Anatomy of a Ransomware attack and How to Protect Your Company

October 2023

By Julie Baker

Chief Information Security Officer

1st Franklin Financial Corporation

Common Ransomware Attack Pattern

#1. Attack Against the Human

It Primarily Starts Here

The weakest link

#1 Attack Against the Human

It only takes one user, clicking one malicious link in an email

Phishing emails with links	Malicious email attachments	Malicious websites the user visits
Pop up ads	SMShing	Social Engineering – “Hi, I’m Tim from IT….”

Attack Against the Human

Help the Human!

Brand Monitoring and Phishing Takedown service – monitors malicious sites spoofing 1st Franklin sites and performs takedowns.

Email security – Microsoft provides some good protections, but need a product that has additional intelligence capabilities, BEC protections, proactive and automated response. Defenders can't react quickly enough

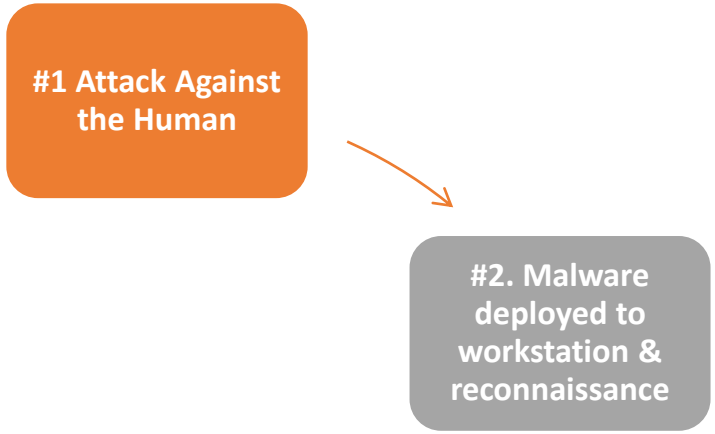
User Training and more user training and more user training – a good interactive and engaging security awareness training program is essential

Frequent phishing simulation tests with remedial phishing training for all users who do not pass & manager notification for continued non-passage

Internet category blocking – block access to suspicious and potentially malicious Internet content.

For small companies, make sure you train your employees and yourself on how to recognize a phish. There are some free resources out there to help like getgophish.com, https://www.proofpoint.com/us/learn-more/security-awareness-phishing-kit. Might be worth it to invest in some training and can be done without breaking the bank.

Common Ransomware Attack Pattern



#2 Malware deployed to workstation & reconnaissance

- Deployment of the payload – user downloads a malicious file from the Internet, opens a poisoned attachment
- Bad actors use what has been downloaded to gain privileged access to the workstation or server. These can be:
  - Reconnaissance tools to find vulnerabilities and understand your network
  - Malware – to scrape passwords from memory and exploit the vulnerabilities on the machine

The bad actor can remain resident, doing reconnaissance for weeks or months. Or this can take minutes or hours if the attack is automated.

Malware deployed to workstation & reconnaissance

Endpoint Protections

Endpoint Detection & Response (EDR, XDR) - Monitoring and remediation agent on all workstations and servers – alerting on suspicious activity and taking automated remedial action

Currency & Patch Management – make sure all endpoints are patched on an ongoing basis. Make sure the operating systems and applications are kept up to date. It is never one and done.

Intelligence feeds – machine readable intelligence to feed the EDR/XRD with indicators of compromise from other companies for proactive response

