Breaking Down Ransomware

Ransomware has plagued the technology world with its evilness, only bringing harm and is usually undetected until it is too late. Let's take a look at what makes ransomware so successful and break down the anatomy to understand what our enemy is working with.

Anatomy of a Ransomware Attack

While there are many different types of ransomware attacks (we will cover these later), each attack's premise is usually the same. Each attack is curated to its intended target. Lets review at a high level, what steps are involved in most ransomware attacks so we can become better familiar with the outcomes. We will also provide known techniques that have been observed for each step as collected by the MITRE ATT&CK framework.

Step 1

The Target (Initial access)

While there are many different types of ransomware attacks (we will cover these later), each attack's premise is usually the same. Each attack is curated to its intended target. Lets review at a high level, what steps are involved in most ransomware attacks so we can become better familiar with the outcomes. We will also provide known techniques that have been observed for each step as collected by the MITRE ATT&CK framework.

Step 2

Spread and Conquer (Credential Theft)

Once the attack can get a foothold within an environment, the next step is to spread to as many systems as possible. More devices or data on the network will incentivize the owner to pay the ransom further. By further compromising accounts/systems, the malicious accounts ransomware can propagate throughout an entire network.

Brute force, compromising password stores, force authentication, input capturing, man-in-the-middle, network sniffing OS credential dumping and stealing web session cookies are only some of the ways an attacker can compromise accounts across your network infrastructure.

Step 3

Finding the golden key (Persistence)

Now that the ransomware has the right persistence, it's time to search for an account with privileges. Data consisting of company secrets, proprietary source code, or even customer files would be deemed essential and in play for most ransomware. Attackers will perform tasks like creating a new account, compromising browser extensions or even injecting themselves in the boot initialization scripts to ensure they have a way in and out. These are just to name a few ways that gain persistence on a device that may go unnoticed.

Step 4

Stick and Move (Lateral Movements)

By utilizing the admin account obtained in step 3, the actors are now able to traverse throughout the network and continue to identify all the locations of sensitive data. In this step, the ransomware is essentially mapping out its attack plan of what it is going to compromise. The MITRE ATT&CK framework does a great job of listing out all the known techniques for lateral movement seen in the wild today:

- Exploiting remote services
- Spearphishing
- Session hijacking
- USB replication
- Using software deployment tools
- Shared content
- Using alternate authentication methods to bypass security.

Step 5

Spread and Release Payload (Payload)

Lastly, the attackers will release the payload, which usually involves encrypting user data and planting its ransom note in each system or location. Usually by this step, it is too late to prevent any damages from occurring. The following should be expected once an attacker has reached the payload stage:

- Account removals
- Data destruction/encryption
- Data manipulation
- Defacement
- Disk wiping
- Denial of service
- Firmware corruption
- Resource hijacking (crypto mining)
- Services disabled
- System shutdown

Types of Ransomware

There are five major types of ransomware that have been found in the wild over the years. Each follows the above sequence of steps, with slight variations depending on the target.

Encrypting Ransomware

As the name suggests, these category of Ransomware typically encrypt the data/ contents and then demand ransom against the release of the decryption keys

Non-Encrypting Ransomware

These types of Ransomware typically lock access to mission critical resources – for example, by changing the passwords – and then demand ransom to release access

Exfiltration Ransomware

Such Ransomware threaten to publish stolen information unless the ransom demands are met

