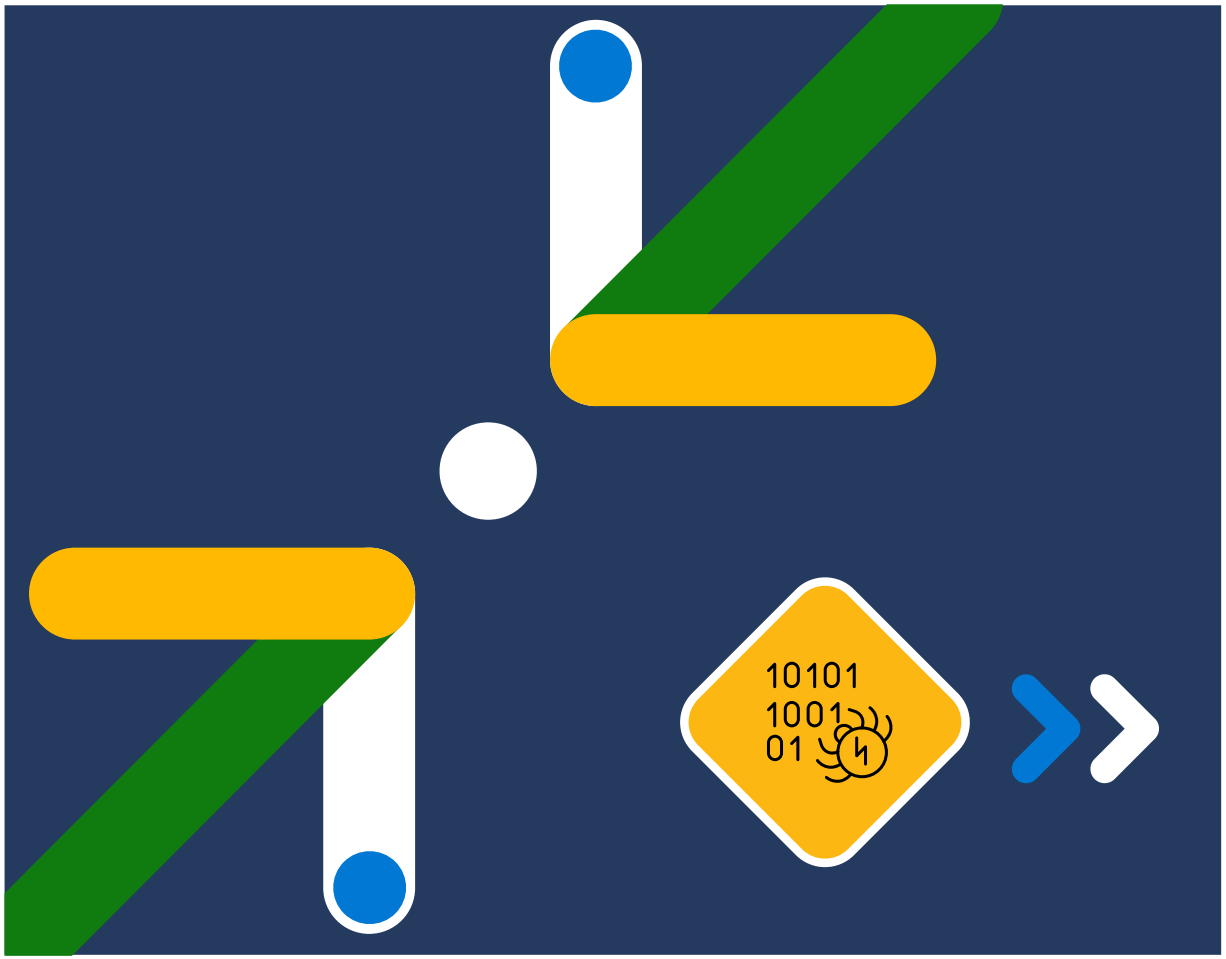
Microsoft Security



CYBERATTACK REPORT

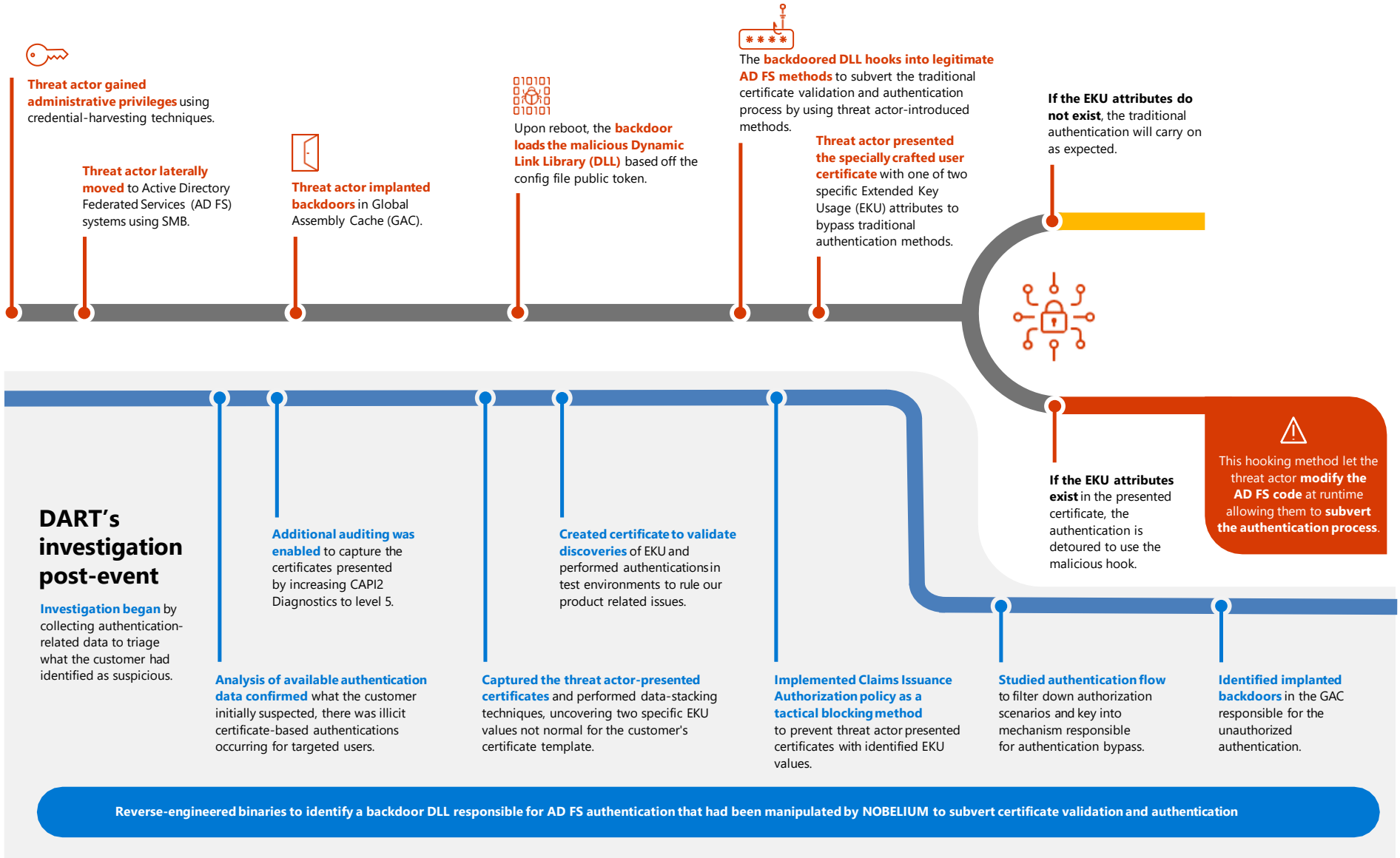
NOBELIUM MagicWeb exploit

Solving one of NOBELIUM's most novel attacks

The combination of the ever-evolving adversary NOBELIUM, a security-conscious customer, and a never-before-seen attack yielded one of the most memorable cases in Microsoft Detection and Response Team's (DART) 15-year history. This report describes the first time a Global Assembly Cache (GAC) implant was seen in the wild. This new malware, later dubbed MagicWeb, allows the attacker to authenticate as anyone in a targeted network. Discover how the team identified what happened and stopped this persistent bad actor, and learn best practices for protecting your business.

