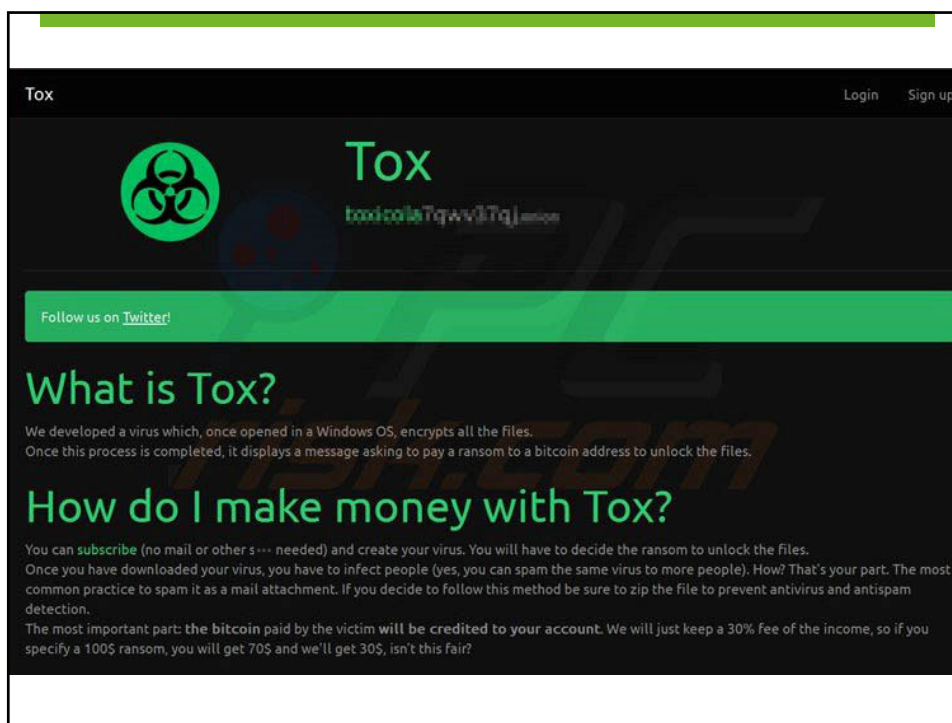
13

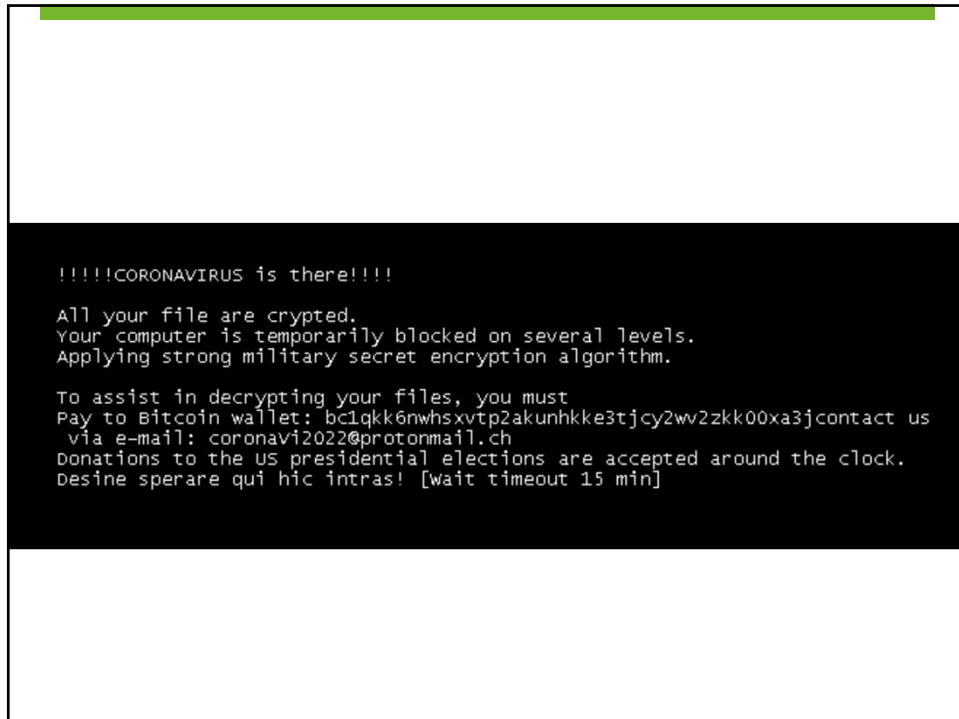


14

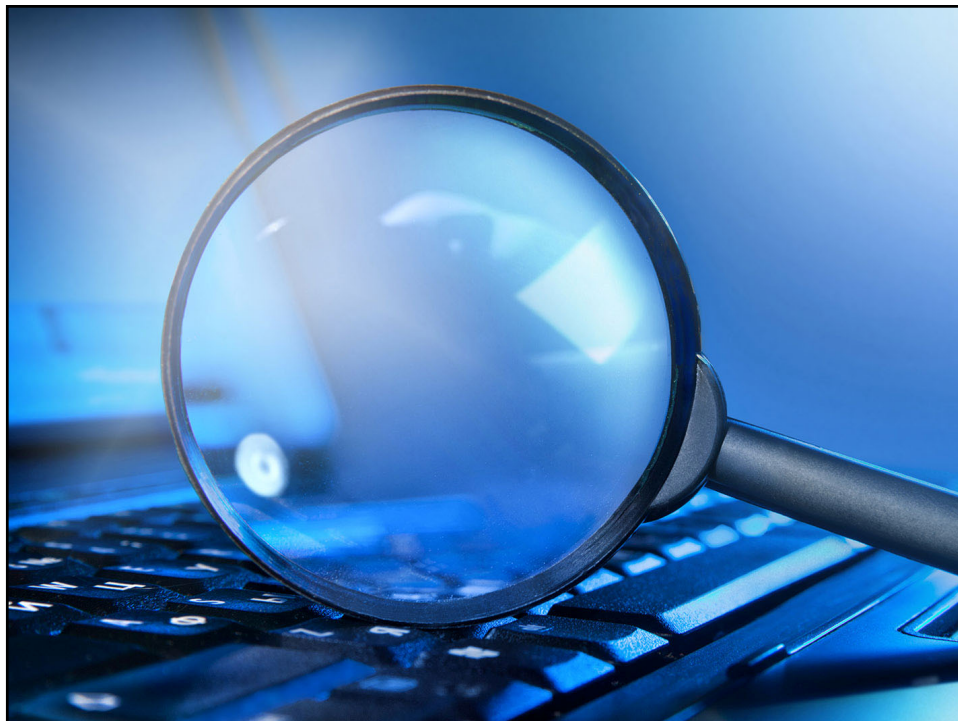








19



20



21



22

## Predominance of Ransomware

---



Source: Sophos "The State of Ransomware 2021" Report

23

## Predominance of Ransomware

---

- 37% of organizations hit in 2021
- Reduction could be in part to evolving attack methods
  - Less automated, more hands-on "human-hacking"
- Targeted attacks
  - Potential for damage is much higher

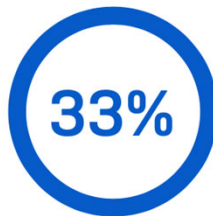
Source: Sophos "The State of Ransomware 2021" Report

24

## Predominance of Ransomware

- Larger organization are more likely to be affected

100 - 1,000  
employees



1,001 - 5,000  
employees



Source: Sophos "The State of Ransomware 2021" Report

25

## Predominance of Ransomware

- Geographics
  - India, Austria, and the U.S. are top popular targets
    - U.S. – half of organizations reported being hit
- Sector-specific
  - Retail and education still at the top (44%)
  - Health care and financial below average (34%)

