Countdown to Ransomware: Analysis of Ransomware Attack Timelines

June 1, 2022

This research was made possible through the data collection efforts of Maleesha Perera, Joffrin Alexander, and Alana Quinones Garcia.

Key Highlights

The average duration of an enterprise ransomware attack reduced 94.34% between 2019 and 2021:

- 2019: 2+ months — The TrickBot (initial access) to Ryuk (deployment) attack path resulted in a 90% increase in ransomware attacks investigated by X-Force Incident Response (IR) in 2019.
- 2020: 9.5 days — Increased initial access broker economy and RaaS industry built upon a repeatable ransomware attack lifecycle established in 2019. Efficiencies adopted such as the ZeroLogon vulnerability to obtain privileged access to Active Directory and CobaltStrike as the C2 framework.
- 2021: 3.85 days — Large scale malspam campaigns such as with BazarLoader and IcedID and increased speed to transition access to ransomware affiliates like Conti.

Overview

IBM X-Force analyzed the evidence from multiple ransomware attack investigations that occurred between 2019 and 2021. In each investigation, access to the victim network was obtained through an initial access broker(initial access brokers are cybercriminals who specialize in breaching companies and then selling the access to ransomware attackers). The emphasis of the research was to better understand the duration of the activities during the various stages of a ransomware attack.

The findings of this research revealed the average duration of an enterprise ransomware attack (time between initial access and ransomware deployment) reduced 94.34% between 2019 and 2021. This is a substantial reduction and while ransomware attack lifecycle time decreased significantly, the research did not reveal substantial changes in the tools, techniques and procedures used by threat actors.

Additionally, X-Force analyzed victim organizations' ability to prevent, detect, and respond to ransomware attacks prior to the deployment of the ransomware and found that ransomware attacks have continually been successful against organizations who have not implemented effective measures to combat the threat of ransomware.

Instead, the evidence revealed the time in transferring access from the access broker to an interactive session to carry out the ransomware attack has decreased significantly, and ransomware operators have become more efficient in gaining privileged access to Active Directory and deploying the ransomware. Understanding the speed and efficiency of ransomware attacks enables organizations to develop a detection and response strategy that is specifically designed to address the ransomware threat.

Initial Access Broker Ransomware Relationship

Initial Access Brokers (IABs) are criminal groups that obtain access or credentials to organizations and then sell that access to other cybercriminals for profit. IABs can obtain various levels of access in a victim network, ranging from credentials to remote services such as virtual private network (VPN), remote desktop protocol (RDP), web shells, and use malware such as TrickBot, Dridex, Emotet, or Buer Loader to establish foothold in a victim network.

In 2019, a relationship between Emotet, TrickBot, and Ryuk ransomware was discovered, where the Ryuk ransomware operators were granted access to an organization through a TrickBot infection. The TrickBot to Ryuk attack path resulted in a 90% increase in ransomware attacks investigated by X-Force Incident Response (IR) in 2019. As the Ransomware as a Service (RaaS) model increased in popularity through 2020, the relationship between other first-stage malware and ransomware attacks were established such as, Dridex malware to BitPaymer ransomware or Gootkit malware to REvil ransomware.

Throughout 2021, the ransomware affiliate Conti exploded in popularity and have been associated with obtaining access through Emotet and IcedIDinfections.

How Ransomware Attacks Happen

In November 2021, X-Force released research detailing how most ransomware attacks occur in a predictable five-stage pattern: Initial Access, Post-Exploitation Foothold, Reconnaissance/Credential Harvesting/Lateral Movement, Data Collection and Exfiltration, and Ransomware Deployment.

Understanding the Adversary: How Ransomware Attacks Happen

While no two ransomware incidents are identical, by analyzing the evidence across all ransomware-related investigations where initial access was obtained via an IAB, X-Force identified four core objectives that enabled the ransomware operators to advance through the 5 stages of a ransomware attack.

1. Establish interactive access
2. Move laterally
3. Obtain privileged access to Active Directory
4. Deploy ransomware at scale

While data theft does occur in most ransomware attacks, evidence of data theft and the duration of data theft activities are limited in many investigations. X-Force was unable to draw any concrete conclusions on the time ransomware operators spent on this stage of the attack.

Download the Definitive Guide to Ransomware

Ransomware Attack Timelines

To learn more about the timeframes involved with a successful ransomware attack year over year, X-Force researchers mapped evidence recovered during X-Force incident response engagements to points in time when the Initial Access Broker first obtained a foothold within the target network as well as when the adversary completed each of the four core objectives of the ransomware attack.

