RANSOMWARE MITIGATION STRATEGIES

wba
ON AIR
WISCONSIN BROADCASTERS ASSOCIATION

Oct. 12, 2022

AGENDA

What is ransomware & how has it evolved?

How does ransomware work?

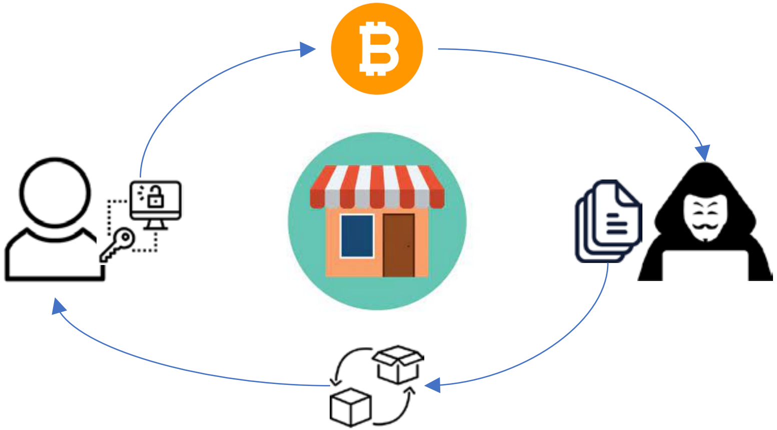
Prevention and mitigation strategies

Ransomware response

ORIGINS OF RANSOMWARE

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the system that rely on helm unstable.

Cyber Security and Infrastructure Security Agency



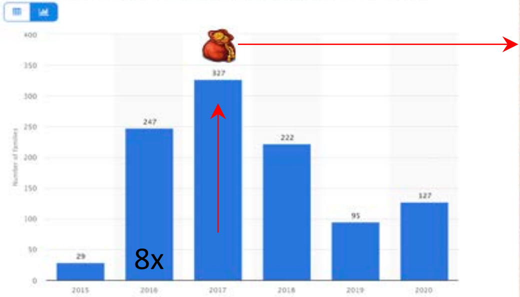
Every functioning commercial enterprise needs a marketplace to sell goods and currency to purchase goods.

RANSOMWARE BANDWAGON: ALL ABOARD!!!

In 2016, there was a massive uptick in ransomware variants as cybercriminals were organizing their business models to be more efficient. Ransomware as a service was created which started a golden age for cybercriminals in 2017.

2016-1028: The Golden Era of Ransomware

*Number of newly discovered ransomware families worldwide from 2015 to 2020



WANTED

- Ranzy
- Avaddon
- Babu Locker
- Clop
- Conti
- Cuba
- Darkside (Colonial Pipeline)
- Doppelpaymer
- Egregor
- Everest
- Lockbit
- Maze
- Mespinoza
- Mount Locker
- Nefilim
- Nemty
- Netwalker
- Ragnalocker
- Ransomexx
- REvil
- Sekhmet
- Snatch
- Suncrypt

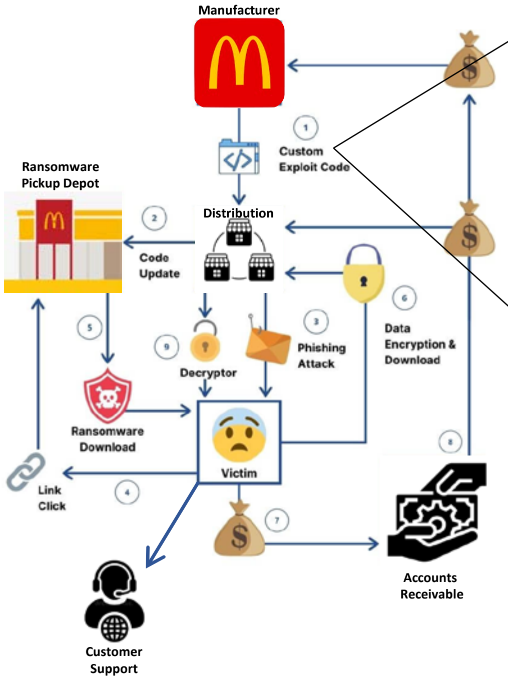
*Source: Sophos State of Ransomware Report

RANSOMWARE AS A SERVICE (RAAS) OPERATION

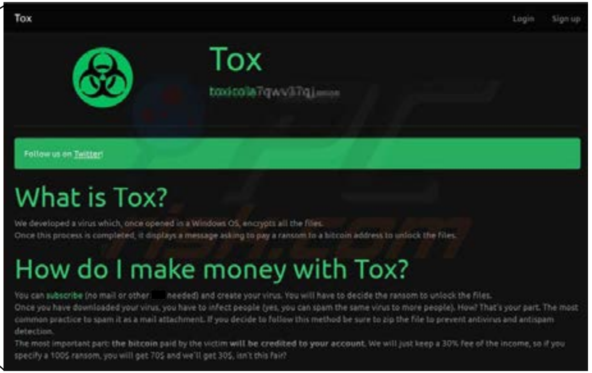
Business Model

RaaS Operators	RaaS Affiliates
• Develops ransomware code • Recruit affiliates on forums	• Pays to use ransomware or profit-sharing agreement • Agrees on service fee per collected ransom
• Gives affiliates access to a “build your own ransomware” package • Creates dedicated “Command & Control” dashboard for affiliate to track the package	• Targets victims • Sets ransom demands • Configures post-compromise user message
	• Compromises victim’s assets • Executes ransomware
• Sets up victim payment portal • ”Assists” affiliates with victim negotiations	• Communicates with the victim via chat portals or other means
• Manages a dedicated leak site	• Manages decryption keys

Transaction Workflow



Zero barrier to entry!



Tox

toxicola7qwv37qj.onion

Follow us on Twitter!

What is Tox?

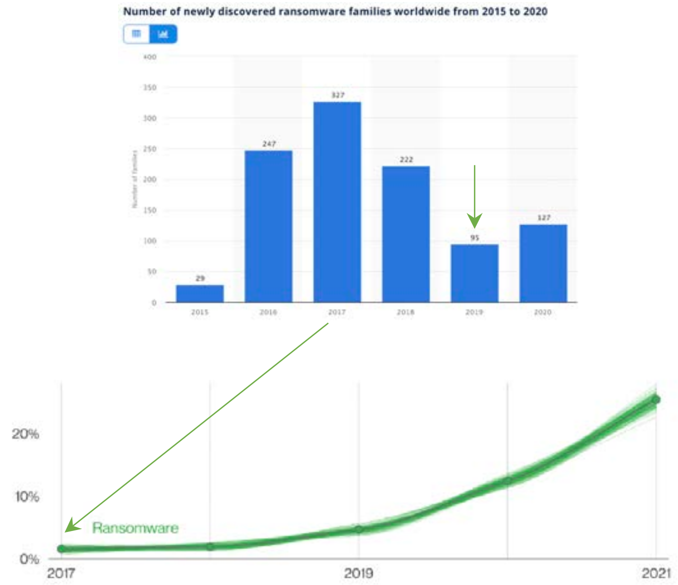
We developed a virus which, once opened in a Windows OS, encrypts all the files.
Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the files.