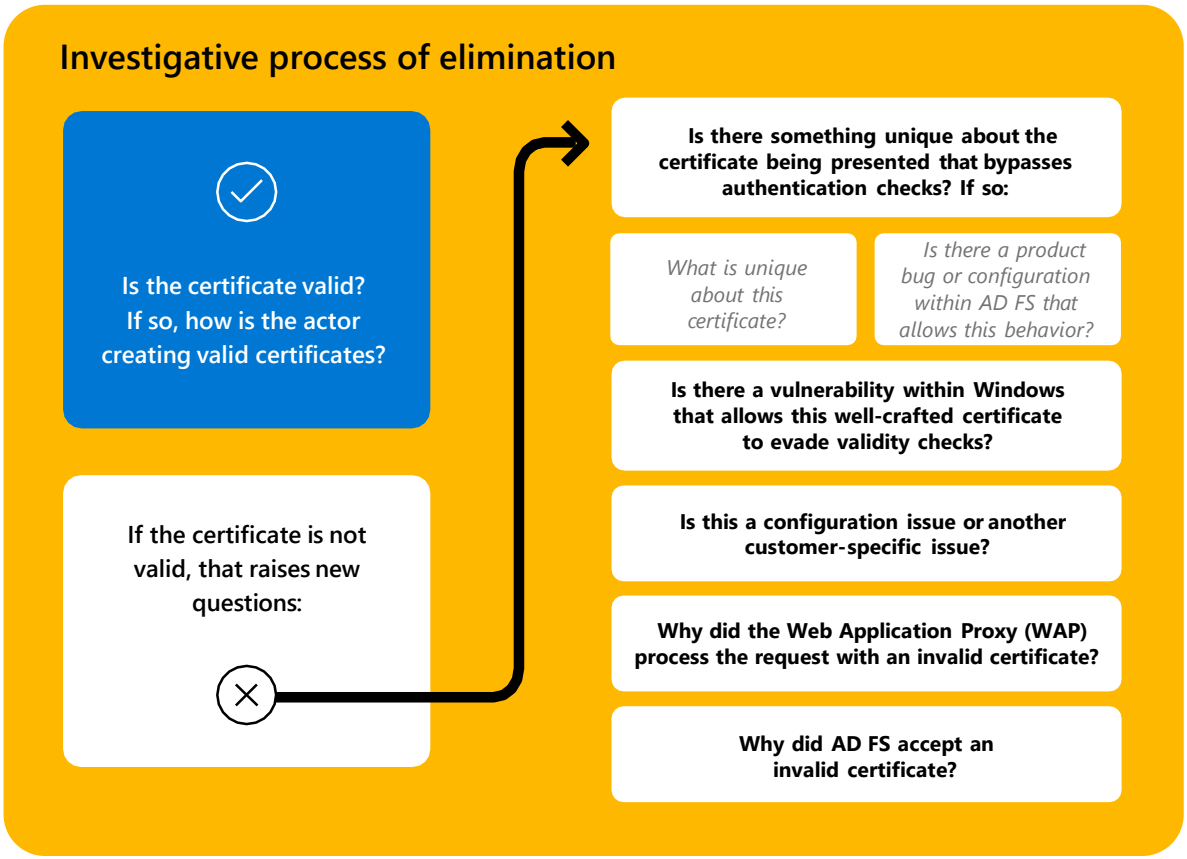
The NOBELIUM threat actor targets organizations across multiple industries, including government agencies, financial institutions, and technology companies.

MagicWeb attack flow



How did it begin?

Most attackers play an impressive game of checkers, but increasingly we see advanced persistent threat actors playing a masterclass-level game of chess. NOBELIUM is perhaps most notorious for the SolarWinds supply chain compromise in December 2020, which is widely regarded as the most sophisticated nation-state cyberattack in history. In fact, NOBELIUM remains highly active, executing multiple campaigns in parallel targeting government organizations, non-governmental organizations (NGOs), intergovernmental organizations (IGOs), and think tanks across the US, Europe, and Central Asia.



Nation-state attackers like NOBELIUM have seemingly unlimited monetary and technical support from their sponsor as well as access to unique, modern hacking tactics, techniques, and procedures. Unlike most bad actors, NOBELIUM changes their tradecraft on almost every machine they touch. Our analysts note that this actor places a very high value on their operations and have exceptional tradecraft, rarely making mistakes and constantly changing tactics, which helps them remain undetected.

In August 2022, a Microsoft customer fell victim to a post-compromise capability now referred to as MagicWeb, which was used by NOBELIUM to maintain persistent access to the customer environment they had compromised. After noticing strange authentication requests, the customer contacted DART. The global team quickly responded and traveled onsite to deliver a real-time investigation.

Upon arrival, DART assessed the situation and performed various data-wrangling actions followed by in-depth data analysis to understand how the threat actor gained access to the environment, implanted the backdoor, and later how the backdoor worked. This included a rapid response to target the removal of the backdoor implants and execute a complete migration off Active Directory Federation Services (AD FS) to Azure Active Directory (Azure AD). Additional monitoring techniques were then put in place to keep a close eye on any actions performed by the threat actor.

How did Microsoft respond?

The incident response team with the support of Microsoft Threat Intelligence Center (MSTIC) divided its resources into different lines of inquiry, focusing on the authentication process and flow and separating the authentication scenario into logical buckets. Following the authentication flow, the user presents a certificate to the Web Application Proxy, a request is proxied to the AD FS Server for the certificate-based authentication process, and then AD FS processes the authentication based on the validity of the certificate and account details.

The incident response team moved ahead to provide evidence in support of the hypothesis made above. They accomplished this by using CAPI2 diagnostic logging to collect the presented client certificates. Following a thorough examination of the customer's certificate templates, the team examined the certificates for irregularities.