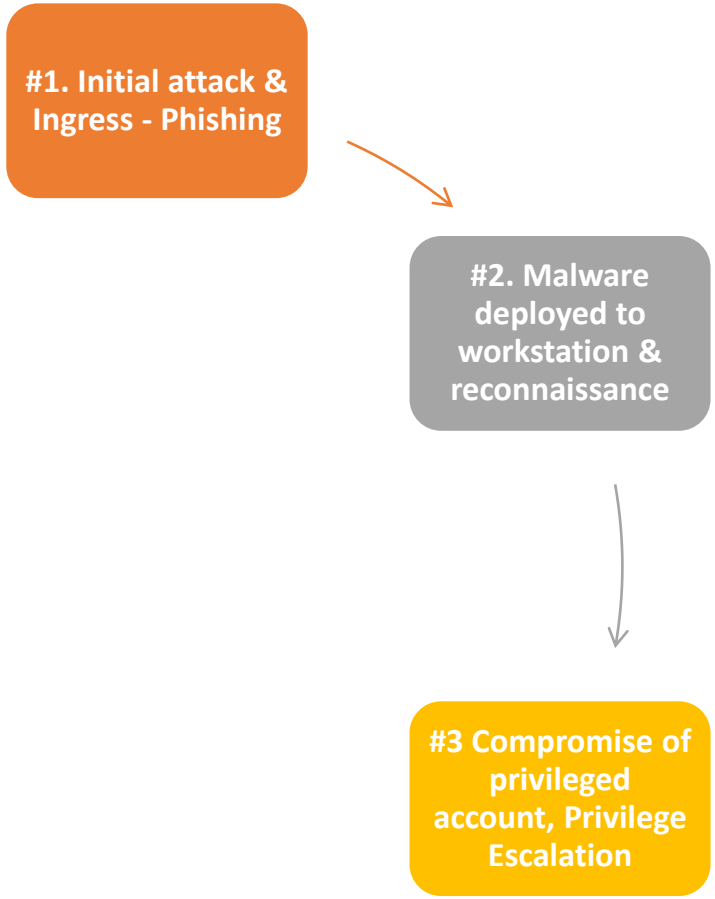
Secure browsing, blocking of unapproved software (applocker) and USB management – these are settings that can be made through software that is used to centrally manage endpoints – SCCM, Intune

Insider risk monitoring and User Entity Behavioral analytics – to look for anomalous user behavior

Monitoring, alerting and response – SIEM & SOC – goal is to limit the blast radius, find them quickly.

For small companies, getting reputable anti-virus/anti-malware deployed on all your workstations is critical. Many also have safe browsing and other capabilities you can turn on to better protect yourselves

Common Ransomware Attack Pattern



#3 Compromise of privileged account, Privilege Escalation

- With the tools deployed in the previous step, the bad actors will find a vulnerability and exploit it to escalate their privileges. Goal is to become a “God” account – on the workstation, in your domain, in your cloud environment.
- Once they have this, they can do anything they want to the workstations and servers in your environment and gain access to whatever data they want.

Make sure your do what you have to do to protect your privileged “God” accounts.

Compromise of privileged account, Privilege Escalation

Privileged Accounts

Hardware tokens for domain admins – strongest MFA protection for the most privileged accounts

MFA and conditional access rules for all privileged (and all user) access – mobile app or hard token only – to validate you are who you say you are.

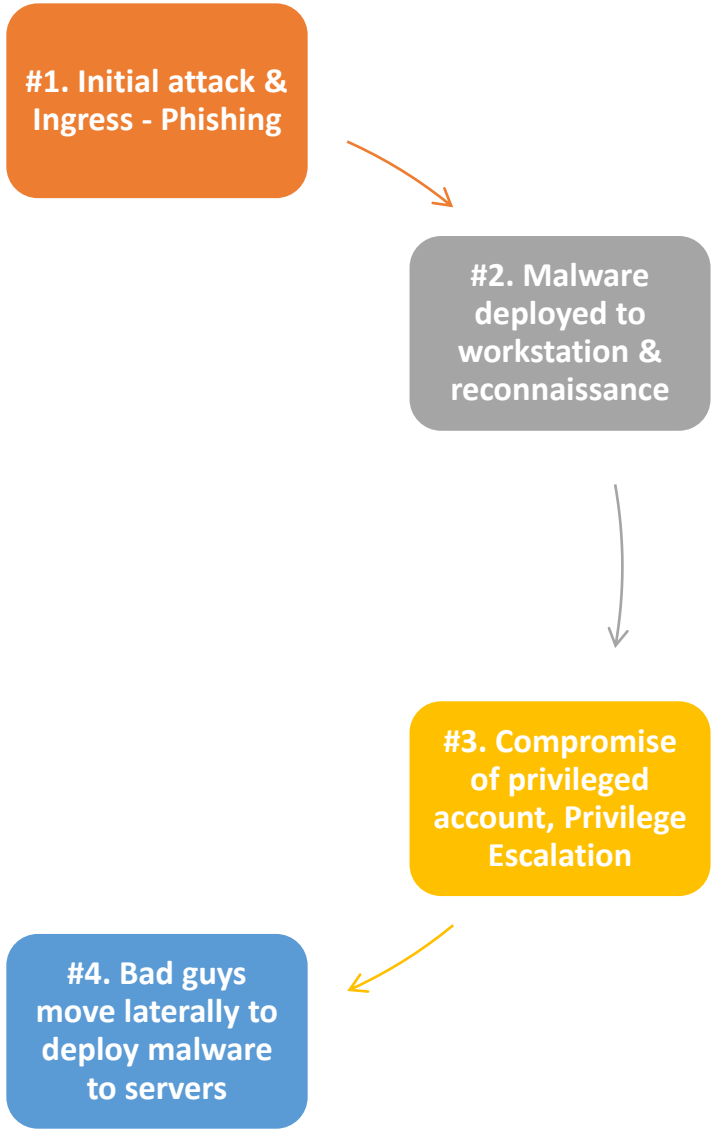
Use of a Privileged Access Management (PAM) tool for securing all privileged user accounts and preventing unauthorized use.

