TECH TALKS: Prepare, Protect and Position Long Term Care

RANSOMWARE PREVENTION STRATEGIES

RANSOMWARE THE BUSINESS

- Cybercriminals operate with different exploitation departments and "customer" service tactics.
- Ransomware strains now posts sensitive data on the Internet if ransoms are not paid.
- Threat actors reach out to local media and patients touting data compromise, rendering Cyber Insurance even more vital for organizations.

CURRENT RANSOMWARE TRENDS:

NAME, SHAME AND SHARE

For organizations who don't pay ransoms, Threat Actors may threaten to expose the attack publicly and may expose exfiltrated data on public share and shame sites.

REPUTATION MANAGEMENT

Ransomware Threat Actors are starting to try to manage the reputational fallout of their activities, selling themselves as benevolent and as security crusaders. This only furthers their mission to use deception as their main strategy.

COVID-19 SCAMS

The pandemic has been leveraged by Threat Actors to craft phishing emails and malicious documents as the initial compromise point for ransomware attacks.

MISUSE OF LEGITIMATE TOOLS

Ransomware Threat Actors are continuing to use legitimate Remote Access tools and Security tools in their attacks.

- Remote Mgmt. Tools
- Cobalt Strike / Cloudflare to protect public sites

PRESENTED BY CHRISTOPHER GERG
CHIEF INFORMATION SECURITY OFFICER
VICE PRESIDENT OF CYBER RISK MANAGEMENT
cgerg@tetradefense.com

HOW THEY GET IN

Compromised User Accounts

BREACH COMPILATION DATABASE
Credentials can be harvested for purchase from the Dark Web.

ABSENCE OF MULTI-FACTOR AUTHENTICATION
(MFA) – The necessary, secondary barriers to protect accounts.

LACK OF PERSONAL VIRTUAL PRIVATE NETWORKS
(VPN) – Maintains a private network on a public internet to keep internal files safe.

LACK OF PASSWORD MANAGERS / VAULTS
We recommend the services 1Password, LastPass, & KeePass. Features include instant creation of strong, random passwords.

Insecure Systems / User Error

INSECURE SERVICE
Remote Desktop Protocol (RDP) is a common gateway into an internal network.

BUSINESS EMAIL COMPROMISE
While messages come from a legitimate address, the author of the messages is not who they appear to be.

UNPATCHED SERVICES
VPNs, Web Servers, and Email Servers operating on older versions are prone to known exploits.

TRICKED END USERS
Phishing and Social Engineering can be convincing and play to a User's impulse to "click here."

HOW TO IMPROVE YOUR DEFENSES

RST RANSOMWARE STRESS TEST™

This free self-assessment evaluates your organization's susceptibility and ability to respond to a ransomware attack. This tool includes comprehensive questions that evaluate your current configuration and procedures. The end result is an in-depth overview of any warning signs and how to remedy them.

Once complete, you'll have access to extensive resources to walk through how to improve and address the vulnerabilities our incident response team sees most.

Start the test at RST.tetradefense.com

M3 INSURANCE | TETRA DEFENSE