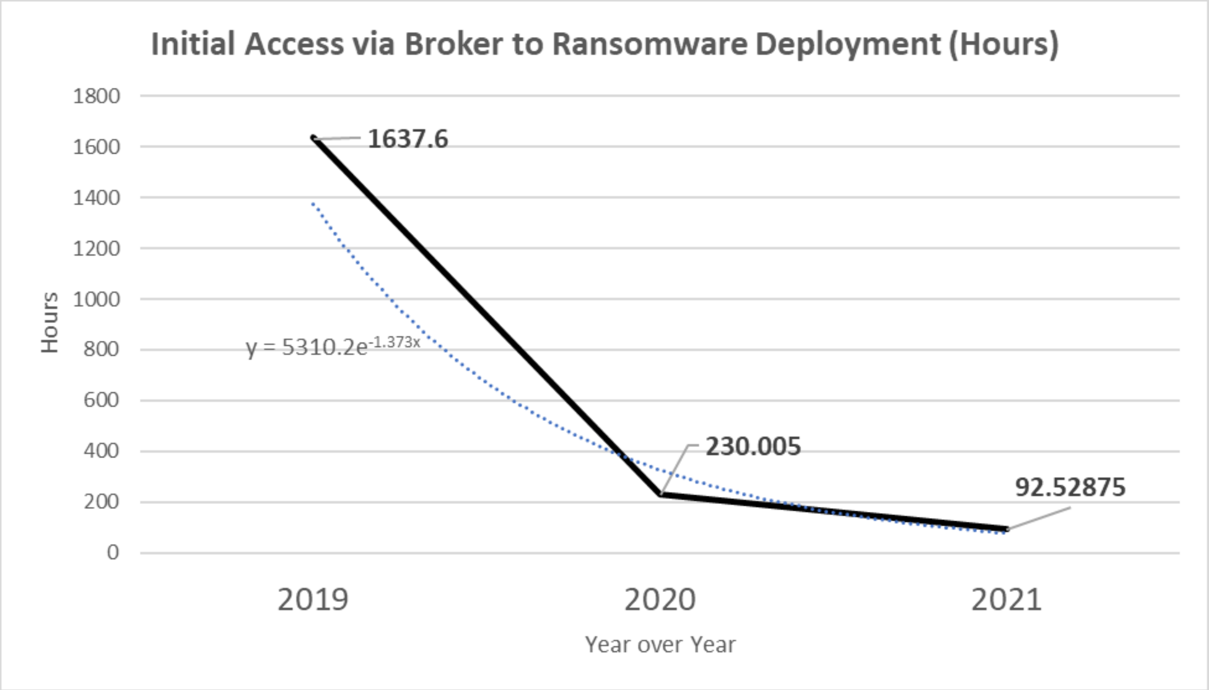

Figure 1: Trendline detailing the reduction in time from initial access to ransomware between 2019 and 2021

In 2019, the average ransomware attack took 1,600 hours or over two months from initial access to ransomware deployment. From this data, X-Force observed the longest attack timeline to be nearly eight months or 5,000 hours. The evidence revealed the longer attack timelines were primarily due to the criminal group TrickBot gaining access to and persisting in environments for the significant duration before passing access to a ransomware operator. Once that access was transferred, ransomware operators were able to deploy Ryuk ransomware and complete the attack on an average of 26.22 days (624 hours).

In 2020, there was a dramatic increase in RaaS activity resulting in ransomware engagements making up 23% (an increase of 20% from 2019) of all incidents responded to by X-Force. From these engagements, Sodinikibi/REvil prevailed to be the most common ransomware variant involved. X-Force analysis of the 2020 incidents revealed, evidence of initial access was obtained through various initial access malware including IcedID, Gootkit, Valak, TrickBot, QBot, and Dridex indicating more RaaS affiliates opting to purchase initial access rather than obtaining independently.

In addition to an increase in the number of ransomware attacks, the speed and efficiency of ransomware attacks increased significantly between 2019 and 2020. In 2020, the average ransomware attack took 9.5 days — a stark 85.96% reduction from 2019. X-Force uncovered significant reductions in the time it took to achieve each of the four core objectives enabling the ransomware operators to advance through the stages of a ransomware attack quicker. One factor that increased both speed and efficiency of ransomware attacks in 2020 was the rapid adoption of the ZeroLogon vulnerability (CVE-2020-1472) to obtain privileged access to Active Directory and CobaltStrike as the C2 framework.

Increased speed and efficiency trends in ransomware attacks continued throughout 2021, and the average time to execute an enterprise ransomware attack was reduced to just 3.85 days and X-Force observed significant reductions in both how quickly access was transferred from the broker to the ransomware operator, and how rapidly the ransomware operator was able to obtain privileged access to Active Directory. Analysis of the ransomware incident evidence indicates that the reduction in time from broker to ransomware operator is likely due to large-scale BazarLoader and IcedID infection campaigns and broker relationships with the Conti ransomware.