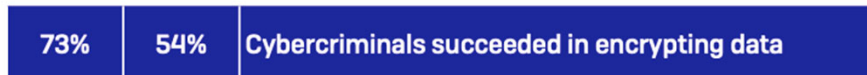
Source: Sophos "The State of Ransomware 2021" Report

26

## Impact

- Encryption of data is down year-over-year
- Great news for organizations
  - Better-trained employees
  - Asset protection methods working
  - Anti-ransomware technology adaptation

**2020**   **2021**



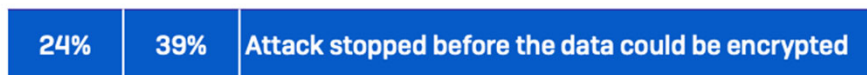
Source: Sophos "The State of Ransomware 2021" Report

27

## Impact

- Extortion of data has almost doubled year-over-year
  - Threat of publishing data
  - Requires much less effort
    - No encryption/decryption needed

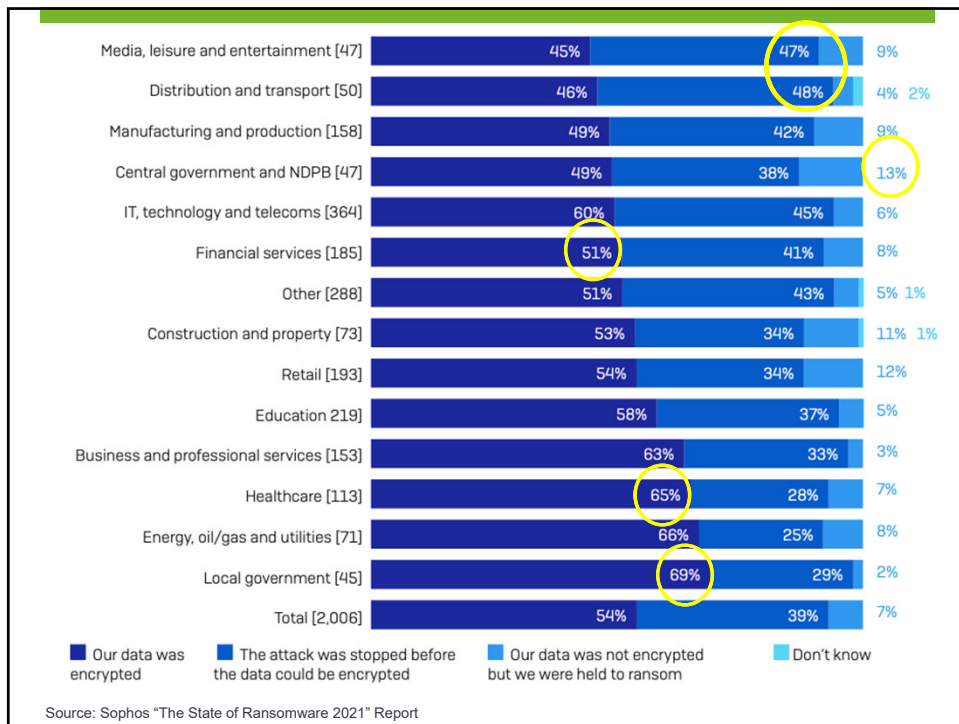
**2020**   **2021**



Source: Sophos "The State of Ransomware 2021" Report

28





29

## Impact

- More ransom payments being made
  - 60% used backups to restore data
- Almost everyone got some of their data back
- Ability to restore data – likelihood to pay ransom



Source: Sophos "The State of Ransomware 2021" Report

30

## Cost

- Paying the ransom doesn't guarantee data restoration
- When data is restored, it isn't all of it
  - All data restored – 8% of victims
- Payment can further target your organization



Source: Sophos "The State of Ransomware 2021" Report

31

## Cost

- Payments vary greatly
  - Organization size
    - 100 – 1000 employees – \$107,000
    - 1000 – 5000 employees – \$225,000
  - Attack nature
  - Physical location



Source: Sophos "The State of Ransomware 2021" Report

32

## Cost

- Remediation has doubled year-over-year
  - Average cost \$1.85 million
  - Varies by location
- Rectifying impact
  - Downtime (systems and people)
  - Device and network costs
- Israel – lowest overall costs



