



A New kind of Windows NTLM Relay Attack

CRITICALITY

23/06/202٢

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A Proof-of-Concept (PoC) for the DFSCoerce NTLM relay attack has been published by a researcher. To take over a Windows domain, the technique makes use of the Distributed File System: Namespace Management Protocol (MS-DFSNM).



Threat Details

The Distributed File System (DFS): Namespace Management Protocol (MS-DFSNM) is used by a new Windows NTLM relay attack known as DFSCoerce to take over a domain. The challenge-response mechanism is exploited by the well-known NTLM (NT Lan Manager) relay attack. It gives malicious parties the ability to occupy a position between clients and servers, intercept, and then transmit validated authentication requests in order to obtain unauthorized access to network resources and, in essence, establish a base in Active Directory environments.

NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN). NTLM is a protocol that authenticates clients by using a challenge and response system. The NTLM relay attacks allow attackers to steal hashed versions of user passwords, and relay clients' credentials in an attempt to authenticate to servers. They use a Machine-in-the-Middle method that allows threat actors to sit between clients and servers and intercept and relay validated authentication requests in order to gain unauthorized access to network resources. The DFSCoerce script is based on the PetitPotam attack, but rather of utilizing MS-EFSRPC, it makes use of MS-DFSNM, a protocol that enables management of the Windows Distributed File System (DFS) via an RPC interface.

An attacker can obtain a certificate that can be used to obtain a Ticket Granting Ticket (TGT) from a domain controller by relaying an NTLM authentication request from a domain controller to the Certificate Authority Web Enrolment or the Certificate Enrolment Web Service on an AD CS system, the CERT Coordination Center (CERT/CC) noted, outlining the attack chain. Security researchers who have tested the new NTLM relay attack have told that it easily allows a user with limited access to a Windows domain to become a domain admin.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.

References

Arntz, P. (2022, June 21). *DFSCoerce, a new NTLM relay attack, can take control over a Windows domain.*

Malwarebytes Labs. Retrieved June 23, 2022, from <https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/06/dfscoerce-a-new-ntlm-relay-attack-can-take-control-over-a-windows-domain/>

Lakshmanan, R. (2022, June 21). *New NTLM Relay Attack Lets Attackers Take Control Over Windows*

Domain. The Hacker News. Retrieved June 23, 2022, from <https://thehackernews.com/2022/06/new-ntlm-relay-attack-lets-attackers.html>

Abrams, L. (2022, June 22). *New DFSCoerce NTLM Relay attack allows Windows domain takeover.* Bleeping Computer.

Retrieved June 23, 2022, from <https://www.bleepingcomputer.com/news/microsoft/new-dfscoerce-ntlm-relay-attack-allows-windows-domain-takeover/>



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to follow the below steps:

- Enabling protections like Extended Protection for Authentication (EPA), SMB signing, and turning off HTTP on AD CS servers.
- Disable the deprecated NTLM authentication where possible and use the Extended Protection for Authentication (EPA).
- Use the Windows' built-in RPC Filters or RPC Firewall to prevent servers from being coerced via the MS-DFSNM protocol.
- Enabling multi-factor authentication and installing all available security updates as soon as possible.
- Disable NTLM for Internet Information Services on AD CS servers in the domain running Certificate Authority Web Enrollment or Certificate Enrollment Web Service.
- Configure the GPO and then open Group Policy and advance to Computer Configuration. Then, head to Windows Settings -> Security Settings -> Local Policies -> Security Options then set 'Network Security -Restrict NTLM -Incoming NTLM Traffic' to the option 'Deny All Accounts' or 'Deny All Domain Accounts'.



Appendix B – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix C – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.