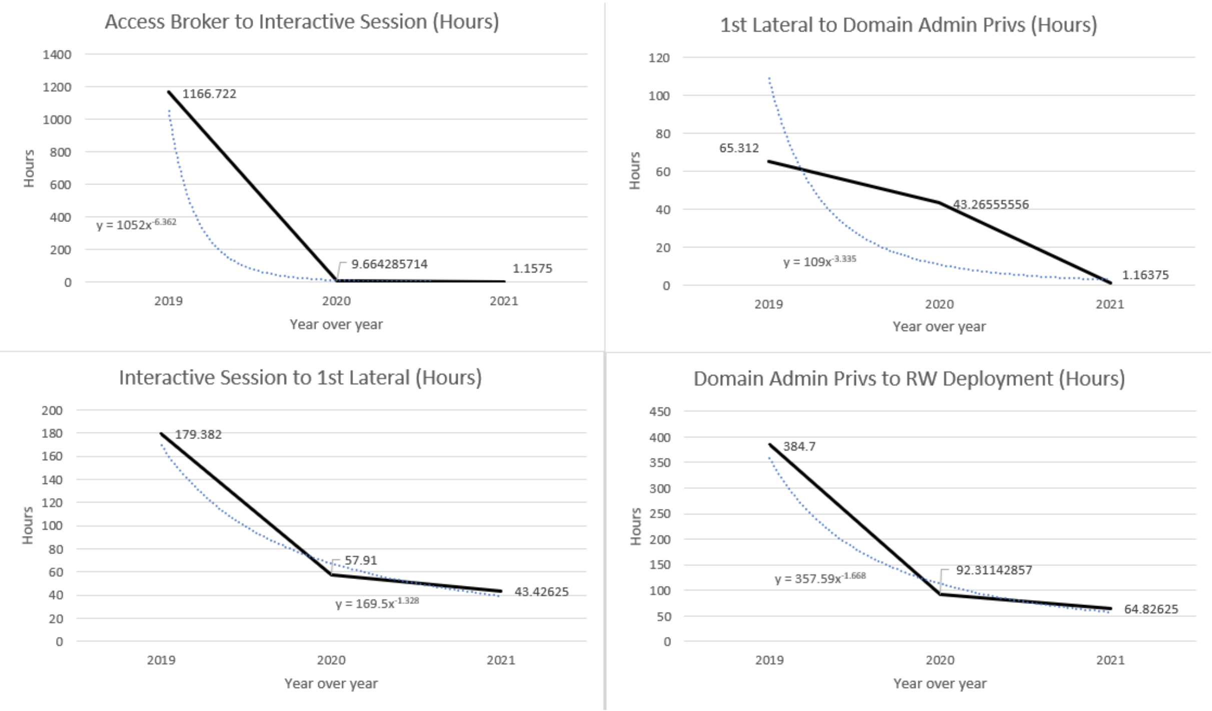

Figure 2: Trendlines detailing the reduction in time to complete each of the four core objectives between 2019 and 2021

Tools Techniques and Procedures

While analyzing the attack timelines and durations to complete objectives, X-Force conducted further analysis on the tools, techniques, and procedures (TTPs) of the ransomware operators to determine if any significant advancements occurred to reduce the time to complete the attack lifecycle.

In 2019, the majority of ransomware investigations were associated with an initial TrickBot infection resulting in a Ryuk ransomware attack. In these attacks, Empire was the most frequent tool leveraged for interactive access (37% of all interactive session tools observed).

Through analysis of 2019 lateral movement and ransomware deployment techniques leveraged by ransomware operators, X-Force discovered a heavy reliance on RDP, server message block (SMB) and remote procedure calls (RPCs) communications between workstations and servers in an Active Directory environment where access to Domain Admin (DA) credentials granted the operator privileged access to all systems within the domain.

Ransomware operators relied heavily on Mimikatz to obtain privileged access to the Active Directory. Mimikatz accounted for 72% of credential harvesting activities.