How do I make money with Tox?

You can subscribe (no mail or other [redacted] needed) and create your virus. You will have to decide the ransom to unlock the files.
Once you have downloaded your virus, you have to infect people (yes, you can spam the same virus to more people). How? That's your part. The most common practice to spam it as a mail attachment. If you decide to follow this method be sure to zip the file to prevent antivirus and antispam detection.
The most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will just keep a 30% fee of the income, so if you specify a 100$ ransom, you will get 70$ and we'll get 30$, isn't this fair?

RANSOMWARE EVOLUTION: NEW RECIPE, SAME OLD DISH

- Ransomware has evolved from a “smash and grab” crime of opportunity to a sophisticated, well-planned heist.
- These criminals are investing more time to infiltrate an organization and understand how it operates before detonating ransomware.
- They are employing new methods, dubbed “double extortion," where data is stolen before encryption and threatened to be released.
- They understand the cyber insurance market and are demanding ransoms within coverage to increase likelihood of payment.



* **Figure 6.** Ransomware over time in breaches

*Source: 2022 Verizon Data Breach Investigation Report

RANSOMWARE OPERATORS M.O.

Most common attack paths

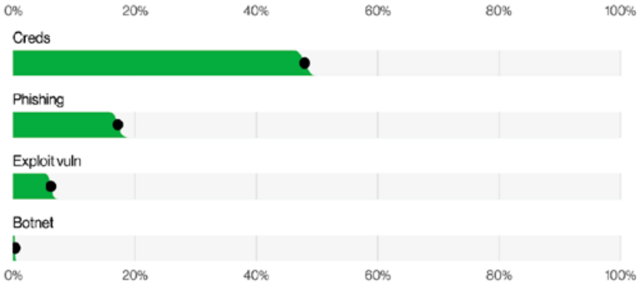


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

Target of attack (WHAT)

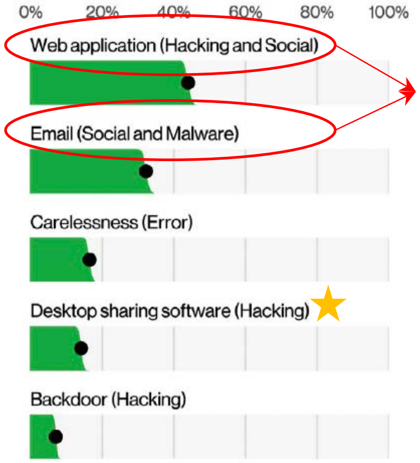


Figure 18. Top Action vectors in breaches (n=3,279)

Internet facing +

Method of attack (HOW)

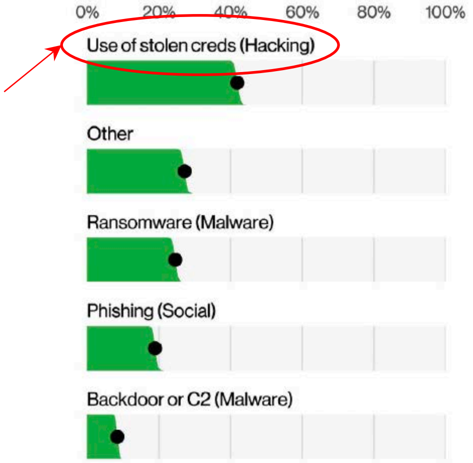


Figure 19. Top Action varieties in breaches (n=3,875)

If it's on the internet it will be targeted...and if it has a login, you can be sure it's constantly being hit with login attempts.

*Source: 2022 Verizon Data Breach Investigation Report

DISRUPTING THE ATTACK CHAIN

Event Chains

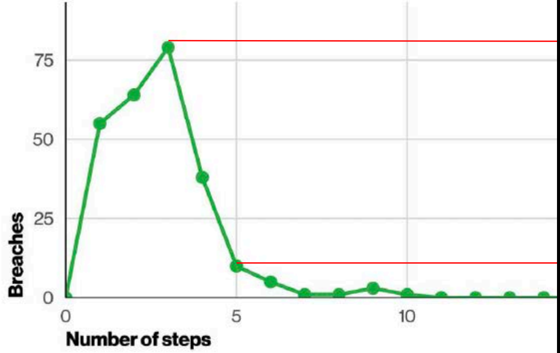
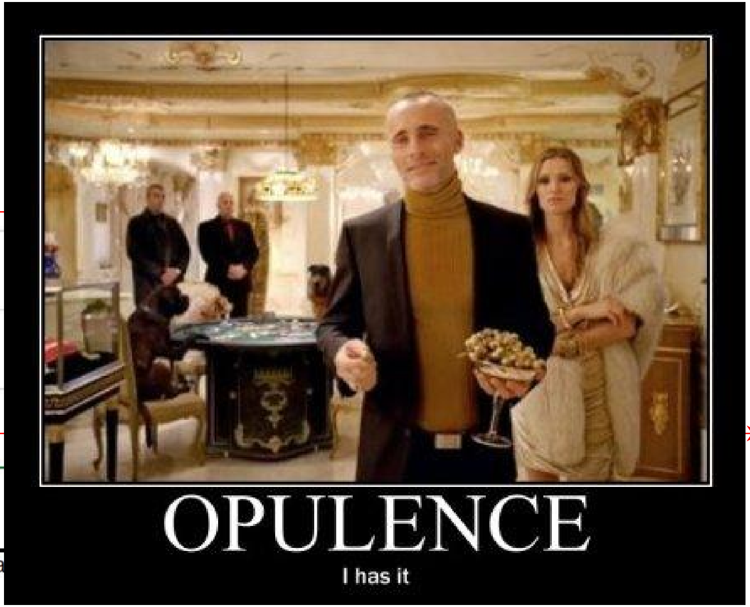
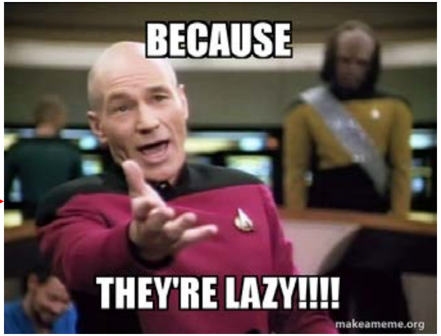