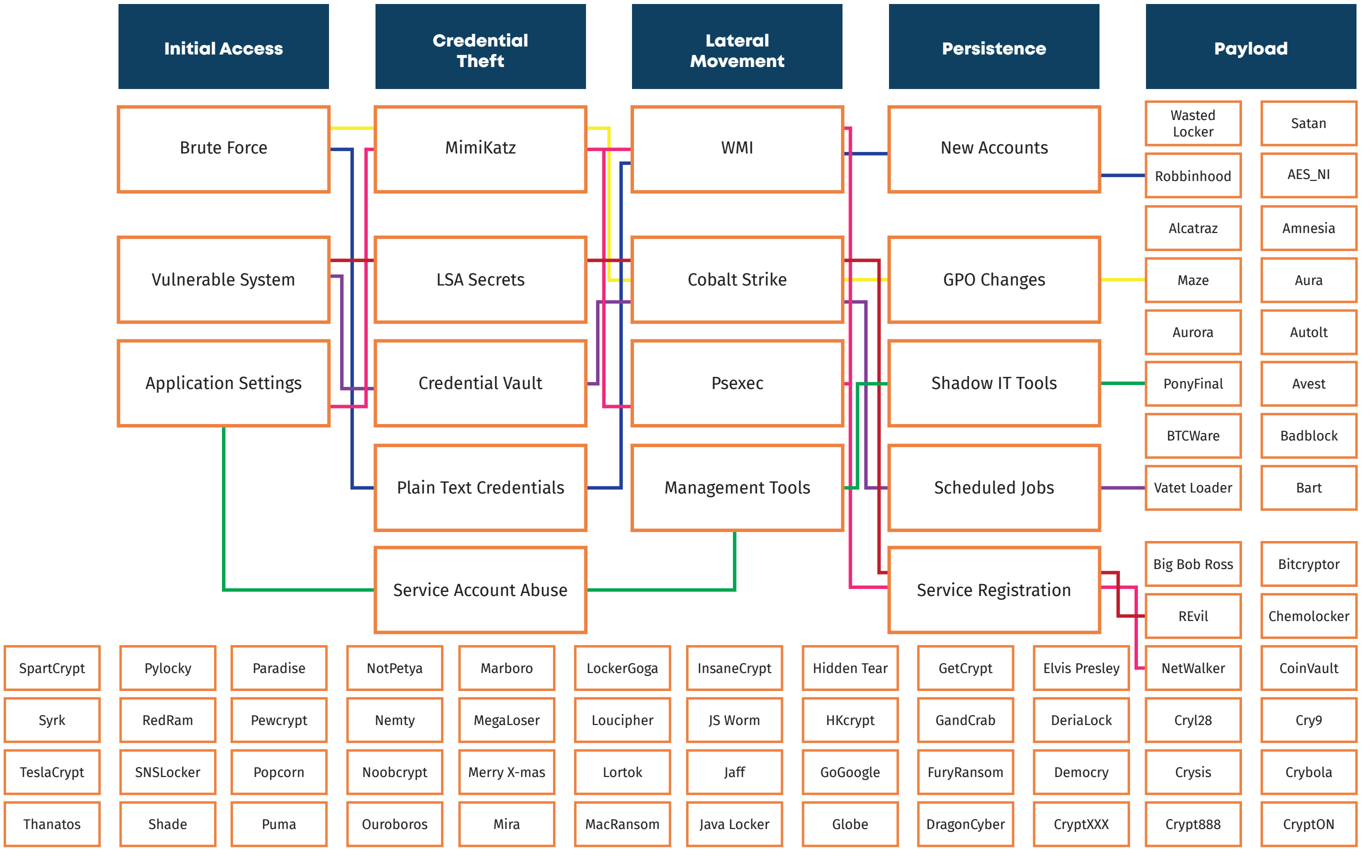
Mobile Ransomware

These types of Ransomware ranges from downloading malicious APK files, stealing icloud credential, or tricking users into given access to devices resources such as camera, microphone, contacts, photos etc.

Known Ransomware

The visual to the right gives you just a taste of only the known attacks. There are perhaps many more in the wide. Note, discovering ransomware doesn't guarantee or confirm a way of retrieving your records once they are lost.

To break this down even further, we have white boarded out a list of known ransomware attacks below. By mapping out only a handle of attacks to their tactics, you can quickly see how creative and unique ransomware is as an attack vector. We have only touched the surface of all the different avenues that a bad actors can take to script and exploit the end-user.