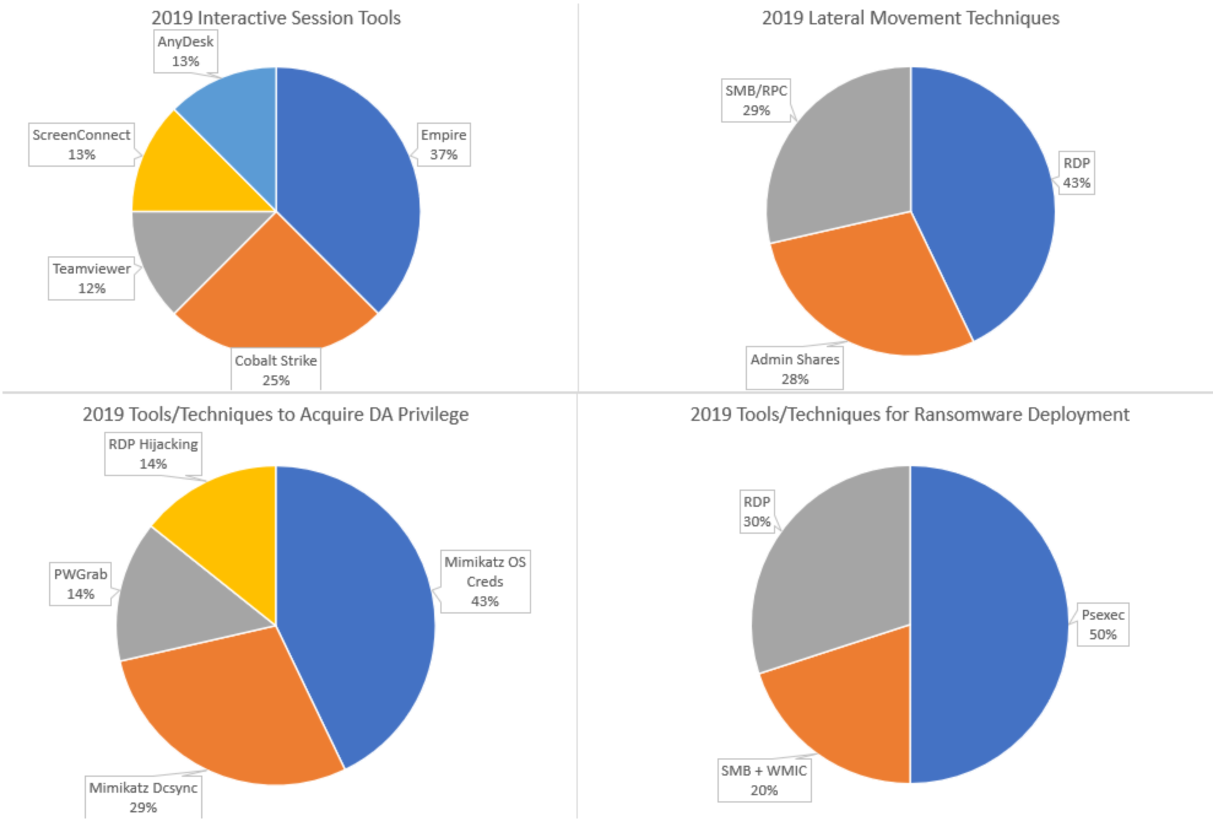

Figure 3: 2019 top tools and techniques to achieve core objectives in ransomware attacks

In 2020, the number of tools leveraged for interactive access increased and CobaltStrike replaced Empire as the most popular interactive session tool. However, reliance on RDP, SMB/RPC, and default DA domain-wide permissions remained vital for the ransomware operators to move laterally and deploy the ransomware.

Ransomware operators were aided in obtaining privileged access to Active Directory with the release of the ZeroLogon exploit, which was rapidly adopted by ransomware operators in Q4 of 2020. However, Mimikatz still played a significant role across ransomware attacks in 2020 accounting for 53% of all credential harvesting activities.