Figure 30. Number of steps per breach in non-Error brea

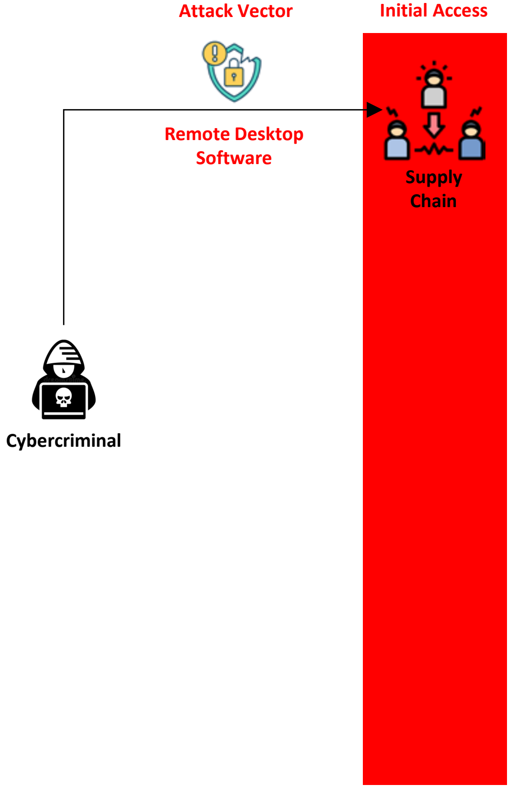




Our job is to complicate the attack as much as possible.

HOW DOES RANSOMWARE WORK?

HOW DOES RANSOMWARE GET IN?



Attack Vector

Initial Access

Remote Desktop Software

Supply Chain

Cybercriminal

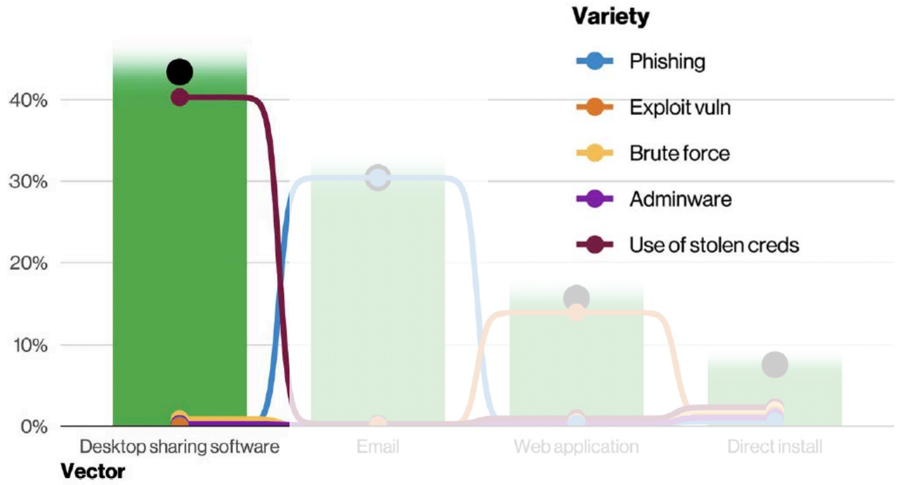
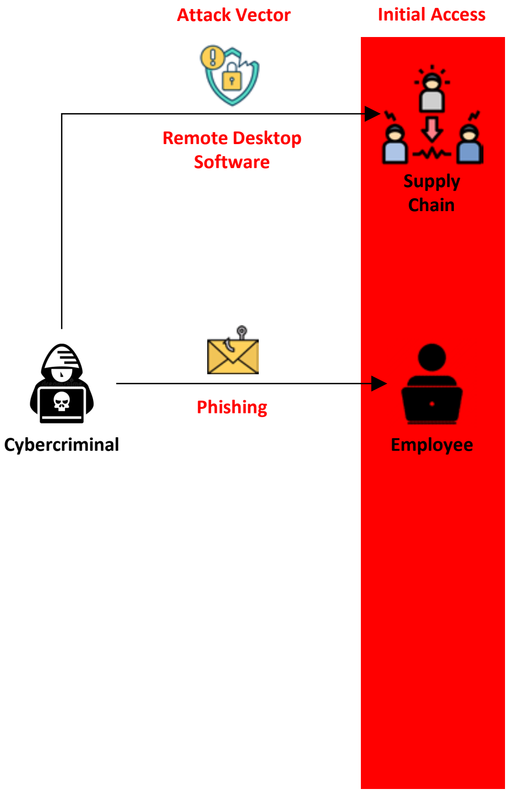


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

HOW DOES RANSOMWARE GET IN?



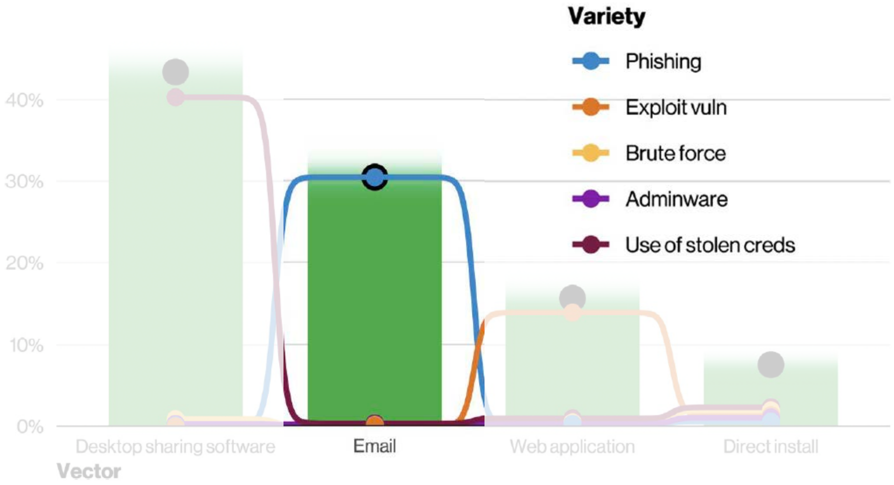
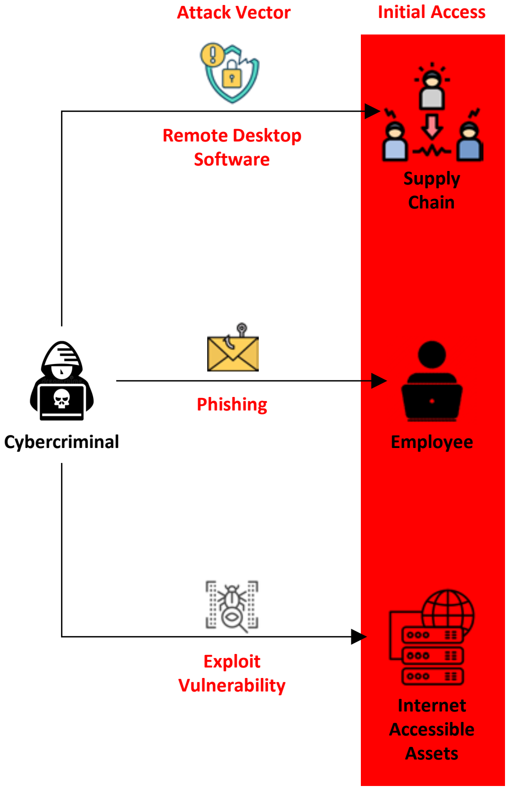