Initial Access

Brute Force

Vulnerable System

Application Settings

Credential Theft

MimiKatz

LSA Secrets

Credential Vault

Plain Text Credentials

Service Account Abuse

Lateral Movement

WMI

Cobalt Strike

Psexec

Management Tools

Persistence

New Accounts

GPO Changes

Shadow IT Tools

Scheduled Jobs

Service Registration

Payload

Wasted Locker

Satan

Robbinhood

AES_NI

Alcatraz

Amnesia

Maze

Aura

Aurora

Autolt

PonyFinal

Avest

BTCWare

Badblock

Vatet Loader

Bart

Big Bob Ross

Bitcryptor

REvil

Chemolocker

SpartCrypt

Pylocky

Paradise

NotPetya

Marboro

LockerGoga

InsaneCrypt

Hidden Tear

GetCrypt

Elvis Presley

NetWalker

CoinVault

Syrk

RedRam

Pewcrypt

Nemty

MegaLoser

Loucipher

JS Worm

HKcrypt

GandCrab

DeriaLock

Cryl28

Cry9

TeslaCrypt

SNSLocker

Popcorn

Noobcrypt

Merry X-mas

Lortok

Jaff

GoGoogle

FuryRansom

Democry

Crysis

Crybola

Thanatos

Shade

Puma

Ouroboros

Mira

MacRansom

Java Locker

Globe

DragonCyber

CryptXXX

Crypt888

CryptON

Credit: Inspiration from Microsoft:
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

AIRGAP

Ransomware Prevention Techniques

When it comes to preventing ransomware, it may seem like a daunting task with no end in sight. To help organize this better, we have put together a list of the top preventions that should be put in play to ensure you get the best bang for the buck. By successfully implementing the following controls, you dramatically reduce the Ransomware's impact on your organization.

Broadly speaking, you can break down the defense in 4 categories as outlined below:

1 Protect the first victim

Following are some of the good practices to follow in order to best protect your endpoints from getting infected in the first place

- Install endpoint detection and remediation solution on all managed devices
- Disable macros in the office documents and prevent unauthorized executables from being downloaded
- Rename VSSadmin to prevent shadow backup copies from being deleted and disable Windows scripting host (WSH) to block .VBS malware
- Remove/restrict admin privileges - malware/ransomware are only as successful as the admin privileges they have to obtain to access sensitive data
- Deploy Zero Trust Isolation to protect unmanaged devices such as mobile phones and IoTs.

2 Prevent lateral propagation

Once inside your network, the Ransomware will propagate for the more devices they control, the bigger the ransom demand. We must be able to prevent lateral movement across managed and unmanage (e.g. IoTs) devices in the network

- Deploy agentless Zero Trust isolation for all devices - By implementing zero-trust isolation/ segmentation across your infrastructure/network you are essentially instructing every device on your network to not trust anything besides what has been approved by administrators. A properly configured zero-trust network will eliminate lateral movement and prevent ransomware from being able to transverse across your assets, thus isolating the threat to a single device

3

Protect business applications and data

The traditional firewall and VPN provide static network level access to your business applications allowing the bad actors access to your business application stacks

- Eliminate network level access to sensitive business applications in favor of multi-protocol proxy-based access. The proxy acts as a layer of defense between network connected devices and the business applications
- Ensure that the proxy supports MFA for all protocols such as Web, SSH, RDP, MySQL etc. We know that the humans can pass MFA but the bad actors cannot and you are able to better protect your business assets
- Filter out the ability to call home - Most ransomware/ malware attacks rely on communication with C&C site aka the ability to call home. By blocking interactions with known C&C Ips/URLs, you hamper attacker's ability to wake up the sleeping cells

4

Protect key business assets such as Active Directory and Windows File Share

Legacy and insecure protocols as well as applications allow bad actors to quickly propagate the payload across the entire organization – this could take as little as 45 seconds giving you no time to intervene

