SILVERFORT AIG

Identity Has Become the Prime Target of Threat Actors

Lack of Full Multi-Factor Authentication is a Key Finding in Numerous Incident Dialog

WHITE PAPER

The ransomware landscape has seen a major escalation in the frequency and scope of attacks in 2023 according to various sources[1]. As cybercriminals have become more sophisticated, they are exploiting most organizations' critical gaps against identity threats—with over 83% already having experienced a breach involving compromised credentials[2]. Identity is also one of the key pillars of the zero-trust strategy,[3] suggesting it is critical for organizations to review their Identity and Access Management strategy. Multi-Factor Authentication (MFA) has long been advocated as a robust measure to bolster an organization's security posture, but misconfigurations and gaps in MFA coverage have proven that a more wholesome and unified approach is decisively required in stemming this dangerous trend in cybercrime.

What Is the Security Value of MFA?

MFA is an authentication mechanism where a user must present two or more factors of evidence to gain access to a website, account, or application. These factors of evidence include 1.) something the user knows (passwords, pins, codes, etc.), 2.) something the user possess (keys, smart phones, smart cards, token devices, etc.) or, 3.) something the user has (facial recognition, retina scans, fingerprint scans, etc.). The authentication mechanism grants access only if each of the authentication factors are successfully verified. In this way, if user credentials (such as a username and password) are inadvertently compromised, a cyber-criminal does not automatically gain access to the account. MFA adds additional layers of security, making unauthorized access more difficult.

Now consider a typical ransomware scenario, which usually consists of three phases: 1.) initial access and gaining initial foothold within the target organization, 2.) privilege escalation (if needed) and lateral movement and, 3.) data exfiltration and/or ransomware deployment and execution. Without MFA on external connections an attacker can leverage compromised credentials to infiltrate the internal network through VPN or any other remote connection in place. Within the internal network, the lack of MFA would enable an attacker to freely move laterally inside the domain and infect any domain-joined system with the ransomware payload. In this sense, backups should not be joined in the domain so that the recovery process is not also compromised.

Properly configured MFA is a proven security mechanism that can prevent malicious access with compromised credentials in real-time.

Why Is MFA Especially Important for Administrative Users?

Administrative users or privileged users have access privileges to all critical resources within the network environment.

This implies that, from an attacker's perspective, compromising a privileged user account is the single best strategy to deploy and execute the ransomware payload on every resource that the privileged user has access to. This makes protection of privileged users with MFA a top priority.

More than **66%** of organizations compromised by a ransomware attack saw ransomware deployment linked to the compromise of a highly privileged account on their Active Directory environment.

AIG Study #1: A regular employee's credential used to log into the organization's corporate resources was compromised. The remote access used by the employee was not configured with MFA. As such, the TA (Threat Actor) was able to connect to a Citrix gateway, used the valid employee's credentials and compromised the organization's external perimeter. From that point, the TA moved laterally across the network using Remote Desktop Protocol (RDP) connections. Then, the TA elevated privileges by compromising a privileged service account used for a backup service and without risk mitigation controls applied the TA used Group Policy (GPO) modifications to run LockBit ransomware malware and encrypted data across the virtual environment. (For more information on privileged Service Account compromise refer to the topic "MFA Coverage Gaps Due to Installation Method" below).

What Are the Challenges of Traditional MFA?

Technology Gap of Legacy Resources and Protocols

MFA as a technology has been around for a relatively long time, but the market continues to demonstrate that it is not as widely used as the reader would expect. For applications or systems born in the cloud, MFA is natively integrated into modern web and SaaS app authentication protocols. This supports a reduction in BEC[4] attacks using these platforms. However, it is important to note that while such an implementation of MFA protects access to the organization's web email or storage apps, this protection does not extend to the organization's on-premises servers, workstations, databases, and apps. For many organizations, a significant portion of their critical infrastructure and access methods still reside in the on-premises environment.

For the on-premises environment, AIG has further learned through the process of reviewing cyber insurance applications from potential policyholders that applicants have difficulty meeting the MFA requirements due to the following challenges:

- In versions prior to Windows 10, MFA does not come as a pre-configured, ready-to-deploy option as part of standard, on-premises Microsoft Active Directory deployment.
- The access to critical resources was done via native authentication protocols such as Windows New Technology LAN Manager (NTLM) or Kerberos, which if compromised the TA can take over the domain. Also, command line access to workstations and servers, IT and networking infrastructure, old applications, and many more that don't support MFA technology.

MFA Coverage Gaps Due To Installation Method

The traditional MFA installation method relies on either installing an MFA agent on resources that need protection or placing a proxy in front of their network segment. Both methods introduce inherent coverage gaps.

63% of organizations that stated they used MFA for protecting privileged access were still impacted by a ransomware event linked to coverage gaps in MFA configuration/installation method.[5]

AIG Study #2: We observed several organizations authorizing direct remote privileged user access through a remote access solution such as VPN. Even if MFA-enabled, organizations should authorize unprivileged remote access only followed by a second step of privilege escalation from within the network. The privilege-escalation MFA should be a dedicated/separate security control.