All machine/service accounts managed via vault technology and/or certificates to prevent unauthorized use.

Additional monitoring and logging on all privileged accounts with various 3rd party tools

Small companies should also turn on MFA for their Microsoft accounts, bank accounts and any other business accounts/personal. Make sure to use long, complex passwords/passphrases, and never log in as administrator accounts for normal day to day work.

Common Ransomware Attack Pattern



#4. Bad guys move laterally to deploy malware to servers

- Now that the bad actors have privileged account access, they will start moving beyond the workstation they have compromised.
- They are gathering information about your network and cloud environment.
- They are looking for your data so they will look at server names and other network data to try to figure out where it is.

Bad guys move laterally to deploy malware to servers

Lateral Movement (visibility)

Network segmentation to prevent threat actors from moving easily across the company network – no more one big flat network.

VPN segmentation – VPNs are a common attack vector – limit what your people can get to by role.

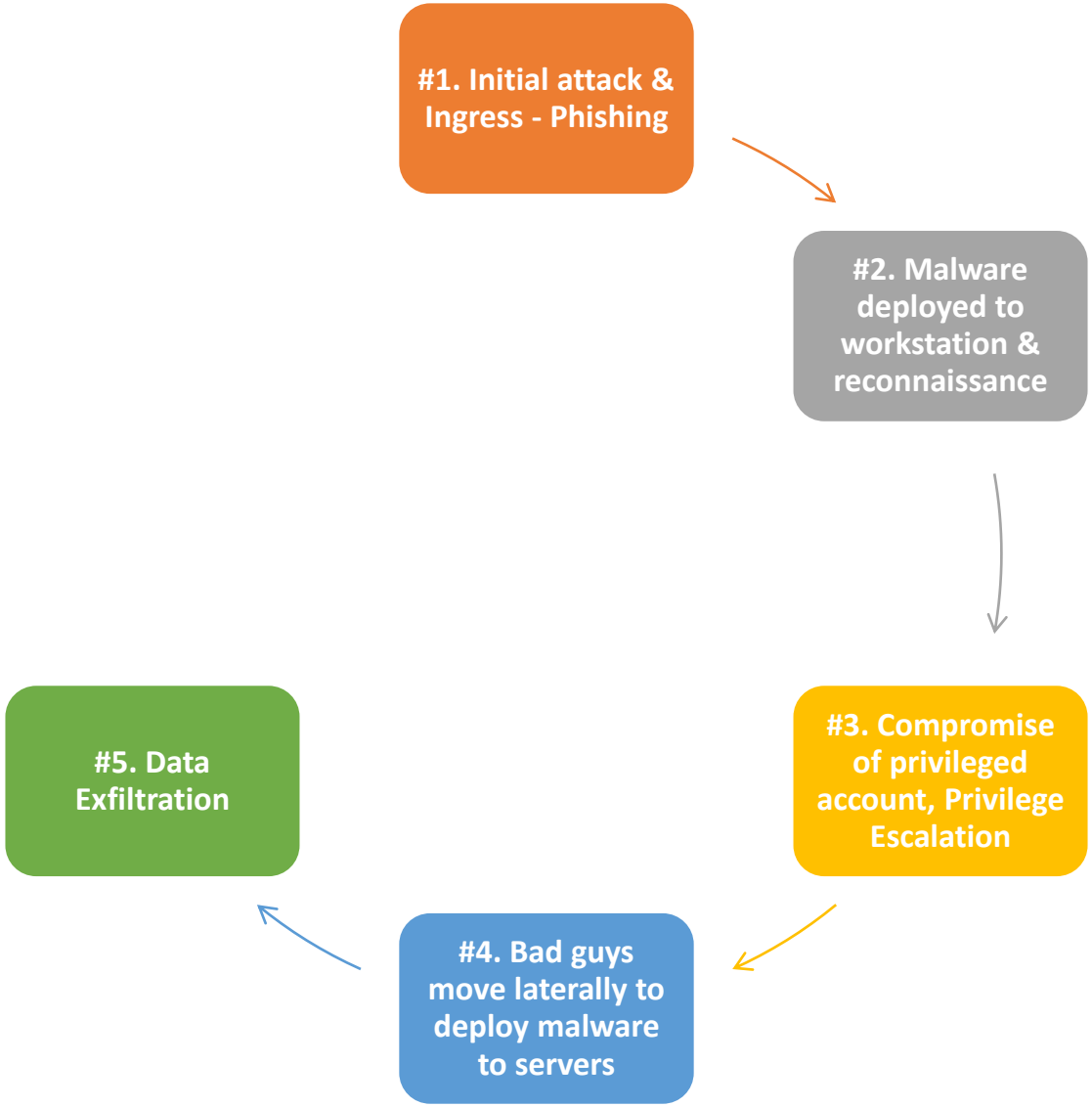
IDS-IPS/firewall logging and monitoring via security incident and event monitoring vendor.

