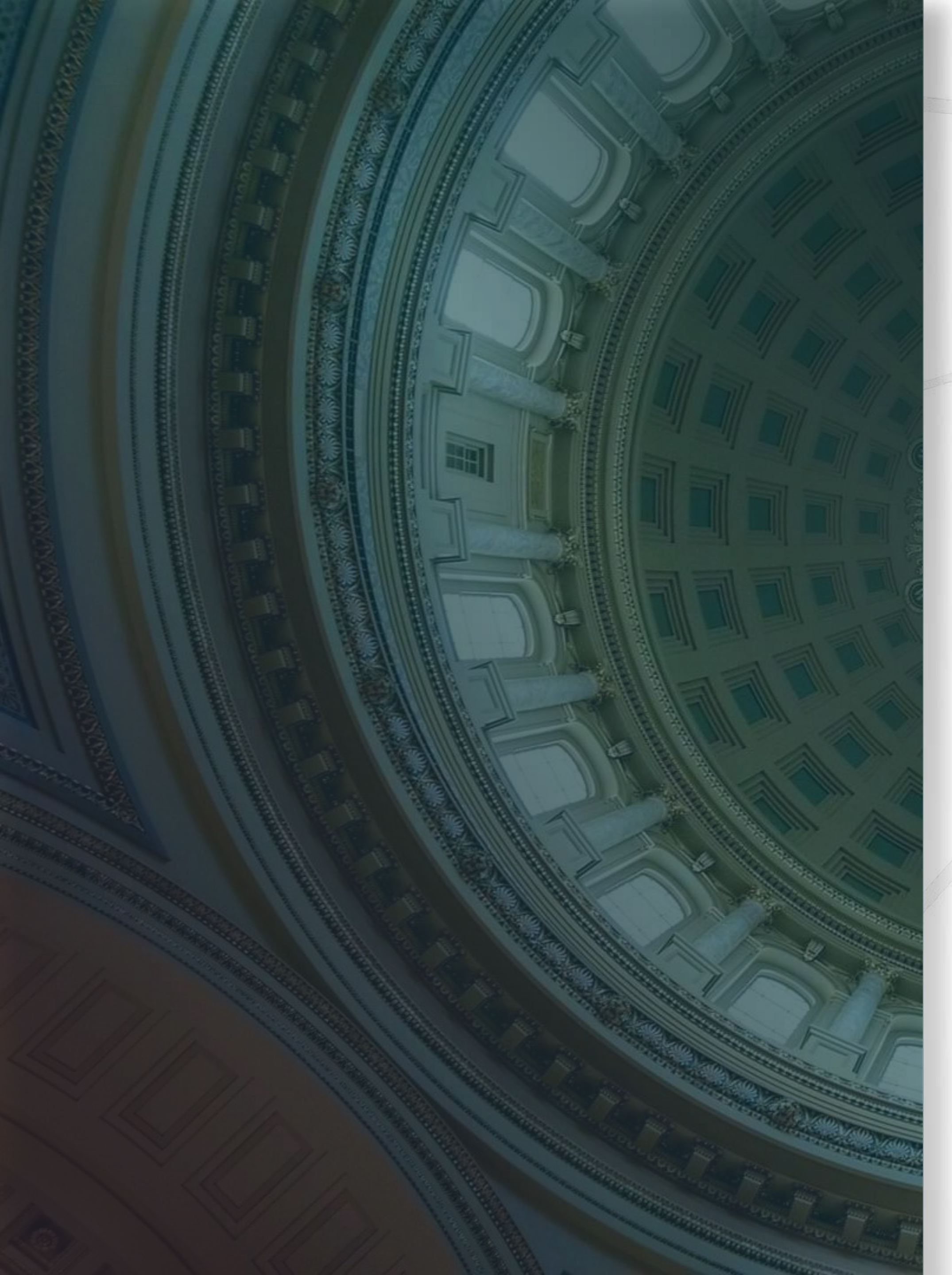
TETRA DEFENSE

RANSOMWARE PREVENTION STRATEGIES

TECH TALKS: PREPARE, PROTECT & POSITION LONG TERM CARE



TODAY'S PRESENTER

CHRISTOPHER GERG

CISO & VP of Cyber Risk Management,
Tetra Defense

cgerg@tetradefense.com

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

Maze ransomware now posts 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.**

CURRENT RANSOMWARE TRENDS:

NAME, SHAME, & 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.

- Sodinokibi
- DoppelPaymer
- Maze

COVID 19 RANSOMWARE SCAMS

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

- Netwalker

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.