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

HOW DOES RANSOMWARE GET IN?



Attack Vector

Initial Access

Remote Desktop Software

Supply Chain

Phishing

Employee

Cybercriminal

Exploit Vulnerability

Internet Accessible Assets

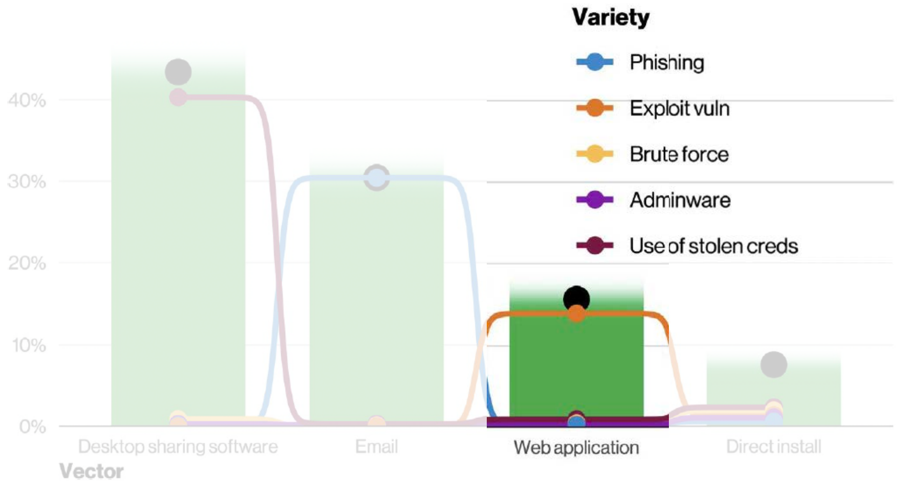
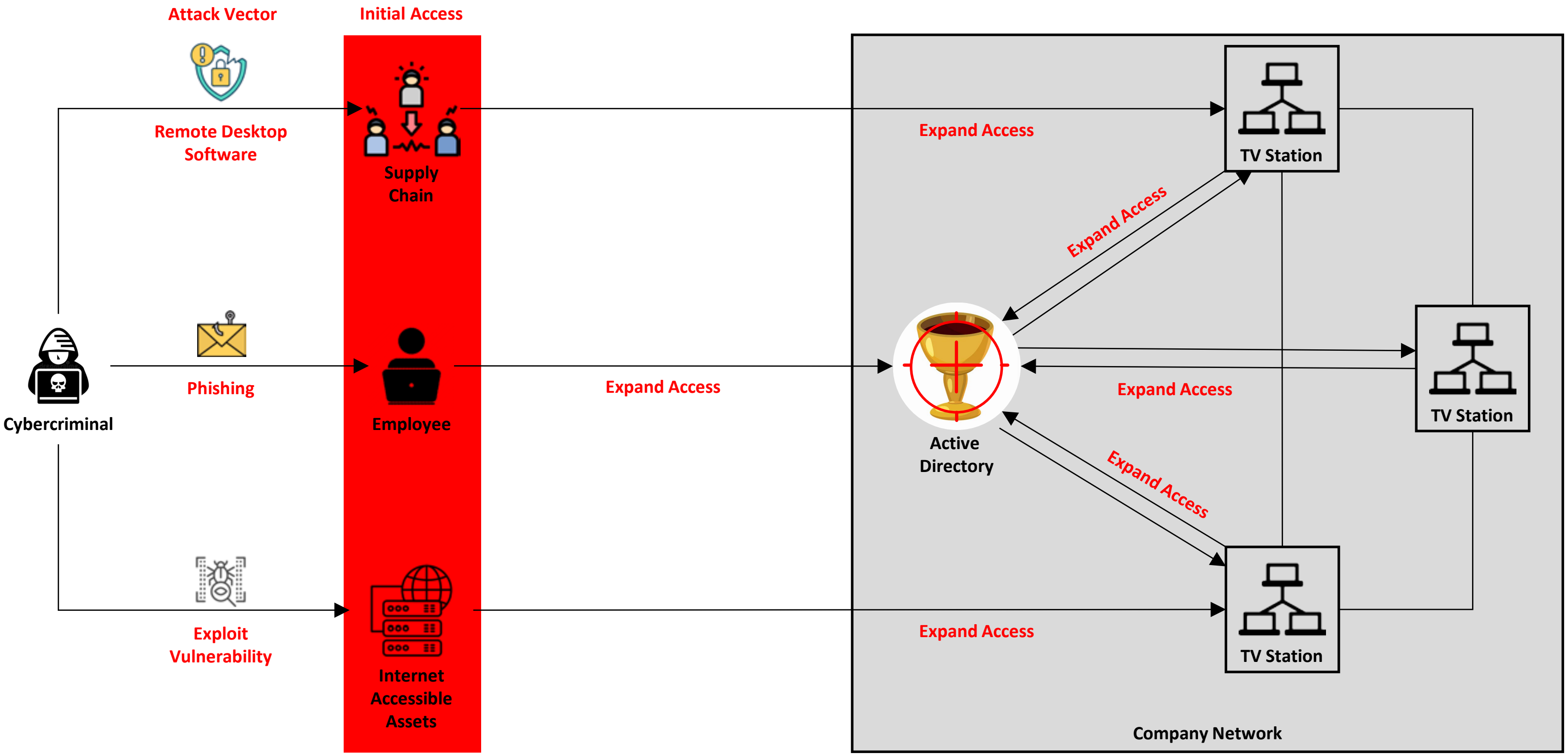


