tenable.ad

A KING'S RANSOM:

HOW TO STOP RANSOMWARE SPREADING VIA AD

Hacking cost the U.S. $3.5 billion in 2019 alone. Despite this figure coming straight from the FBI's annual report on cybercrime, estimating the cost of ransomware is difficult due to limited data. The impact is much higher than reports indicate. One such report by Emsisoft, an IT security vendor, states that the average ransom is roughly $84,000. When considering lost business, time, wages, and files, the global business impact totals at least $170 billion annually. With many cybercrimes going unreported, the 2,047 ransomware events registered with the FBI Internet Crime Complaint Center (IC3) is conservative at best.

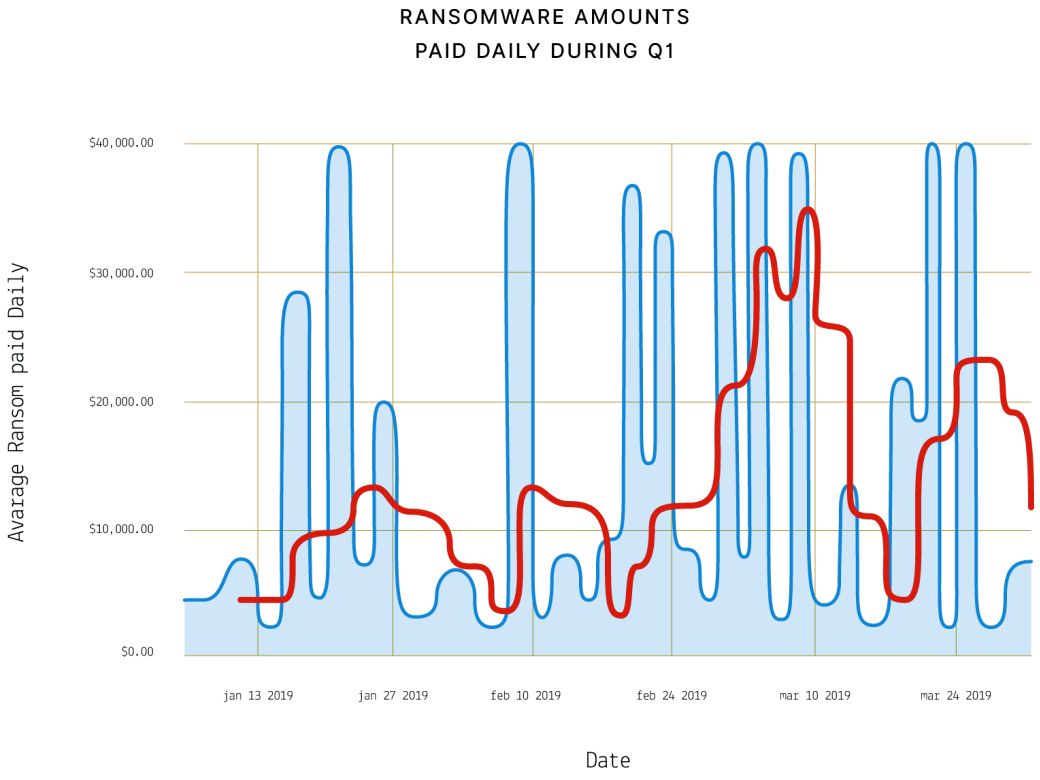
Ransomware Trends in 2019

Ransomware is more damaging than traditional computer malware since it not only infects devices but also encrypts data. A ransom is then demanded in exchange for a decryption key that restores access to the data. But in many cases, the decryption keys provided don't work. It's no wonder the FBI recommends not to pay ransoms.

Hackers are constantly evolving their methods, and 2019 was no exception. Rather than just encrypt the data on infected devices, ransomware authors have started to target resources beyond the devices themselves. For example, files on servers might be encrypted if an infected PC, or the ransomware, has access. Ransomware can enumerate mapped drives and the availability of file shares on the network.

Some hackers go even further by selling sensitive data. There have also been cases of hackers wiping data but still demanding a ransom. Compared to the final quarter of 2018, the average ransom paid increased by 89%.

Local governments in the U.S. have been hit hard by ransomware, including Baltimore, Delaware, and Kentucky. Instead of rebuilding their systems, some chose to pay ransoms against FBI advice. Doing so fueled criminals' incentive to double down.



Ransomware Spreads via Active Directory

The last couple of years have seen ransomware like LockerGoga and Samas omitting a spreader. Malware usually includes a means of propagating itself from an initial infected device to other devices on the same network. But instead of writing and testing the extra code, which may be prone to failure, hackers are leveraging a mechanism that is already present in most organizations: Active Directory.