- DoppelPaymer
- Maze
- Clop

CONTINUED USE 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

HOW THEY GET IN

COMPROMISED USER ACCOUNTS

BREACH COMPILATION DATABASE

(The Dark Web)

ABSENCE OF MULTI-FACTOR AUTHENTICATION

(MFA)

LACK OF PERSONAL VIRTUAL PRIVATE NETWORKS

(VPNs)

LACK OF PASSWORD MANAGERS/VAULTS

(1Password, LastPass, KeePass)

Insecure Systems / User Error

Insecure Services

(RDP)

Business Email Compromise

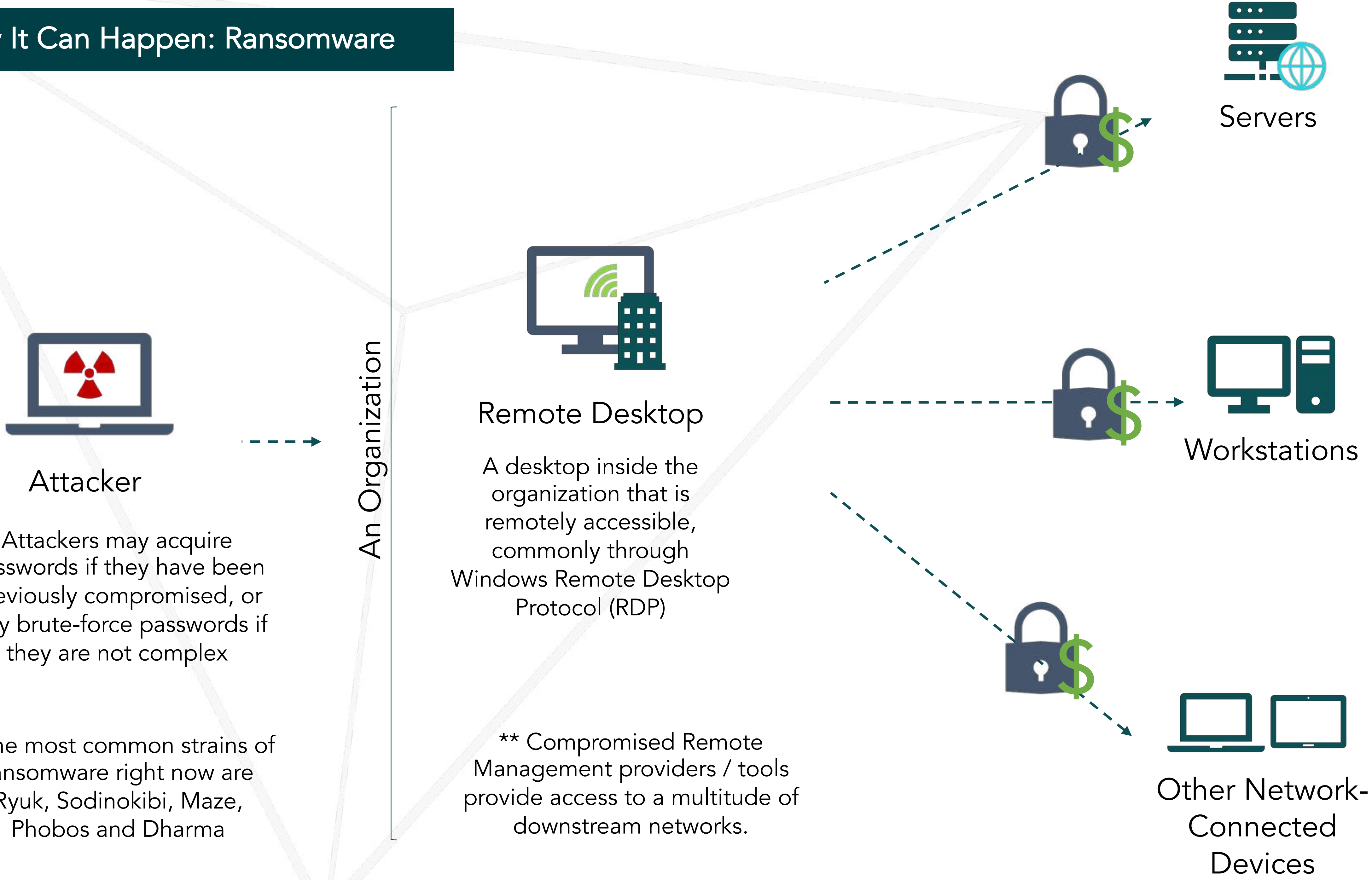
Unpatched Services

(VPNs, Web Servers, Email Servers)

Tricked End Users

(Phishing, Social Engineering)

How It Can Happen: Ransomware



Attacker

Attackers may acquire passwords if they have been previously compromised, or may brute-force passwords if they are not complex

* The most common strains of ransomware right now are Ryuk, Sodinokibi, Maze, Phobos and Dharma