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

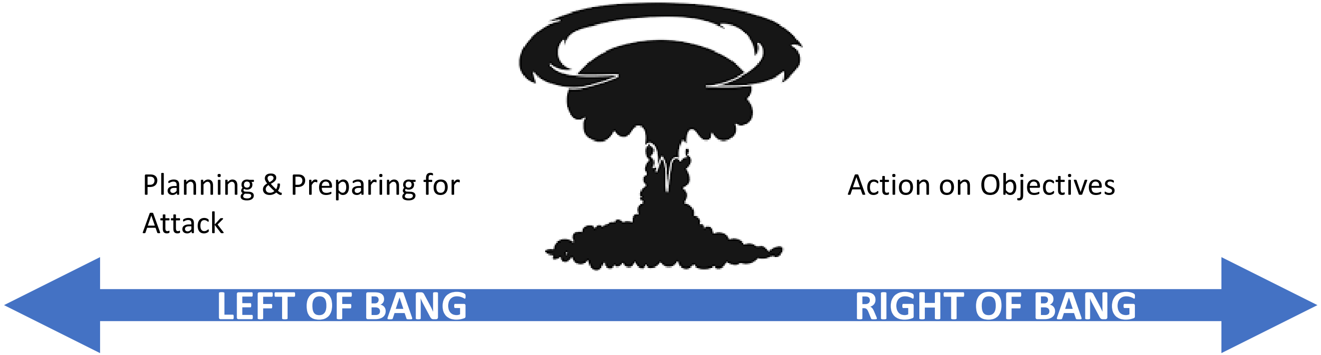
HOW DOES RANSOMWARE SPREAD?