Windows Server Active Directory (AD) is Microsoft's on-prem identity management product. It allows organizations to centralize management of user login credentials, configure settings on servers and workstations, and manage other aspects of an organization's security like its Public Key Infrastructure (PKI) and Role-Based Access Control (RBAC).

If a hacker gains privileged access to AD, it is easy to own an organization's entire IT infrastructure. On-prem and cloud solutions are both vulnerable. AD contains information about all users, endpoints, applications, and servers. Standard administration tools can be used to query the directory without being detected by security software. Hackers can then use AD to propagate ransomware to every device in the organization.

Even in businesses where IT has taken extra steps to secure domain controllers—the servers that run AD Directory Services—AD can still be easily compromised via end-user devices joined to AD if security best practices are not followed.

Examples of Recent Ransomware Attacks

Some of the highest profile attacks in the last few years spread using Active Directory. But AD is also being used in non-targeted attacks. While multinationals and government agencies tend to grab the headlines, smaller businesses and organizations are also falling victim to ransomware.

When IT providers specifically are hit, the impact extends to healthcare, government, education, and other industries. The consequences of a ransomware attack can be devastating. Entire networks can be encrypted, including backups and Active Directory domain controllers. Even if "good" backups are available to restore systems, the time and costs involved will be significant.

Here are a few examples of how hackers are harnessing AD to spread ransomware:

Norsk Hydro

The Norwegian aluminum company Norsk Hydro was hit by LockerGoga in March 2019. The infection started at a plant based in the U.S. before it spread to other facilities. The ransomware outbreak forced Norsk Hydro to switch to manual processes in many of its factories.

Norsk Hydro worked to restore its systems rather than pay a ransom and was only able to continue operations because it had a thought-out disaster recovery plan, which included failing over on-prem emails to Microsoft's Office 365 cloud service. But using the cloud as part of a disaster recovery plan isn't an option for companies that need to keep data in their own data centers for regulatory or compliance reasons.

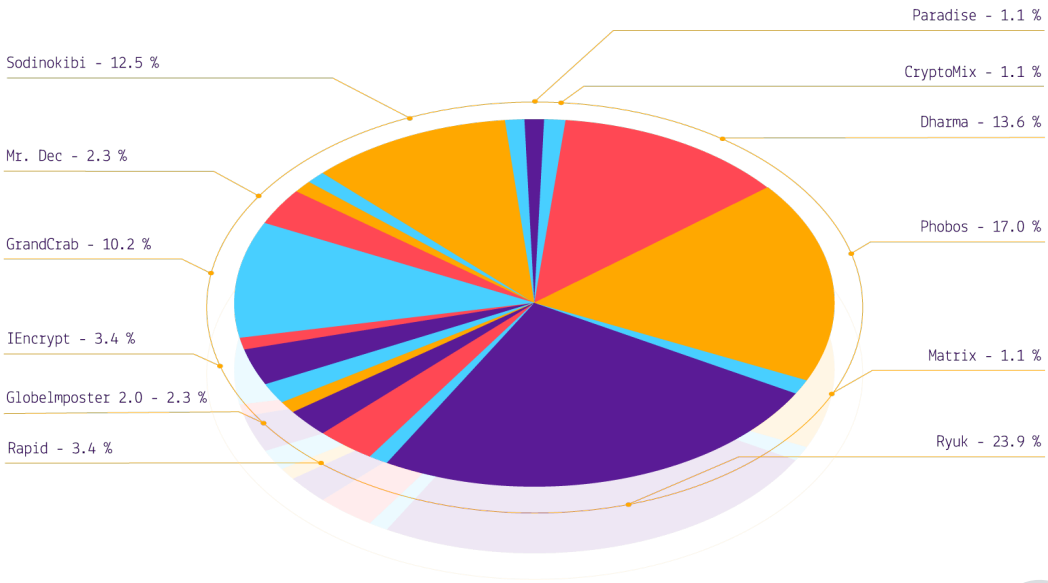
Oil and Gas Facilities

Late 2019 also saw Active Directory used to spread the Ryuk ransomware. ThreatGen, an operational technology cybersecurity services firm based in the U.S., reported that several of its clients in the oil and gas industry were hit by Ryuk.

The hackers used a vulnerability in Microsoft's Remote Desktop Protocol (RDP) to compromise Active Directory and get privileged credentials. The Ryuk ransomware was then inserted into a login script so that all clients logging in to AD were infected. When users and IT staff logged into their PCs or servers, the devices were locked and encrypted.

After initially compromising Active Directory, the ransomware lay dormant for months before it was inserted into login scripts. Laying low for so long could have allowed enough time to collect information on the infected organization's systems and data or to make it more difficult to restore from backup. One affected company tried to restore its systems but found that its backups were also infected with the ransomware.