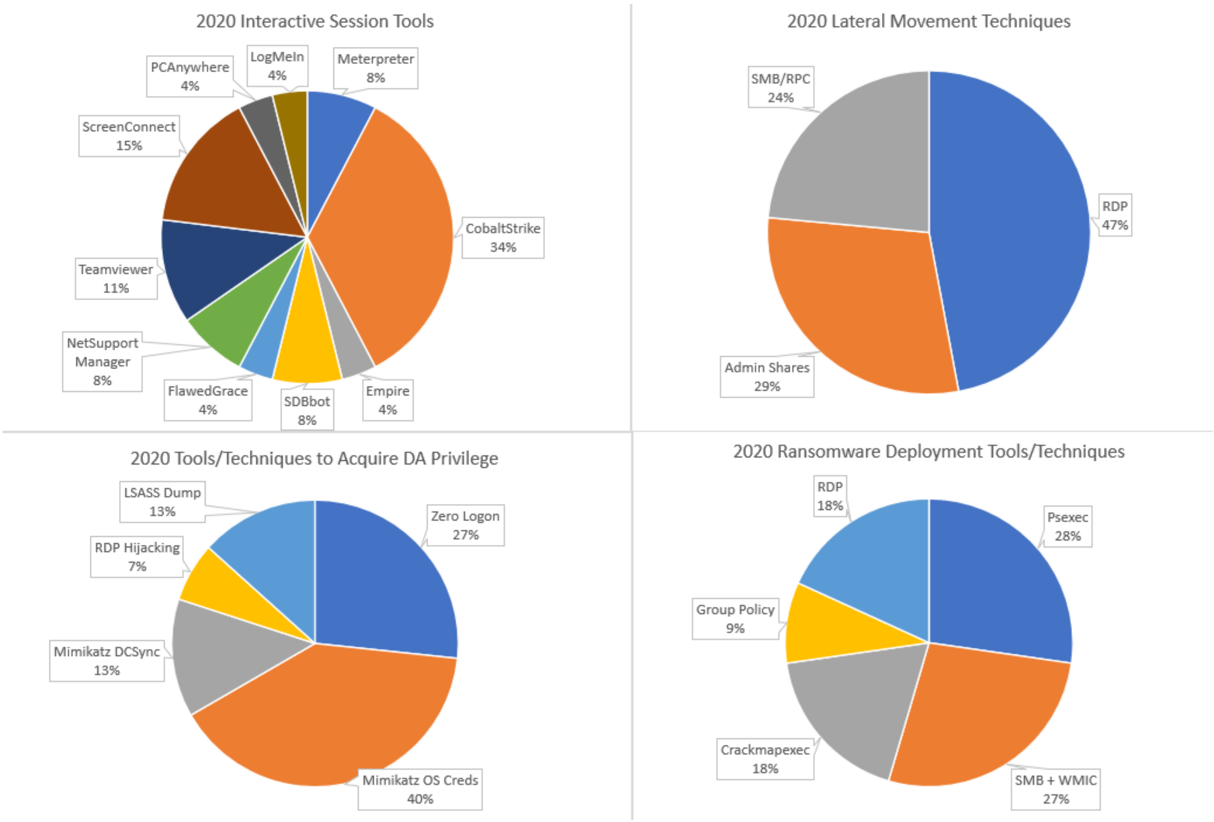

Figure 4: 2020 top tools and techniques to achieve core objectives in ransomware attacks

2021 ransomware attacks continued where 2020 left off, with ZeroLogon highly utilized to obtain privileged access during the first quarter of the year, however as organizations patched the vulnerability, the operators shifted back to acquiring credentials through the operating system.

One behavioral change that was observed by X-Force was a decrease in Mimikatz usage and an increase in operators acquiring credentials from the Local Security Authority Subsystem Service (LSASS) process within Microsoft Windows. Based on the evidence, X-Force believes the ransomware operators began utilizing LSASS to acquire credentials as a stealthier alternative to Mimikatz. CobaltStrike usage continued to increase from 2020 to 2021 accounting for 50% of interactive session activity in ransomware attacks.

While there was some minor modifications to the tools and techniques throughout 2021, X-Force observed that ransomware attacks continued to rely upon many of the same protocols and default permissions utilized in 2019 and 2020 to achieve their goal.