PREVENTION & MITIGATION STRATEGIES

INCIDENT MANAGEMENT 101

Enemy Activities



Planning & Preparing for Attack

Action on Objectives

DAMAGE PREVENTION

LEFT OF BANG

RIGHT OF BANG

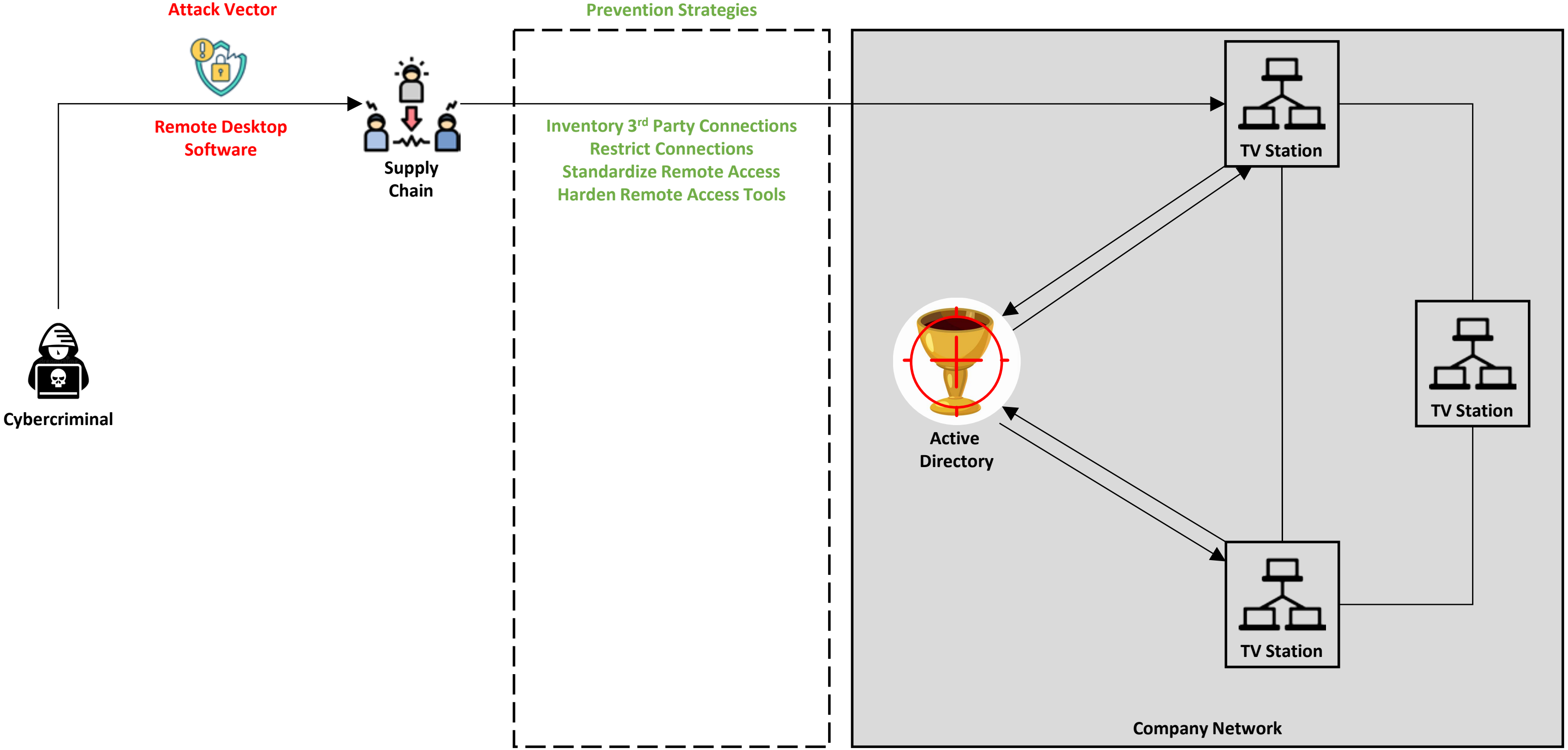
DAMAGE MITIGATION

Observe Pre-Event Indicators & Act to Prevent

Incident Response

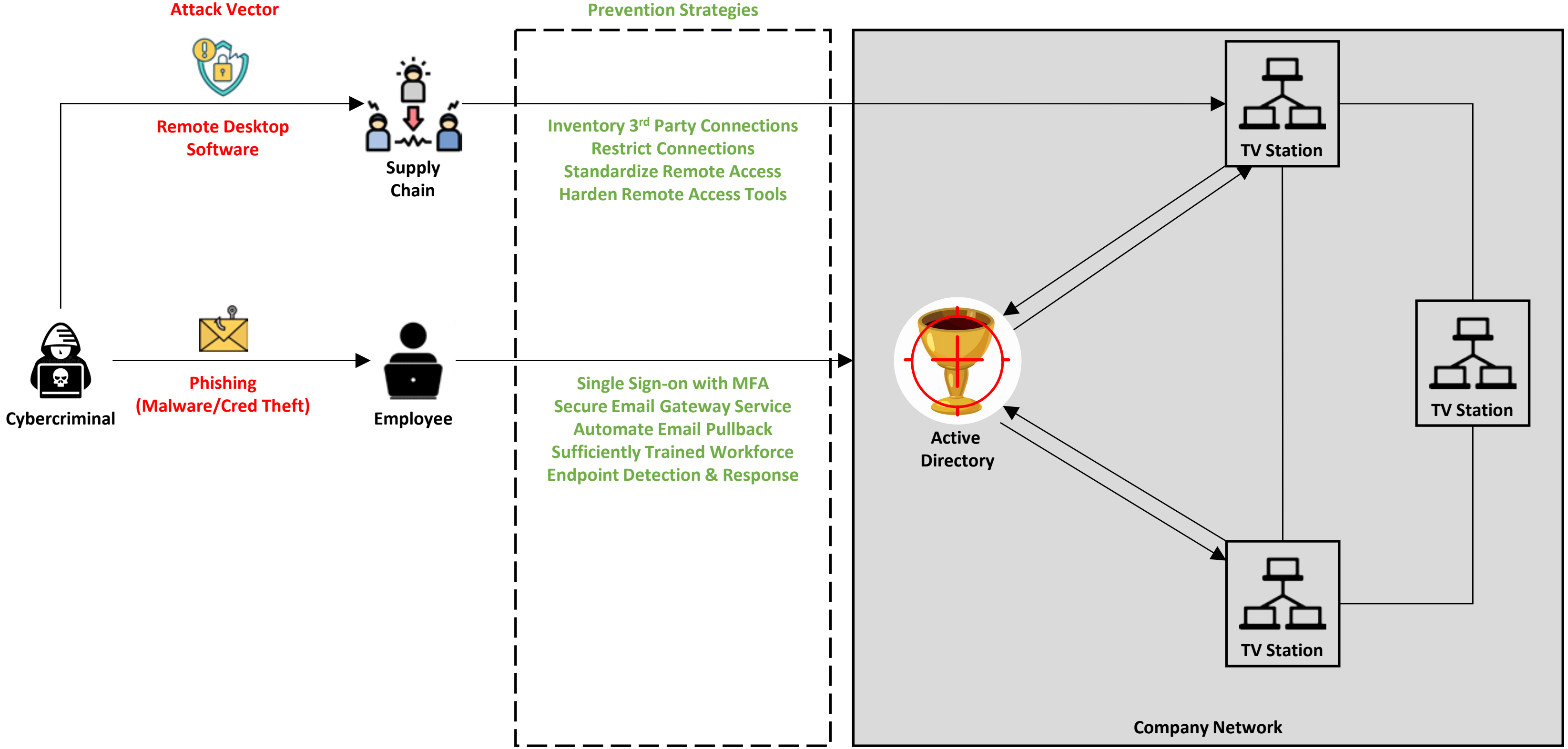
Friendly Force Activities

PREVENTION STRATEGIES



Inventory 3rd Party Connections
Restrict Connections
Standardize Remote Access
Harden Remote Access Tools

PREVENTION STRATEGIES



Attack Vector

Remote Desktop Software

Supply Chain

Prevention Strategies

Inventory 3rd Party Connections
Restrict Connections
Standardize Remote Access
Harden Remote Access Tools

Cybercriminal

Phishing (Malware/Cred Theft)

Employee

Single Sign-on with MFA
Secure Email Gateway Service
Automate Email Pullback
Sufficiently Trained Workforce
Endpoint Detection & Response