Furthermore, many machines within the enterprise environment cannot sustain an MFA agent due to operability issues, such as service accounts. Service accounts in Active Directory (AD) are user accounts that are not owned or used by people and instead are dedicated to a specific application or system. These accounts are frequently configured to run a service on servers and/or workstations in an environment. Service accounts are typically granted privileged rights in the environment and are often added to highly privileged groups such as the Domain Admins group. This is frequently due to the recommended and supported installation model pushed by software vendors to avoid permission issues or functionality mishaps during installation and operation. In order for these accounts to work, the service account name and password must be stored locally on the system. Service accounts have a password that is set when created and rarely changed. If an attacker can guess or otherwise discover the password, including compromising a system where the service account is used, they would be able to extract and employ those service account credentials to exploit the environment.

Microsoft's best practices guidance is that Domain Admins should not be used outside build/fix, and instead proper delegation and "least privilege" should be enforced, but our study shows this isn't happening in practice and ransomware actors are taking advantage.

In many of the over-privileged service accounts analyzed by AIG in cyber insurance applications submitted by potential policyholders, it was discovered that the elevated privileges were not necessary for the operation of the service account on servers or workstations. Service accounts[6] rarely require the highest level of privilege to perform the function on a server or worse a workstation. Having a service account with high privilege while the risk of being compromised was very high due to the nature of those service accounts.

AIG Study #3: AIG has conducted numerous incident dialogs where an over-privileged service account was identified as the root cause behind TA acquiring a highly privileged credential allowing the TA to elevate privileges and compromise all domain-joined systems. In many cases, applicants were unaware of the risk while in other cases the risk was ignored because of fear of breaking the service by deprivileging the service account. In one case, a service account was inadvertently added to the VPN profile allowing the TA to use that account for remote access without MFA because MFA is virtually impossible to enforce on service accounts.

MFA Bypass Due To Telephony-Based Authentication Methods

Over the past year there has been an increase in MFA bypass as a defense evasion technique. As such, it is extremely important to give consideration during implementation and the approved methods allowed for MFA authentication. MFA Interception[7] is one of the more common MFA bypass techniques used for Credential Access. Typically, MFA Interception is accomplished via one of the following methods: SIM Swapping against SMS based MFA implementations, and eSIM number porting used against call back based MFA implementations. Other methods of MFA bypass include social engineering to trick a user into providing the MFA code in real-time, the use of fake SSO sites to capture the MFA code in real-time, and the use of MFA Authentication Request Generation[8] designed to cause MFA fatigue.

AIG Study #4: AIG has conducted numerous incident dialogs where the use of SMS based MFA was identified as the root cause allowing the TA to gain initial access via SIM Swapping. Recently, AIG identified a case where MFA Interception occurred via eSIM number porting such that the MFA code provided during the call back was given directly to the TA.

Overcome the MFA Challenge With an Approach That Provides Full MFA Coverage

To overcome the MFA challenge presented in this paper, the client should consider an approach that aims to solve the challenges that a traditional MFA implementation fails to address. The approach should manage and integrate all cloud and on-premise identity providers (IdP) in the environment. Solving for cloud alone leaves gaps that can be exploited for on-premise environments. The concept is to ensure that every authentication and access request is analyzed prior to granting or denying user access. Presuming that some requests can't or shouldn't be analyzed leaves potential gaps. These gaps are what has led to events described in this paper. It is important to state that the approach of analyzing access requests and triggering of MFA must be protocol agnostic, including those originating from legacy authentication protocols, command line, file share, and any other on-prem resources to guarantee full MFA coverage. This means that by using this approach, MFA can be extended to all resources that are traditionally beyond the scope of this type of protection.

Key Takeaways

1 Risk Analysis of Your Environment

Perform a risk analysis based on your resources and environment to assess the potential gaps and misconfigurations that could increase the risk of compromising your entire network.

2 Prioritize the Users That Need Protection

Compile a list of users including service accounts whose protection is a must-have. This would include all admin user at a minimum, but also any other users that have access to critical resources.

3 Choose an MFA Solution With Full Coverage

Don't compromise on your MFA's protection coverage. Ensure that it applies to all resources and access methods with special emphasis on the unique needs of your environment.

4 Apply MFA Protection In a Non-Negotiable Manner

Configure MFA policies for all users who need it and ensure they understand it's a non-negotiable deal. Don't exclude anyone from this protection either fully or partially. Remember that MFA partial protection is as good as zero protection.

5 Ensure That MFA Implementation Is Phishing Resistant

Identify any applications that may use SMS or call back based MFA, with added emphasis on legacy applications, and ensure that those methods are updated as soon as possible. For additional awareness and assistance, we recommend following the guidance provided by the Federal Trade Commission[9] and Cybersecurity and Infrastructure Security Agency[10].

Footnotes

1. World Economic Forum
2. The State of the Identity Attack Surface
3. Embrace proactive security with Zero Trust - Microsoft
4 Business Email Compromise and Tips to prevent it - Microsoft.
5. The sample includes about 100 AIG insureds from 20 countries and 18 industries over a two-year period that suffered a ransomware incident where AIG conducted a post-incident dialogue.
6. Implementing Least-Privilege Administrative Models - Microsoft
7 Multi-Factor Authentication Interception, Technique T1111 - Enterprise | MITRE ATT&CK®
8 Multi-Factor Authentication Request Generation, Technique T1621 - Enterprise | MITRE ATT&CK®
9 SIM Swap Scams: How to Protect Yourself | Consumer Advice (ftc.gov)
10 Implementing Phishing-Resistant MFA (cisa.gov)