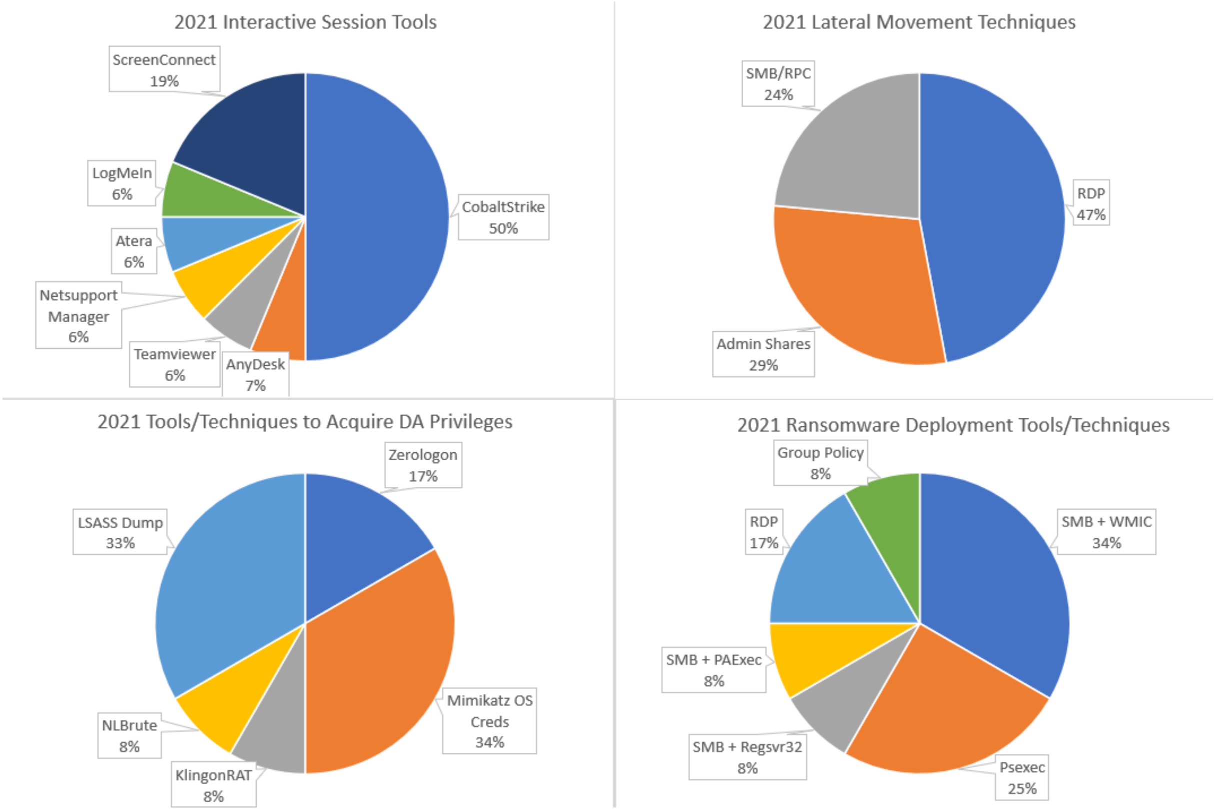

Figure 5: 2021 top tools and techniques to achieve core objectives in ransomware attacks

Ransomware Readiness

To assess the ransomware readiness of the victims and determine if the increasing speed of ransomware attacks is due to increased sophistication to bypass security controls or detection and response solutions, X-Force compared the existing security controls and detection and response capabilities of the victims against the fundamental components of the X-Force's ransomware readiness model.

X-Force differentiates protective and detection/response by the following conditions:

A protective control are design implementations aimed that preventing an attack from occurring or proceeding to the following stages of the attack lifecycle.

A detection and response control are technical solutions designed to detect and take action upon attacker activities as the attacker attempts to proceeding through the stages of the attack lifecycle.

Ransomware Protective Controls

X-Force identified five fundamental security controls specifically targeted to disrupt the ransomware attack lifecycle:

- Restrict and Implement MFA and PAM for Privileged Accounts
- Prohibit Workstation Logon with Domain Admin Credentials
- Restrict SMB/RDP/RPC for Internal Communication
- Implement Managed Service Accounts
- Restrict Software Execution on Domain Controllers and Secure Administrative Systems

See Controls section at the end of this report for detailed explanations for each of the aforementioned security controls

Results

X-Force discovered that in all of the successful ransomware attacks between 2019 and 2021, only one victim organization had implemented any of the five fundamental security controls specifically targeted to disrupt the ransomware attack lifecycle indicating that victim organizations have not adopted sufficient protective measures.

Ransomware Detection and Response Capabilities

To determine if the lack of adoption of detection and response capabilities played a significant role in the acceleration of the ransomware attack lifecycle, X-Force assessed the victim's ability to detect and respond to ransomware operators in their environment before the ransomware was deployed.

To assess the ability of the victim to detect ransomware operators based on the known ransomware operator TTPs, X-Force measured the number of successful ransomware attacks vs the ability of the victim to monitor endpoint visibility either through an endpoint, detection, and response (EDR) solution or centralized logging of detailed information about process creations, network connections, and changes to file creation time.

To assess the ability of the victim to respond to ransomware operators based on the known ransomware TTPs, X-Force measured the number of successful ransomware attacks vs how often responders were able to recover alerts of the attack prior to the ransomware deployment within the client's existing security tooling.

Results

X-Force determined that while detection capabilities increased throughout 2019 and 2021, it appears to have had little impact in slowing down the ransomware attack lifecycle. It is important to note, that while analyzing successful ransomware attacks vs detection capabilities, X-Force continually uncovered evidence of misconfigurations and oversights (Example: detect only policy vs blocking) within the tooling that enabled the attacks to progress without interruption. Additionally, X-Force discovered that responders were able to recover more alerts within existing security tools (including EDR) over the years between 2019 and 2021 indicating that security tooling has increased in volume and ability to detect ransomware operators prior to deploy of the ransomware but victims did not build out effective response policies and procedures to act on these detections.