RANSOMWARE MARKET
SHARE BY TYPE: Q2 2019



Kmart

In December 2020, US department chain Kmart fell victim to a brutal Egregor ransomware, which established a "ransom note" that verified Kmart's Active Directory domain being compromised during the attack. This ransomware was known for utilizing a double-extortion technique, where only a portion of the breached data is published to mobilize the victim to pay the ransom quickly. Typically, this ransomware type is injected through a loader. Once the initial breach has taken place, the ransomware disables the firewall settings and activates Remote Desktop Protocol (RDP). The malware is then able to move laterally through the network to detect and deactivate AV software. With last-stand defense disabled, the ransomware accesses and encrypts the breached data.

United Nations

In March 2020, the United Nations revealed that numerous servers across three UN offices were breached. Some of the compromised servers were used for user/password management, firewall, databases, and system controls. A UN spokesperson confirmed that their Active Directory lists of internal users were extracted by the attackers. A vulnerability (CVE-2019-0604) on the SharePoint server was used by the attackers to access and move laterally through the network. Almost 4000 UN staff were affected, with various types of personal information being compromised.

SaveTheQueen Ransomware

Early 2020 saw a new strain of SaveTheQueen ransomware, which first appeared in 2019, that encrypts and appends files with the .SaveTheQueen extension. The new strain spreads by inserting itself into Active Directory's SYSVOL share, which is replicated to every domain controller. SYSVOL can be read by all authenticated users, but it can only be written to by users with privileged access to AD.

Security company Varonis reported that the new strain of SaveTheQueen uses AD's SYSVOL share to write log files that monitor the progress of the attack on new devices. SYSVOL stores code for a scheduled task that runs a PowerShell script on devices to infect them with the ransomware.

Samas Ransomware

Active Directory has also been used to spread the Samas ransomware, which dates to 2016. Freely available tools are used to steal privileged Active Directory credentials. Then attackers work with standard administration tools to query AD to identify devices to encrypt. But in cases where Samas has encrypted files, AD is used for reconnaissance only, and the malicious code spreads like a traditional "worm" virus.

How to Prevent Ransomware Spreading via Active Directory

Ransomware attacks that use Active Directory to propagate or to perform reconnaissance require privileged access to the directory. Most organizations don't properly restrict or manage the use of privileged AD accounts, leaving IT systems exposed to ransomware and other kinds of attack.

Here are six ways that you can protect access to privileged AD accounts and make it difficult for attackers to weaponize Active Directory:

1 Reduce privileged AD group membership

2 Restrict the use of privileged AD accounts

3 Manage end-user devices using a local account

4 Protect privileged AD accounts with multifactor authentication

5 Monitor Active Directory for unusual activity

6 Implement a tiered administration model for Active Directory

1. **Reduce Privileged AD Group Membership**
   Microsoft recommends reducing the use of privileged accounts in an Active Directory domain to a bare minimum. While it is important to limit membership of the Domain Admins and Enterprise Admins groups, they are not the only privileged groups in AD. Schema Admins is an example of another privileged group.
   Tip: You can start by auditing the membership of privileged AD groups and by working to reduce their membership.