An Organization

Remote Desktop

A desktop inside the organization that is remotely accessible, commonly through Windows Remote Desktop Protocol (RDP)

** Compromised Remote Management providers / tools provide access to a multitude of downstream networks.

Servers

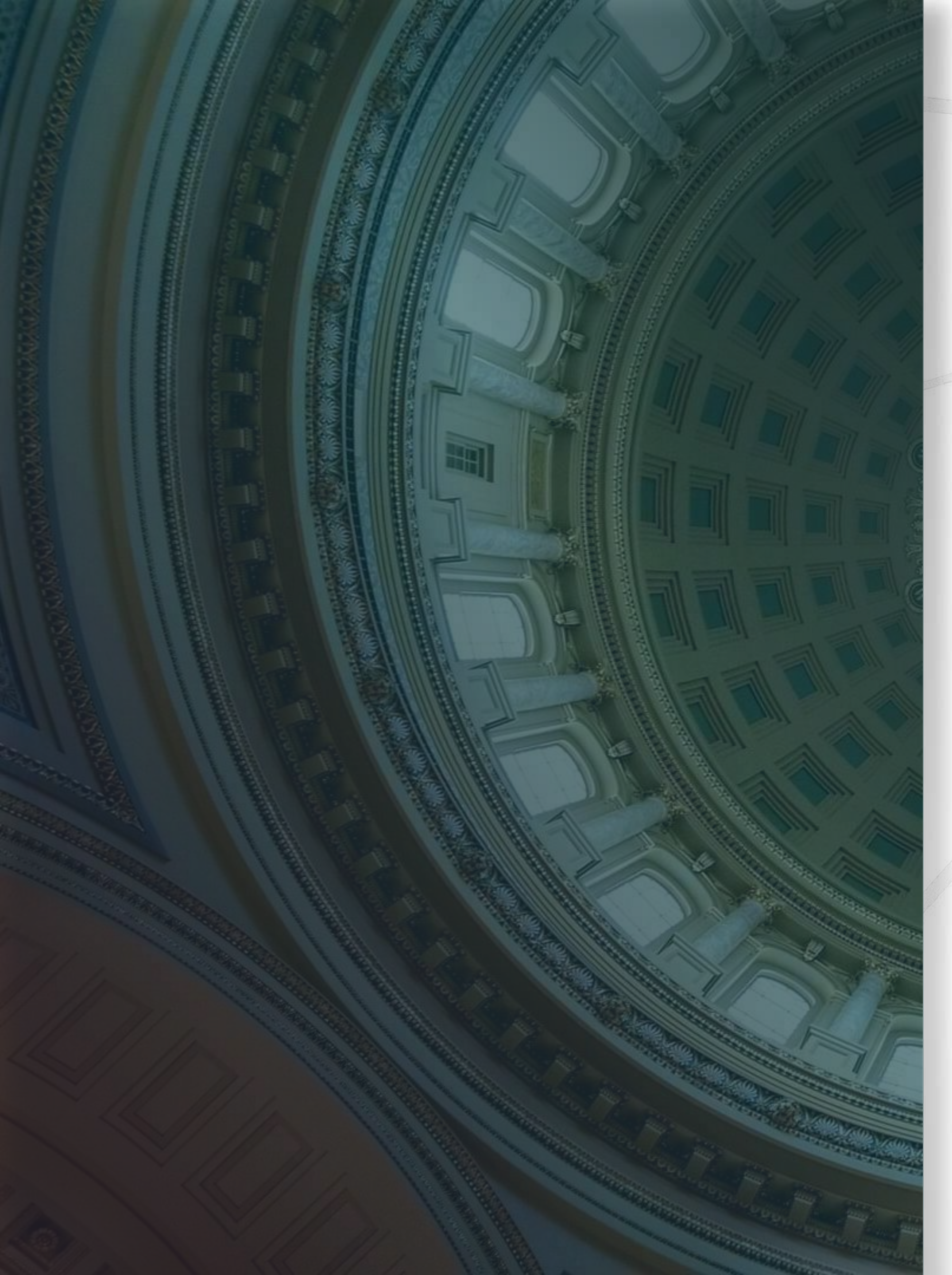
Workstations

Other Network-Connected Devices

HOW TO IMPROVE YOUR DEFENSES

HOW CAN I REDUCE MY RISK?

- ✓ Limit what services you open up to the public Internet
- ✓ Keep systems and services patched and updated
- ✓ Set remote access restrictions and multiple login lockout
- ✓ Increase email compromise/ phishing awareness training
- ✓ Always use complex passwords and two-factor authentication
- ✓ Always verify email senders are valid and trusted



RANSOMWARE STRESS TEST™

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

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

THANK YOU