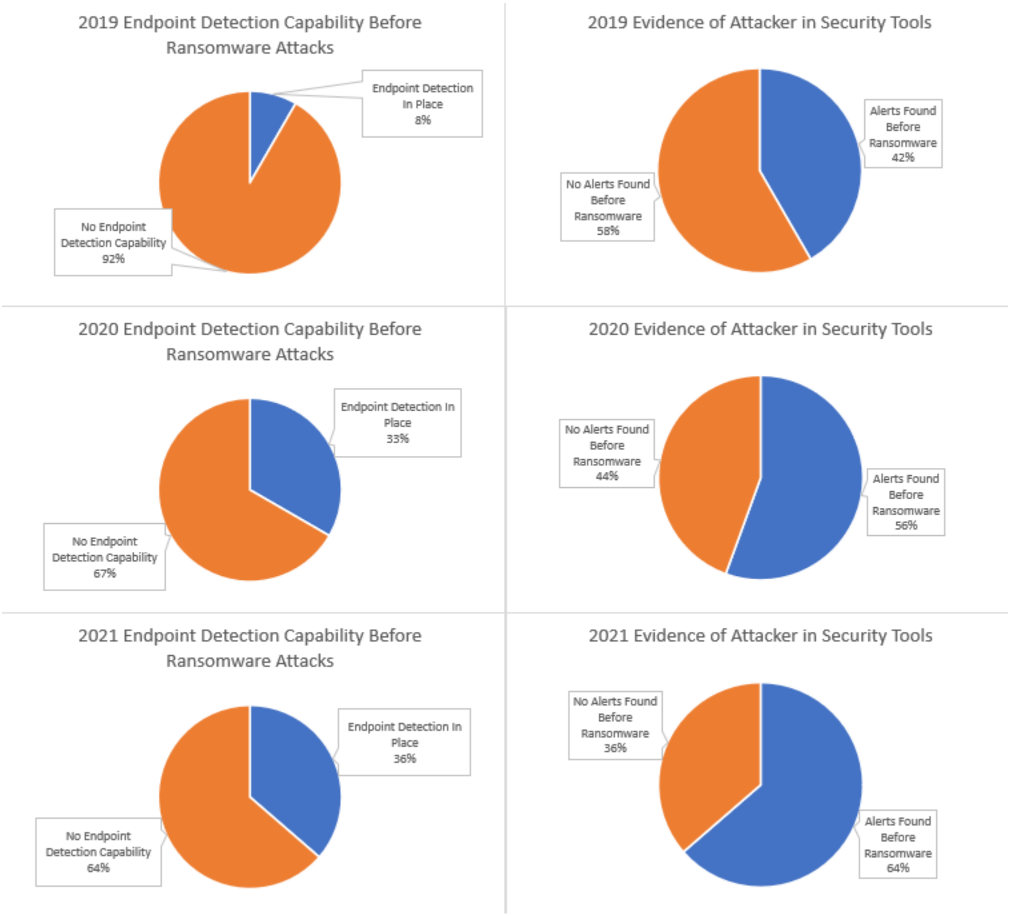

Figure 6: Detection and response capabilities for successful ransomware attacks 2019-2021

Conclusions

The results of this analysis indicate that the ransomware attack lifecycle has not experienced a great deal of innovation over the years. Furthermore, the reductions in attack timelines are likely due to the operationalization of ransomware attacks within the ransomware affiliates and execution against organizations that have yet to implement protection, detection, and response solutions designed to combat the ransomware threat.

Considering the trends observed through the analysis of ransomware attack timelines, X-Force maintains that ransomware attacks will continue to increase in speed and efficiency throughout 2022. X-Force recommends organizations properly invest in protection, detection, and response efforts to effectively combat the increasing speed of the attack lifecycle.

IBM X-Force

If you have questions and want a deeper discussion about ransomware prevention, detection, and response techniques or learn how IBM X-Force can help you with incident response, threat intelligence, or offensive security services schedule a follow-up meeting here:

IBM X-Force Scheduler

For more information about IBM ransomware protection solutions visit the IBM Ransomware Solutions Landing Page.

If you are experiencing cybersecurity issues or an incident, contact X-Force to help.

US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034

Learn more about how to protect your organization with the new Definitive Guide to Ransomware.

Controls

Restrict and Implement MFA and PAM for Privileged Accounts

A critical first step within this control is to establish a least privilege model within the organizations to prevent privilege escalation and credentials harvesting which is often to a critical step in a domain-wide compromise. X-Force recommends all organizations remove local administrator rights for all accounts unless absolutely necessary.

If privileged access is required for any system or systems within the organization, X-Force recommends organizations implement the following controls to address the threats of privileged account compromise.

The threat landscape has significantly evolved in recent years and X-Force no longer considers passwords alone to be an effective access control mechanism. Consequently, X-Force recommends that organizations securing privileged accounts using Multi-Factor Authentication (MFA) and Privileged Access Management (PAM).