Zero Trust - the idea is there is no more perimeter – you trust no one. Everything has to authenticate and be subject to security monitoring and controls. There are vendors that support this model.

Ensure the firewall rules are not configured permissively, but are tightly managed, especially with regard to 3rd party access.

For small companies, it would be worth it to hire an IT expert to come and configure your Internet router and local workstation firewalls for maximum protection. This person could help with setting up other protections discussed in this presentation as well.

Common Ransomware Attack Pattern



#5. Data Exfiltration

- Once the bad actors find the data they will start to exfiltrate it.
- There are a number of native tools they can use to do this or they will bring their own.
- Often they will encrypt the data stream to avoid detection from data loss prevention tools.

The more you can do to minimize the amount of sensitive data on your network, the better

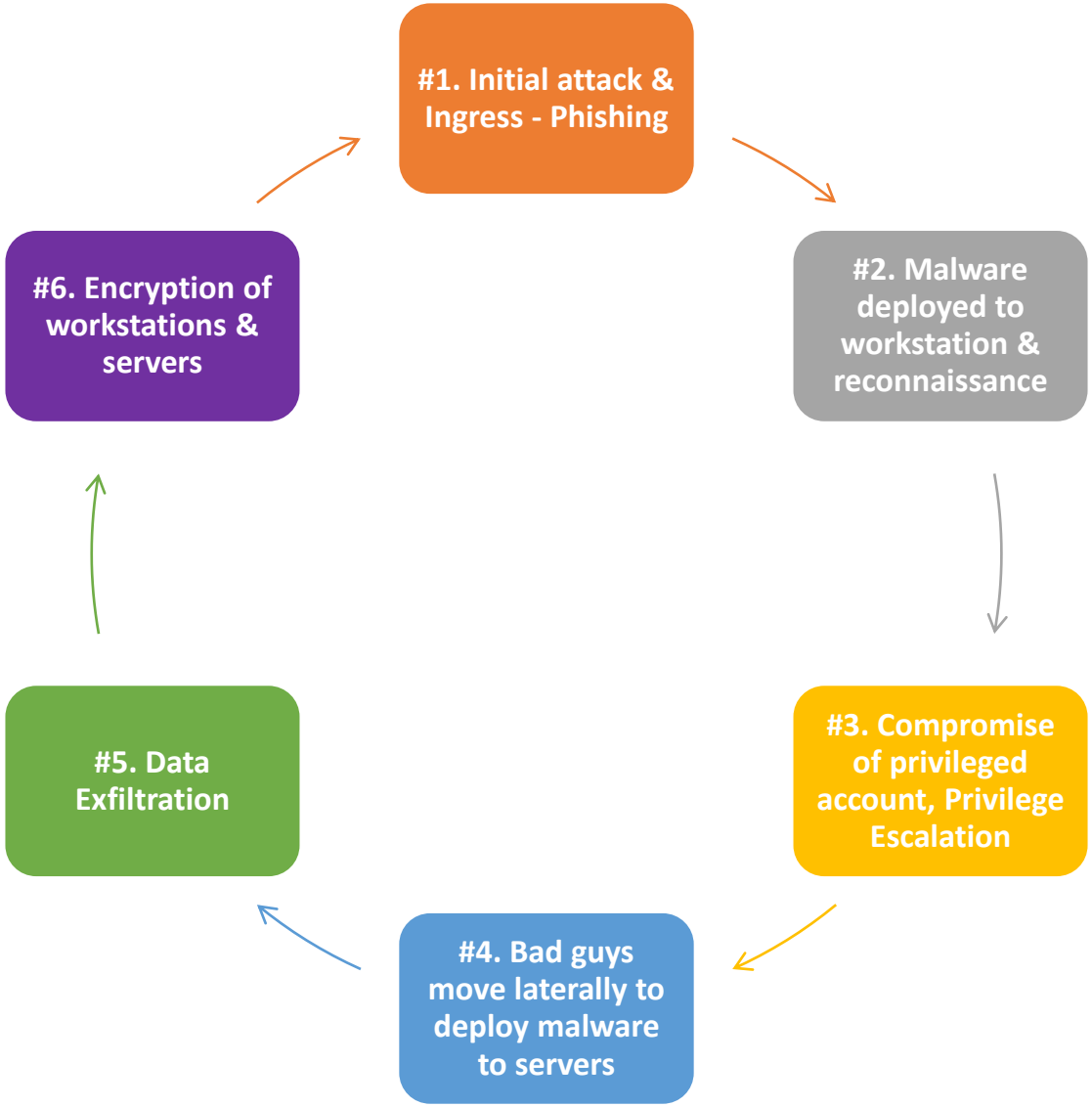
Data Exfiltration

Data Protection

- Data Loss prevention – enable blocking to prevent sending of unencrypted email and endpoint communications
- Data Classification and encryption – auto-label files to identify sensitive data; use encryption and/or masking to protect files.
- Data retention – enforce data retention requirements including archiving and deletion. Minimize the data the bad actors can get to
- Cloud Access Security Broker – monitoring for cloud application communication and data sharing
- Database monitoring and security for monitoring and protecting databases
- Data transfer protections – ensure all users are trained on tools that allow for secure sharing of data.
- SSL Decryption at the firewalls – allows for greater visibility for the IS and IT teams (if technically feasible)