TV Station

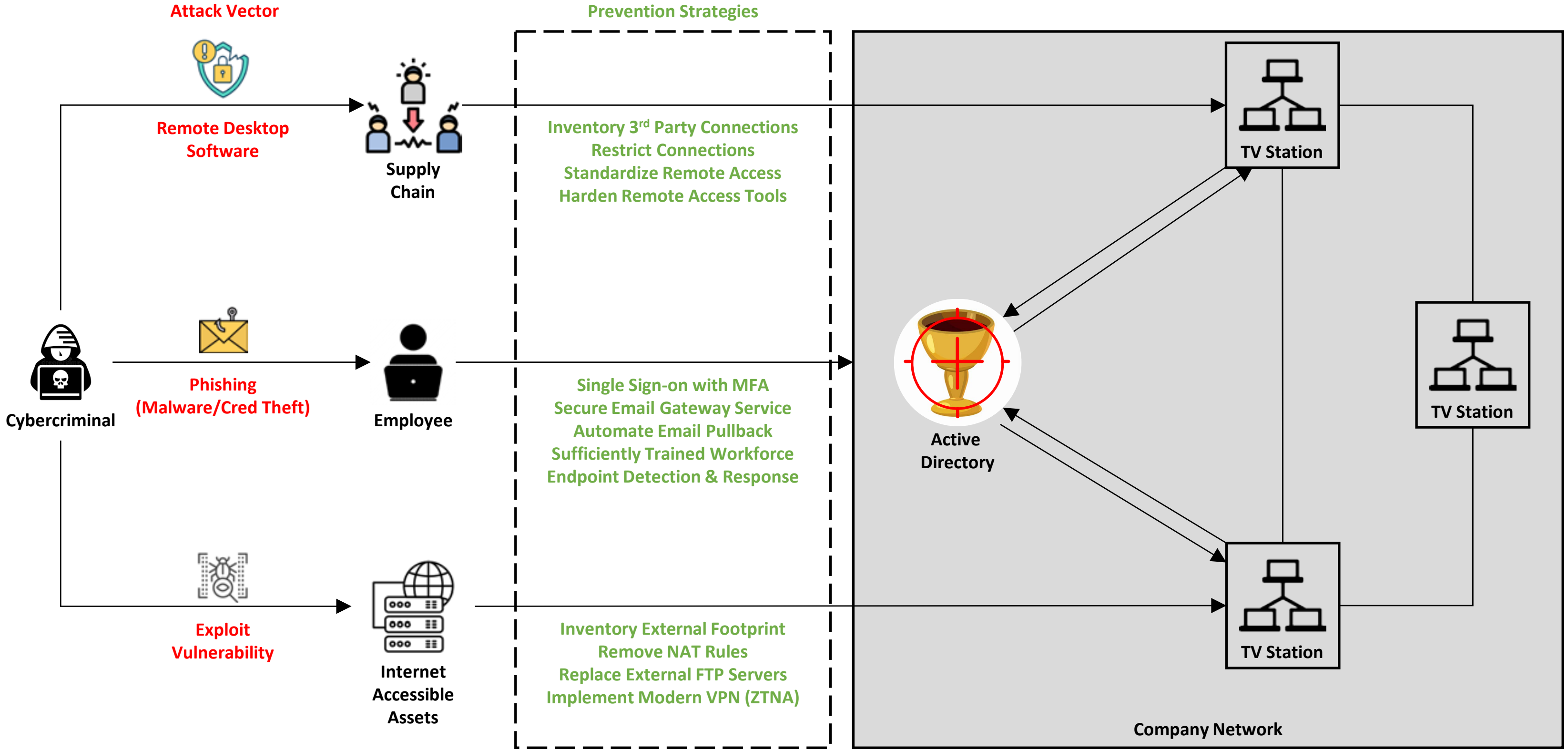
Active Directory

TV Station

TV Station

Company Network

PREVENTION STRATEGIES

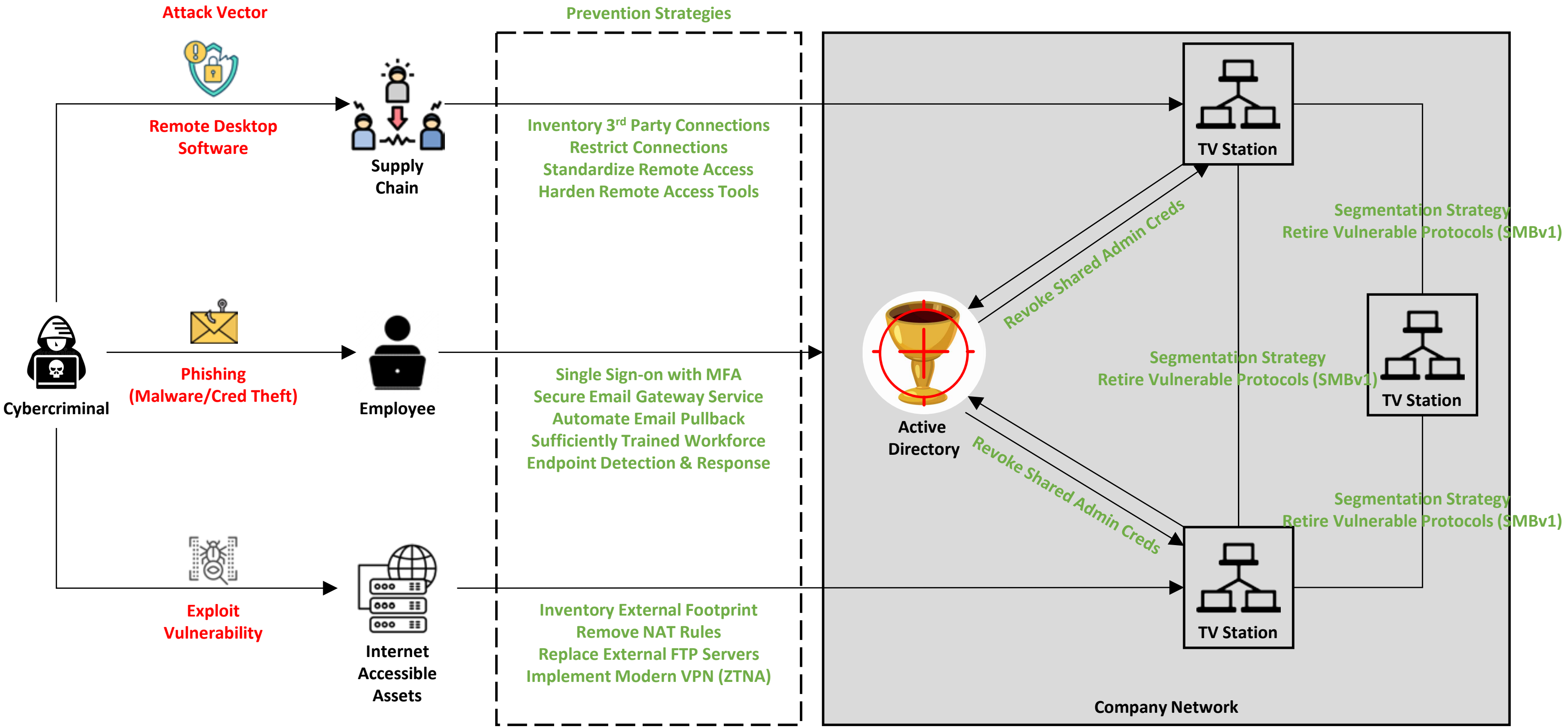


Inventory 3rd Party Connections
Restrict Connections
Standardize Remote Access
Harden Remote Access Tools

Single Sign-on with MFA
Secure Email Gateway Service
Automate Email Pullback
Sufficiently Trained Workforce
Endpoint Detection & Response