Multi-Factor Authentication (MFA) is an authentication mechanism that grants access to a security principal only after providing two or more verification factors to confirm their identity and allow authentication to a computer system. MFA will enable organizations to enhance protection against credential theft. Implementing an MFA solution to enhance security in scenarios where the risk of compromised credential use is the greatest, such as:

- Users accessing systems via the Remote Desktop Protocol (RDP)
- Privileged users who are an appealing target for credential harvesting attacks necessary to escalate privileges
- VPN users that internal network from the Internet or other untrusted networks
- Users accessing corporate resources exposed to the internet, such as O365 webmail

PAM is a security technology allowing organizations to manage and secure the credentials for privileged accounts, including users with elevated privileges, local and Active Directory (AD) accounts, system administrators and super users, service accounts, and application accounts, among others. PAM reduces the risk of credential harvesting by malicious threat actors by providing temporary, session-specific credentials to perform a specific task.

At a minimum, X-Force recommends organizations enable Multi-Factor Authentication (MFA) for privileged accounts. This would include domain, enterprise, and local administrators.

Prohibit Workstation Logon with Domain Admin Credentials

X-Force recommends organizations implement a Group Policy to prevent workstation login by Domain Admin credentials. The following high-level steps are recommended by Microsoft to complete this recommendation.

In GPOs linked to OUs containing member servers and workstations in each domain, the DA group should be added to the following user rights in Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignments:

- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on locally
- Deny log on through Remote Desktop Services user rights

Detailed information on prohibiting Domain Administrator Login to workstations is available on the following webpage:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f–securing-domain-admins-groups-in-active-directory

Restrict SMB/RDP/RPC for Internal Communication

Review the need for and restrict where possible SMB, RDP, and RPC connections between internal VLANS, subnets, or class of system such as:

- Review the need for these protocols between workstations and block/deny these connections if possible.
- SMB and RPC are often required for client/server services and applications however, X-Force recommends organizations determine which services/applications require these protocols and scope firewall rules to accommodate and block/deny all unmercenary connections.
- Deploy dedicated administrative systems (i.e. “jump systems”) to facilitate necessary administrative uses for RDP, SMB, and RPC connections to workstations and servers. At a minimum, X-Force recommends Domain Controllers only be accessible via RDP from specific administrative systems.

Implement Managed Service Accounts

A service account, which can be either a local or domain account, often refers to a user account that provides a security context for services running on a Windows system. Windows offers the following built-in accounts to run services:

- Local system
- Local service
- Network service

System administrators often create service accounts to define specific security privileges for an application instead of using the build-in accounts. Another use case for service accounts is where a single identity is required by multiple systems.

Service accounts often have inherent risks associated with them, such as non-expiring passwords and interactive logons enabled. To address password management issues and prevent interactive logons with service accounts, a solution is to create and use a group Managed Service Account (gMSA). The primary advantage of this approach is that Windows handles password management and rotates the password periodically. Furthermore, a gMSA provides a single identity solution for services running on a server farm, or on systems behind Network Load Balancer. System administrators can configure services to use the new gMSA principal.

In cases where gMSAs cannot be implemented, X-Force recommends configuring security restrictions for regular accounts used as service accounts, including:

- Enforcing the principle of least privilege by assigning the minimum privileges required by the service.
- Denying interactive logons.
- Enforcing a minimum password length of 64 characters.
- Restricting the use of those accounts to the systems and tasks that require those accounts.

The above recommendations can be implemented via the built in Group Policy Object (GPO) functionality within Active Directory.

Restrict Software Execution on Domain Controllers and Secure Administrative Systems

X-Force recommends organizations to design application control policies for Domain Controllers, and secure administrative hosts and enforces those policies through an application whitelisting solution.

Microsoft AppLocker is a built-in application allow list technology that allows organizations to control what software can execute on Windows systems based on attributes, such as executable file path, hash, and publisher. The files that AppLocker can restrict includes executable files, dynamic-link library (DLL) files, Windows installer files, packaged apps, and scripts.

X-Force recommends organizations to design application control policies for Domain Controllers and secure administrative hosts and enforces those policies through AppLocker and Group Policy Objects (GPO) to protect those hosts against unwanted software or unauthorized execution, including malware and attacker utilities.

System administrators must configure an explicit rule and enforce it through a Group Policy for specific software to execute on systems. Any software that is not explicitly allowed will be denied by default. Consider the following approach to minimize the risk of operational impact:

- Configure AppLocker in an audit mode, review logs, and gradually tune application control policies before switching to an enforcement mode.
- Understand the enforcement mode's impact by configuring audit mode and regularly reviewing event logs to understand what software AppLocker would block in the enforcement mode.
- Consider sending AppLocker audit logs to SIEM and creating rules to alert on unauthorized software, such as PsExec or other known legitimate tools commonly leveraged by threat actors.