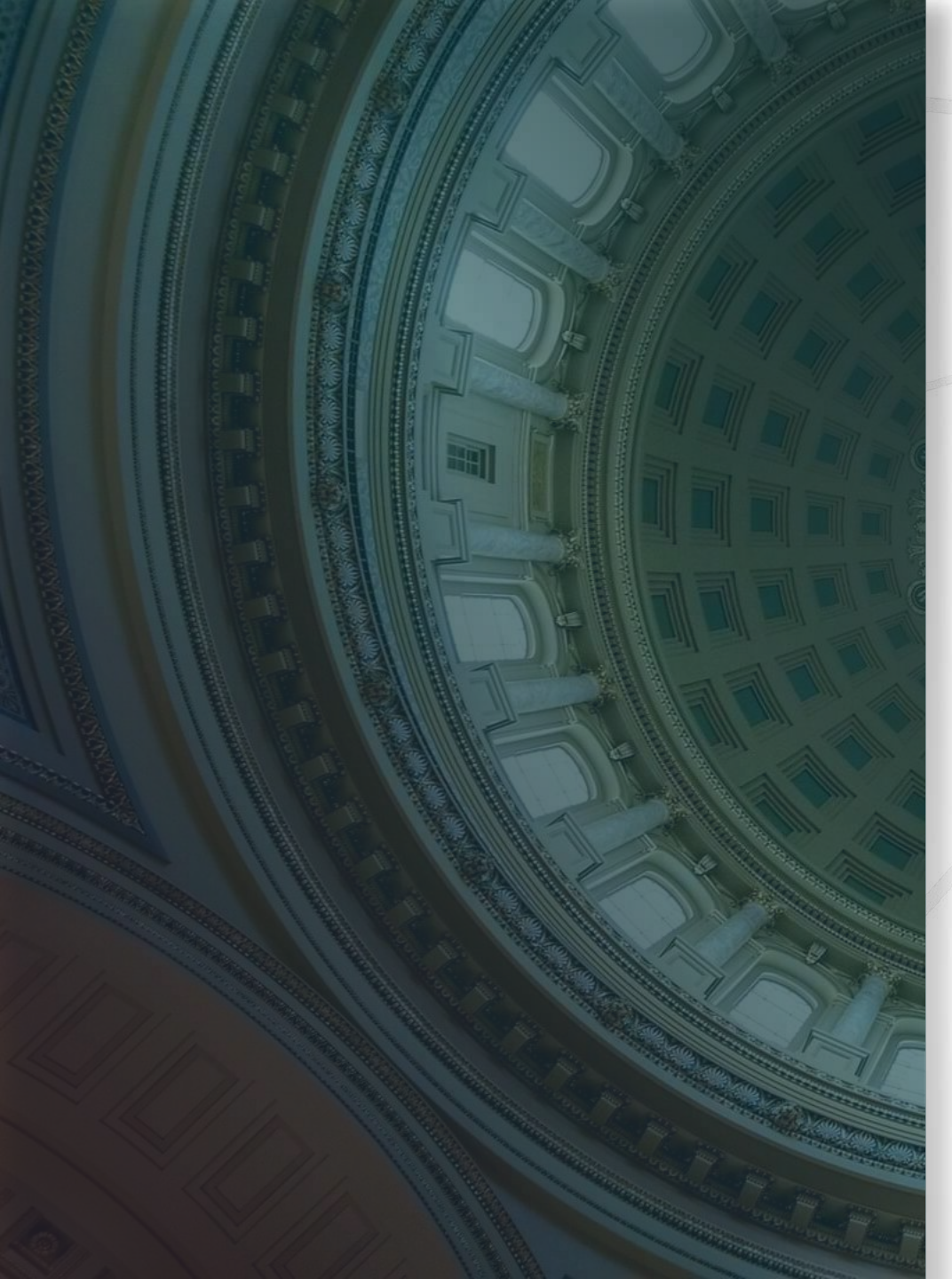
Best Practices Following a Ransomware Event

TECH TALKS: PREPARE, PROTECT & POSITION LONG TERM CARE



TODAY'S PRESENTER

CHRISTOPHER GERG

CISO & VP of Cyber Risk Management,
Tetra Defense

cgerg@tetradefense.com

TETRA DEFENSE

RANSOMWARE THE BUSINESS

RANSOMWARE IS A CRIMINAL **INDUSTRY**

Cybercriminals operate with different exploitation departments and "customer" service tactics.

A noticeable attack is most likely not their first step – they've possibly been in your network for MONTHS.