The certificates weren't valid and chained up to a trusted issuing authority. After stacking the data, the incident response team discovered one specific field in the captured client certs: two distinct hardcoded object identifiers in the EKU attribute of the certificate. With the deltas in the actor certificate identified, the team began to reverse-engineer the attack and duplicated the activity with crafted certificates of their own. Our experts were back to tackling the largest puzzle in the case: how did MagicWeb subvert authentication?

Concluding that only AD FS and specially crafted certificates were the source of trickery, the team zeroed in on the AD FS authentication processes and process dependencies. This led them to identify that NOBELIUM implanted a backdoored copy of a DLL (Microsoft.IdentityServer.Diagnostics.dll) and a modified configuration file (Microsoft.IdentityServer.Servicehost.exe.config).

Digging deeper into the identified binaries, analysts identified that the loading of NOBELIUM's malicious (Microsoft.IdentityServer.Diagnostics.dll) into the AD FS process was made possible by editing the configuration file to specify a different public token, thus loading the malicious DLL from the Global Assembly Cache (GAC) upon reboot. This allowed the actor to intercept and manipulate the claims pipeline through loading the backdoored DLL with added .NET classes and static constructors that hooked into the legitimate AD FS methods.

The four main methods identified in the technical analysis of MagicWeb indicated that the X509 certificate passed checking for specific EKU attributes, and upon a match would effectively bypass certificate validation. This satisfied Multifactor Authentication (MFA) to authenticate the user based off the user certificate details.

What can organizations do to detect and respond to this threat and similar techniques?

Maintain AD FS and all Identity Service Providers (IdPs) as a Tier 0 asset.

Identity-based attacks continue to rise so implementing a "privilege access strategy" can protect all identity providers.

Mandate MFA organization-wide, all the time.

Where applicable, enforce Multifactor Authentication (MFA), preferably with location-based and number match requirements. Recent identity-based attacks were initiated from MFA fatigue attacks or lack of MFA enforcement.

Identify, log, and audit your organization's authentication flow.

Detecting identity-based attacks in your organization begins with determining what identity platforms are responsible for the authentication and authorization. Once the authentication flow is identified, centralizing logging and auditing to establish an authentication baseline will increase your organization's visibility and ability to react to unusual authentication events.

Increase the cost of threat actor's operations.

Basic security hygiene still protects against most forms of cyberattack. Implement a "brilliance in the basics" strategy for cybersecurity hygiene. With this, organizations can force threat actors to increase the cost of their operations by removing the "low-hanging fruit." A foundational element of every organization's security roadmap should include Asset Discovery, MFA Enforcement, Device Management, Vulnerability Assessments, and Patch Management.

Summary: MagicWeb

Evicting the persistent attacker NOBELIUM required rearchitecting the customer's entire environment. Here we detail moves made by NOBELIUM and the steps taken by the customer and Microsoft's Detection and Response Team (DART) to null the threat:

NOBELIUM's MagicWeb attack flow

1. Accessed a vulnerable application through Azure AD App Proxy.
2. Moved laterally to the AD FS servers using an Active Directory privilege escalation vulnerability.
3. Added a modified DLL and config file to the Global Assembly Cache (GAC) on each AD FS server.
4. Crafted a certificate using a rogue certificate authority containing a "magic" value.
5. Presented the crafted certificate to AD FS - the modified DLL sees that magic value and stamps the Multifactor Authentication Claim into the SAML assertion.

Microsoft's investigation

1. Systematically investigated possibilities – implant, bug, stolen private keys, and configuration.
2. Leveraged in-depth knowledge of AD FS to enable additional logging to track actor activity and capture actor-presented certificates.
3. Identified distinct differences in the actor-crafted certificate compared to a legitimate certificate, uncovering a delta in the extended key usage (EKU) attributes.
4. Recreated the attack leveraging a certificate crafted by the team that contained the "magic" extended key usage attribute.
5. Captured a memory dump from the AD FS server to identify malicious code in memory.
6. Leveraged Microsoft Defender for Endpoint to identify how the malware was copied to the AD FS servers from another, unrelated system that was accessed via App Proxy by the threat actor.
7. Executed a rapid migration away from AD FS.

Steps customers can take

1. Maintain AD FS and all IdPs as a Tier 0 asset.
2. Identify, log, and audit your organization's authentication flow.
3. Mandate multifactor authentication (MFA) organization-wide, all the time.
4. Keep up with basic security hygiene to force threat actors to increase the cost of their operations.

To learn more about Microsoft's specialized support before, during, and after an incident, please visit:
https://aka.ms/SecurityServicesIncidentResponse