- Secrets and key management - protect the passwords and keys used to secure 1FFC data and systems.

Small companies can encrypt the sensitive data – gpgforwin is free. Make sure you know where the data is, keep it for as short a time as possible, ensure all data transfers are encrypted and properly authenticated (preferably with MFA). Make sure your vendors are protecting the sensitive data also!

Common Ransomware Attack Pattern



#6. Encryption of workstations & servers

- If this is happening, then they have your data and want to inflict the most damage they can.
- You will need to make sure you have a solid disaster recovery and business continuity plan in place.
- You will also need to make sure you have a solid incident response process in place, to do your best to not end up here.
- The fact is a determined attacker will get in – the goal is to find them as quickly as possible and limit the blast radius.

Your Disaster Recovery plan & Incident Response Process are your friends

Encryption of Workstations & Servers

Disaster Recovery & Incident Response

- Offline/Airgapped backups – tested semi-annually
- Data archive solution – to support data retention requirements
- Develop and implement strategy for cloud DR sites
- Create Departmental & Company Business Impact Analysis & Business continuity plans
- Perform a full cloud and/or data center disaster recovery test annually
- Incident response process testing including tabletop exercises

Small companies should make use of cloud applications that have redundancy built in like Sharepoint or Google Docs. But these can also be encrypted. So make sure to create an offline backup – large, external hard drives are cheap and can be used to backup data on a regular basis

Common Ransomware Attack Pattern