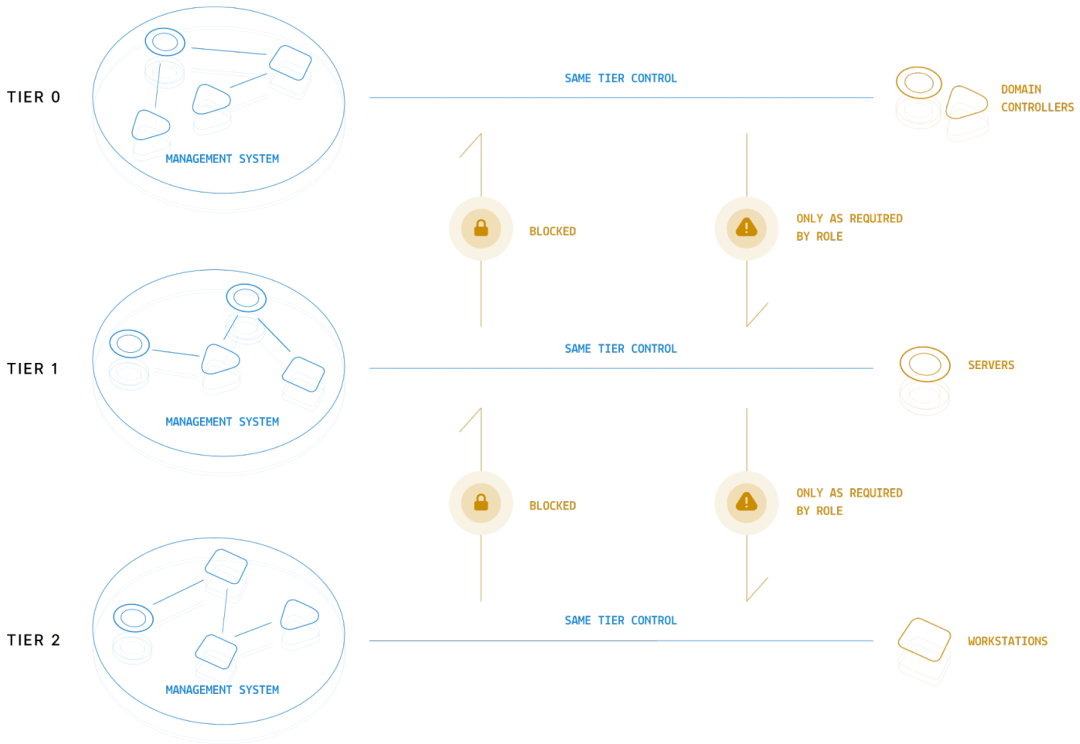
2. **Restrict the Use of Privileged AD Accounts**
   There are some technologies in Windows that can help reduce the exposure of privileged AD credentials, like the Protected Users group and Windows Defender Credential Guard. But you should follow Microsoft's best practices and limit the use of privileged AD accounts to devices that are specially secured for the purposes of administering Active Directory.
   Tip: Create a set of Privileged Access Workstations (PAW) used exclusively for performing administrative tasks that require privileged access to Active Directory.

3. **Manage End-User Devices Using a Local Account**
   Microsoft recently changed its advice on accessing client devices remotely using a local administrator account. Organizations generally grant remote access to clients using a domain user account. If you have a system in place to randomize and periodically change the local administrator password on each device, like Microsoft's Local Administrator Password Solution (LAPS) tool, then you can avoid a domain account for remote support. Using a local account for supporting end user devices makes it harder for hackers to compromise Active Directory.
   Tip: Audit local administrator account passwords. Make sure that each device has a unique local administrator account password. Then stop using domain accounts for remote support.

4. **Protect Privileged AD Accounts with Multifactor Authentication**
   Passwords are insecure because they can be easily abused if obtained by a hacker. But many organizations rely on passwords alone to protect privileged AD accounts. According to Microsoft, multifactor authentication is proven to block 99.9% of automated attacks. MFA requires users to provide something in addition to their password, like a biometric gesture or one-time passcode generated by an authenticator app.
   Tip: Add multifactor authentication to Windows Server Active Directory. Azure MFA and other products can be used to add MFA to AD.

5. **Monitor Active Directory for Unusual Activity**
   Just as antimalware software scans Windows for unusual files and processes, it is important to monitor Active Directory for unusual activity. The Windows Event Log contains a lot of information that could reveal misuse of privileged accounts and other malicious behavior. With the right data, organizations can proactively stop ransomware attacks spreading via AD. Security Information and Event Management (SIEM) products can be used to collect information forwarded from the Windows Server Event Log and other systems. Up-to-date threat intelligence can provide an automated way for organizations to identify threats in the data collected from security events. That said, neither Windows Logs nor SIEM products are enough on their own.
   Tip: Deploy SIEM with threat intelligence to proactively block ransomware and other types of malware before they infect your entire network.

6. **Implement a Tiered Administration Model for Active Directory**
   Microsoft recommends organizing resources in Active Directory to manage them using a more secure tiered model. The model defines three tiers that act as buffers to separate the administration of high-risk devices, like end-user PCs, from valuable servers, like domain controllers. Tier 0 includes resources like privileged AD accounts, domain controllers, and Privileged Access Workstations. Tier 1 is used for member services and applications. And Tier 2 is for end-user PCs and the objects in AD used to manage PCs, like helpdesk user accounts.
   Tip: Using a phased approach, reorganize Active Directory so that it can be managed with a tiered administration model.



Tenable.ad: Proactively Stop Ransomware from Infecting Entire Networks

Following Microsoft's security best practices is a good starting point to secure Active Directory and to stop hackers using it to spread ransomware. But the out-of-the-box tools in Windows Server do not provide a way to monitor Active Directory in real time, nor do they supply the threat intelligence needed to automate responses in an ever-changing threat landscape.

Tenable.ad can identify security issues with AD before attackers exploit them to spread ransomware. Built-in knowledge and threat intelligence help organizations mitigate issues and remediate threats. Tenable.ad integrates with SIEM and security tools to proactively improve AD security, providing dynamic dashboards to give you insights that are not possible without specialist security software.

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com