M3 INSURANCE | TETRA DEFENSE

PRESENTED BY

CHRISTOPHER GERG
CISO & VP of Cyber Risk Management
cgerg@tetradefense.com

TECH TALKS: Prepare, Protect and Position Long Term Care

BEST PRACTICES FOLLOWING A RANSOMWARE EVENT

PREPARING FOR RANSOMWARE:

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

- **OBTAIN CYBER LIABILITY INSURANCE**
  Insurance is vital to protecting your organization.
- **DEVELOP AN INCIDENT RESPONSE PLAN**
  Be sure to highlight who is in charge of which plans of action.
- **IMPLEMENT ROBUST ANTI-MALWARE**
  We recommend having more than just a signature-based anti-virus.
- **SEGREGATE BACKUPS FROM INTERNAL SYSTEMS**
  This keeps backups more protected in case of attack.
- **SET UP CENTRALIZED AUDITING AND LOGGING**
  This allows for quick inventory of all actions and devices.

RST

RANSOMWARE STRESS TEST™

This free self-assessment evaluates your organization's susceptibility and ability to respond to a ransomware attack.

RST.tetradefense.com

WHEN DISASTER STRIKES

Ransomware is a Criminal Industry

"CUSTOMER" SERVICE RESOURCES
Most Threat Actors practice reputation management and offer live chat services when negotiating with victim organizations.

DELAYED REACTION
Most victims do not experience an immediate attack after the first sign of suspicious activity. Threat Actors are prone to lurking within a network for months before deploying ransomware.

"NAME AND SHAME" TACTICS
As opposed to simply encrypting files and rendering them inaccessible, Threat Actors may incentivize paying ransoms by threatening data breaches on their sites.

CUSTOMIZED ATTACKS
Personalized messaging, taunting requests, and even reaching out to relevant local media outlets are common tactics used by threat actors.

Example Ransom Note

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 -

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
or use Tor Browser over VPN.
Tor Browser user manual

!!! 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.

STEP-BY-STEP RESPONSE

Call your insurance agent / carrier or Incident Response Firm	Invoke your Incident Response plan and communicate with key leaders	Unplug the Internet and remove infected systems from the network entirely if possible
Do NOT reboot infected systems — doing so may damage evidence	Do not turn on machines that may have already been off during the attack	Identify any remaining security gaps with a 3rd-party assessor