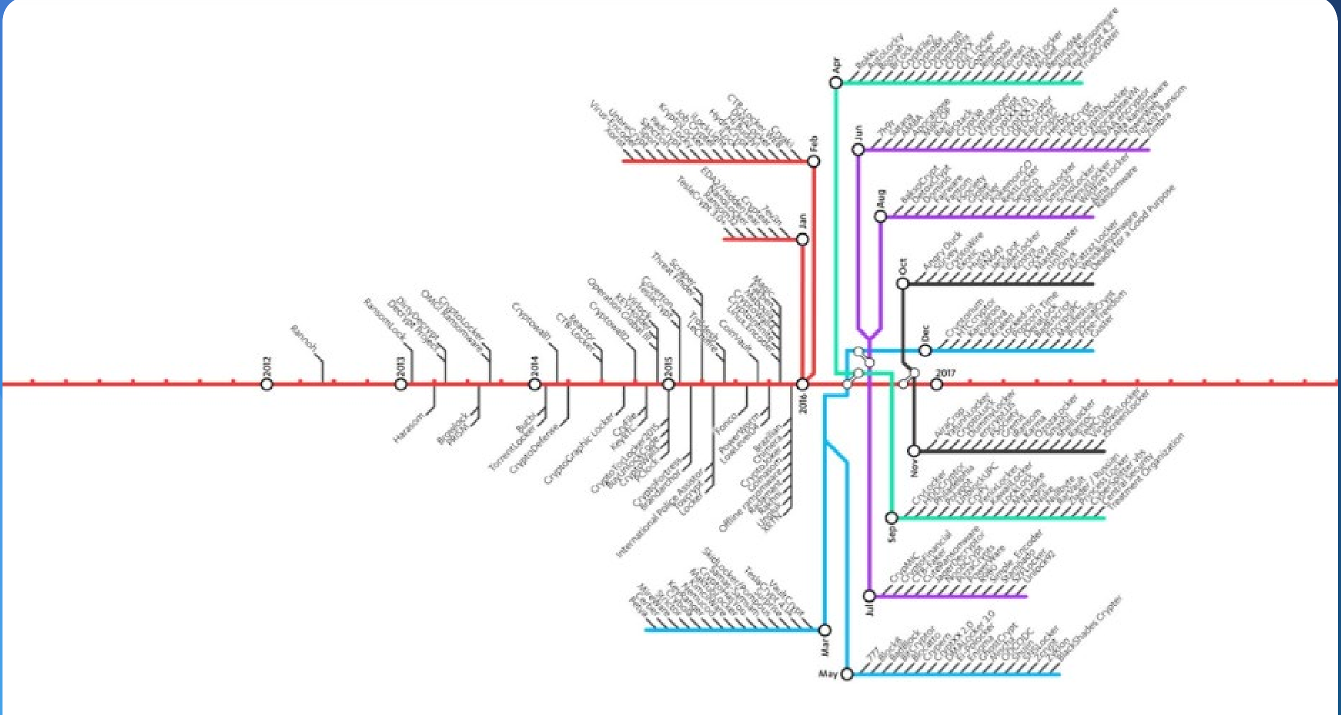
- Eliminate unauthorized access to key business assets, specially the legacy insecure applications/protocols
- Monitor for anomalies (e.g. sudden spike in encrypted traffic) originating from one source and synching to multiple destinations and lock down the system if such an anomaly is detected
- Isolate Backup server from the main domain via additional layer of segmentation between your backup server and the rest of your network to ensure that "if" a ransomware attack does occur, the actors will not have all copies of your data.

Conclusion

Overall, Ransomware will continue to evolve, and new variations will sprout up everywhere. From a security perspective, it is imperative that we put in place the right enterprise architecture that is resilient to Ransomware attacks. As professionals, we need to remain vigilant and continue to hone our detection/prevention methods to ensure that we contain the blast radius to a minimal impact – preferably, no more than one device across the organization.

In closing, take a look at this infographic published by a reputable VPN firm a few years back. In the past ten years, look at all the different types of Ransomware that have evolved. As you can see, this timeline is only growing as we move into the future.

Ransomware discoveries in the past 10 years:



Credit: *https://www.f-secure.com/documents/996508/1030743/cyber-security-report-2017*

Useful Resources:

- https://www.nomoreransom.org/en/decryption-tools.html#SpartCrypt
- https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
- https://www.reddit.com/r/sysadmin/comments/46361k/list_of_ransomware_extensions_and_known_ransom/
- https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml
- https://attack.mitre.org/