THEY ARE CHANGING THE GAME

Several types of ransomware now post sensitive data on the Internet if ransoms are not paid, meaning data was technically exfiltrated and thus considered a breach.

Threat actors are reaching out to local media and patients touting data compromise.

CYBERSECURITY INSURANCE FOR BUSINESSES IS **VITAL.**

TETRA DEFENSE

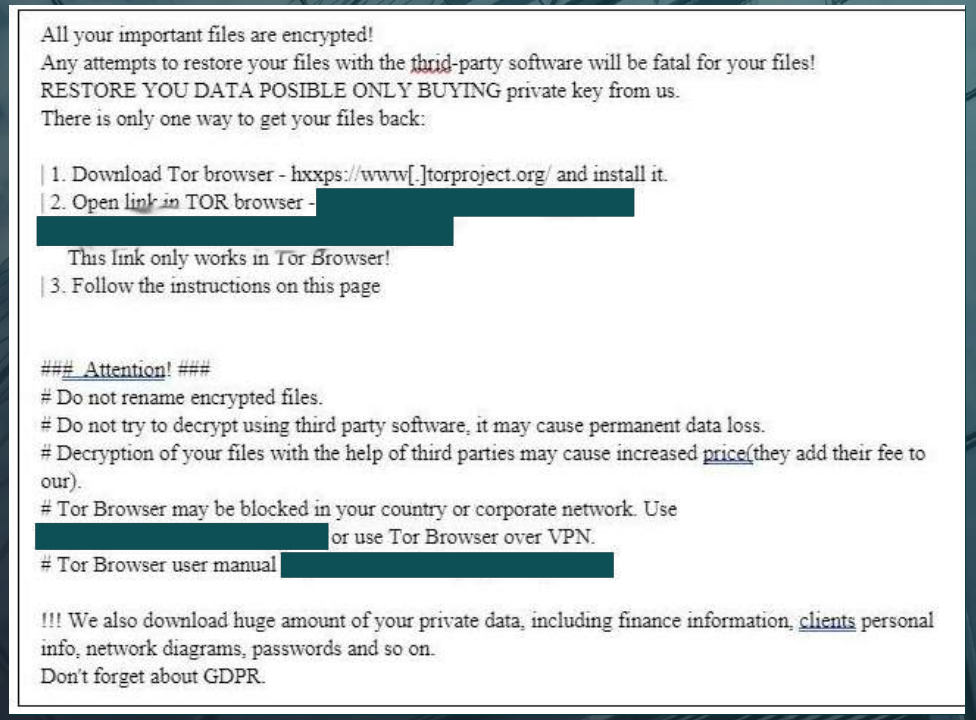
Preparing for Ransomware

Implementation of these safeguards will better prepare your organization in the event of a ransomware attack.

- Obtain Cyber Liability insurance
- Develop (or refine) your Incident Response Plan
- Implement robust Anti-malware (as opposed to signature-based antivirus)
- Segregate your backups from internal networks and systems
- Setup centralized logging and auditing

TETRA DEFENSE

WHEN CRISIS STRIKES



All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

| 1. Download Tor browser - hxxps://www[.]torproject.org/ and install it.
| 2. Open link in TOR browser - [redacted]
This link only works in Tor Browser!
| 3. Follow the instructions on this page

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
Tor Browser may be blocked in your country or corporate network. Use [redacted] or use Tor Browser over VPN.
Tor Browser user manual [redacted]

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on.
Don't forget about GDPR.

Responding to Ransomware

Every incident is different and may require different incident response strategies.

- Call your insurance agent/carrier or an incident response firm.
- Invoke your Incident Response Plan.
- Unplug the Internet and remove infected systems from the network entirely, if possible.
- Do NOT reboot infected systems – doing so will damage evidence to understand what happened.
- Do not turn on machines that might have been off when the attack happened.

TETRA DEFENSE

The Road to Recovery

Attackers may have lurked in your network for months and may have tools in place to get back in. Focusing on large-scale safeguards and a thorough forensics investigation will help determine if there is still imminent threat.

- Examine anti-virus logs for evidence of tools like Mimikatz, Cobalt Strike.
- Install an Advanced Threat Protection (ATP) tool (SentinelOne, Carbon Black, Crowdstrike, FireEye, etc.) on every system.
- Invoke breach notification protocols (if there is reason to believe data was stolen).
- Identify any remaining gaps with a third-party information security assessment.

TETRA DEFENSE


THANK YOU