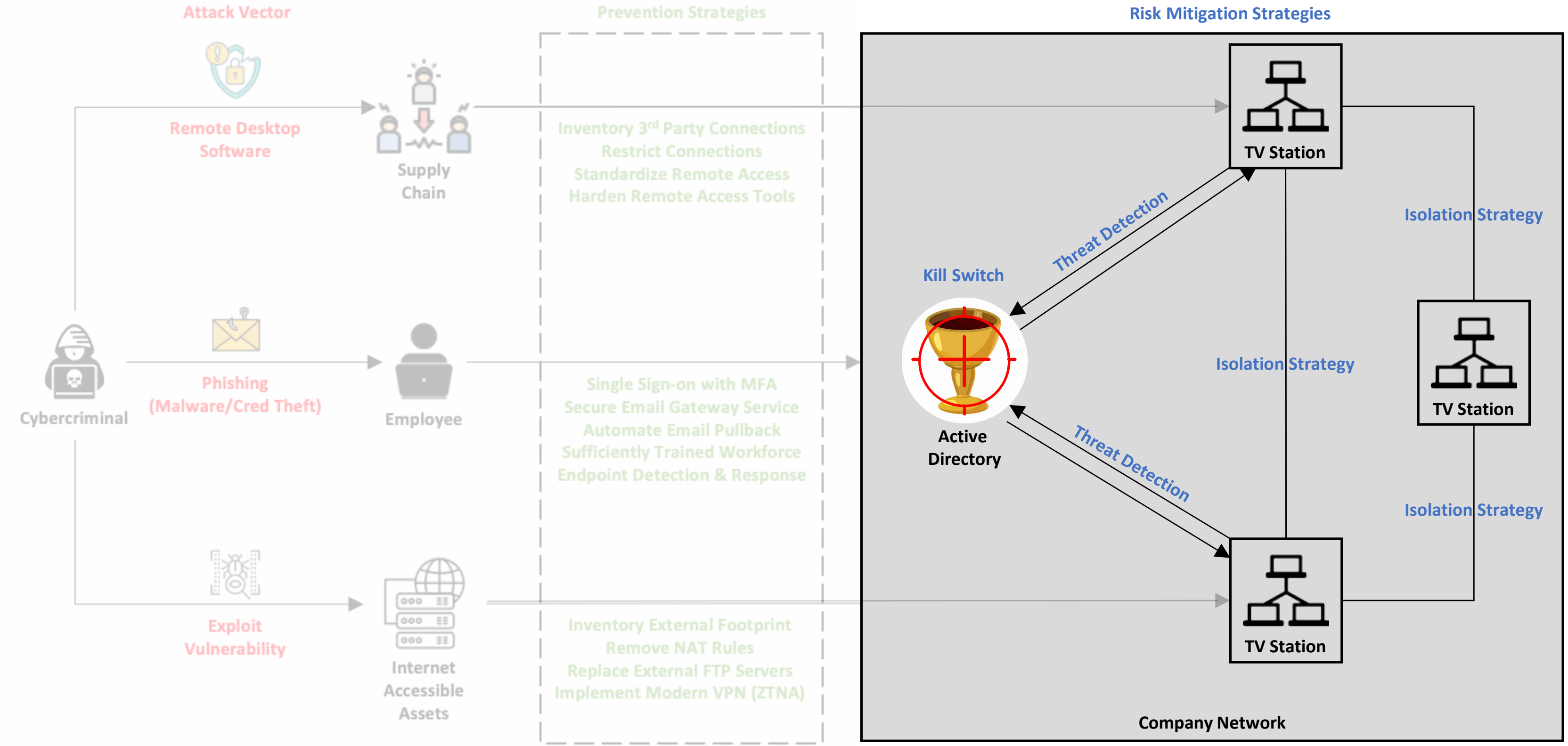
Inventory External Footprint
Remove NAT Rules
Replace External FTP Servers
Implement Modern VPN (ZTNA)

PREVENTION STRATEGIES


Attack Vector
Prevention Strategies
Remote Desktop Software
Supply Chain
Inventory 3rd Party Connections
Restrict Connections
Standardize Remote Access
Harden Remote Access Tools
TV Station
Segmentation Strategy
Retire Vulnerable Protocols (SMBv1)
Revoke Shared Admin Creds
Cybercriminal
Phishing (Malware/Cred Theft)
Employee
Single Sign-on with MFA
Secure Email Gateway Service
Automate Email Pullback
Sufficiently Trained Workforce
Endpoint Detection & Response
Active Directory
Segmentation Strategy
Retire Vulnerable Protocols (SMBv1)
TV Station
Revoke Shared Admin Creds
Segmentation Strategy
Retire Vulnerable Protocols (SMBv1)
Exploit Vulnerability
Internet Accessible Assets
Inventory External Footprint
Remove NAT Rules
Replace External FTP Servers
Implement Modern VPN (ZTNA)
TV Station
Company Network

BANG HAPPENS!!!

REACTION AND RESPONSE STRATEGIES



TAKEAWAYS

Left of Bang

- Know your points of weakness
  - Internet facing asset discovery & vulnerability identification
  - Identify remote access tools and lock down (editing, third parties, etc.)
  - Understand connectivity points between third parties
  - Execute a detailed risk assessment against active directory
- Impede attack progression
  - Implement advanced secure email gateway
  - Automate phishing email pullback
  - Deploy MFA on all internet facing assets (extra credit: SSO + MFA)
  - Utilize endpoint detect response software everywhere possible
- Shrink your attack surface
  - Remove assets in DMZ with SASE solutions or cloud applications
  - Get rid of internet facing FTP servers
- Reduce blast radius
  - Isolate stations from each other (segment network)
  - Isolate on-air chain from regular users (micro-segmentation)
- Build resiliency
  - Perform regular, frequent backups & isolate from network
  - Test backups regularly & use immutable storage where possible
- Update incident response plan
  - Establish a ransomware specific playbook for response
  - Develop procedures to isolate your environment rapidly
  - Test the technical response plan
- Assemble your team in advance
  - External counsel, crisis communication, forensic investigations
- Block unnecessary outbound internet traffic
  - Minimize what is permitted to connect outbound (especially SMBv1!)

Right of Bang

- Execute the plan swiftly
  - Time is not on your side during ransomware incident
  - Act decisively, especially if active directory is compromised
- Leverage endpoint detection response tools
  - Use features in EDR to immediately contain compromised endpoints
- Monitor active directory for suspicious activity
  - Build alerting capabilities for anomalous behavior
- Forensic investigation should guide your actions
  - Ensure the threat actor is eradicated before any restore actions occur
- Have a model for restoration
  - Only introduce systems after they are considered clean

OTHER USEFUL REFERENCE MATERIALS

CISA Ransomware Guide

- Very useful for embedding a playbook into your incident response plan specific to ransomware scenarios
- Includes Ransomware Prevention Best Practices (many of which I covered) and a Ransomware Response Checklist

Incident Response Team

- Besides your internal team, make sure you have the following members on your bench should a full-scale crisis be on your hands
  - External counsel
    - Role: Provide privilege communications, legal expertise for breach notifications, help with crypto payment through broker
    - They should be the first you should call
  - Cyber insurance provider (if you have it)
    - Role: Cover breach related costs
    - Should be notified of any significant incident
  - Computer forensic investigation
    - Role: Investigate systems to identify source of incidents, guide eradication efforts, confirm containment, etc.
    - They should be engaged through your external counsel
  - Crisis communications
    - Role: Assist with external communications and messaging
    - May or may not be engaged depending on scope of incident and internal expertise
  - Law enforcement
    - Role: May be able to assist with ransomware decryption and identify threat actor
    - Consult external counsel before engaging, but local FBI cyber team should be on your list of contacts and DHS