Source: Sophos "The State of Ransomware 2021" Report

33

## Looking Forward

- The Good:
  - Organizations expect to be affected by ransomware
  - Stakeholders express confidence in their mitigation techniques
  - Incident Response Plans becoming standard

Source: Sophos "The State of Ransomware 2021" Report

34

## Looking Forward

---

- The Bad:
  - 37% believe “air gapped” backups won’t result in a ransomware attack
  - 32% claimed cybersecurity insurance protects them
  - **17% don’t believe they are a target**

Source: Sophos “The State of Ransomware 2021” Report

35



36

## Vendor Management

---

- Establish initial and ongoing due diligence
  - Critical and non-critical vendors
- Financials, risk assessments
- Security controls, audit reports
- Recovery and response procedures
- Contract review



37

## Internal Policies

---

- Establish and update cybersecurity-related policies
  - Information Security Program
  - Incident Response Plan
  - Business Continuity & Disaster Recovery
  - Acceptable Use Policy



38

## Asset Management

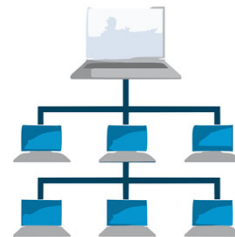
- Centralized management for all devices
  - Security updates, anti-malware
  - Comprehensive inventory for mitigating issues
- Enforce restrictions
  - Cloud data access
  - Unauthorized applications
  - Unauthorized users



39

## Network Protection Controls

- Next-gen anti-malware
- SIEM platform
- Block executable files and email attachments
- Consider additional email controls
  - Sandboxing (APT in Office 365)
  - Authentication technologies
- Egress firewall controls



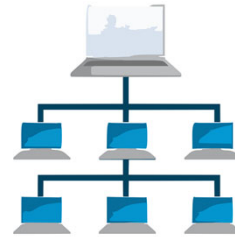
40



## Network Protection Controls

---

- Application whitelisting
- Disable macros
- Restrict/remove local admin privileges
- Deploy file integrity monitoring
- Read-only file shares

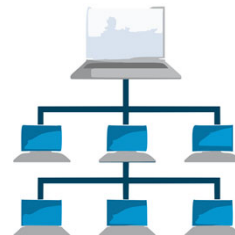


41

## Network Response Controls

---

- Block command-and-control server access
- Recall known phishing emails
- Take infected systems offline
- Check encrypted file ownership



42

## Backup Process

---

- Validate and authenticate current backup processes
- System should allow archive of multiple iterations
- Establish adequate schedule and retention methods
- Routinely test for data integrity



43

## User Administration

---

- Identify and control access to resources
- Provision users correctly
  - Establish rights for each subset of users
  - Create individual accounts for each employee
  - Limit access to data and information
- Review regularly – transfers, terminations, stale accounts



44

## Access Controls

---

- Passwords
  - Various complexities to consider
- Layered security
  - Account lockout
  - Biometric authentication
  - Multi-factor authentication



45

## Training

---

- All employees should participate
- Methods will vary — webinar, email, newsletters, etc.
- Review policies and procedures
- Roundtable testing
- Real-world examples
- Build culture of awareness



46

## Join Us for Our Next Cyber Series Webcast

### **Remote Working: What We've Learned In the Past Year**

Wednesday, August 4

1:00 – 2:00 p.m. EDT

Learn more at [capincrouse.com](https://capincrouse.com)




47

## You Could Win a Free CapinTech Cyber Checkup!

- Receive one entry for each 2021 CapinTech Cyber Series webcast you:
  - Attend live, or
  - Watch the recording of within one week of the webcast date
- Winner announced in December



48



# Thanks

Thomas L. Tyler, Jr.  
Cybersecurity Advisor

---

✉ [ttyler@capincrouse.com](mailto:ttyler@capincrouse.com)

📱 505.50.CAPIN

© 2021 Capin Technology LLC

