Threats Hidden in Employee Workstation through Office Files

Tung-Lin Lee
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 70101, Taiwan

I-Hsien Liu
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 70101, Taiwan

Jung-Shian Li*
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 70101, Taiwan

*E-mail: tllee@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw**

Abstract

With the advent of the Internet of Things era, IoT devices participate in our work environment. From printers, shared files to temperature control, they make our working environment more convenient. Although these IoT devices communicate through different communication protocols, the same identity verification method is often used., hackers can also use this authentication method to steal user identity verification information, This study combines past research results to present our new findings, and further, organize them into a complete attack architecture.

Keywords: Active Directory, IoT, Credentials, Spear-fishing

1. Introduction

In an environment with Active Directory (AD), all resource access authorization authentication will be handled by Active Directory, so that every Server (EX: Exchange server, NAS, printer) does not need to handle every user's authentication credential. Although the server authentication work is shared by Active dictionary, for users, to access a certain function, they still need to enter the password repeatedly once they want to access different resource. To deal with this situation single sign-on implementation was invented.

Due to the single sign-on implementation of windows operating systems, users could save a lot of time without having to enter their account and password again and again. However, this setting also allows hackers to Use some dedicated constructed malicious files to steal the user's identity verification information (NTLM hash), and then launch attacks like passing the hash, and then log in to the user's computer remotely, which becomes a way to gain access to the organization's intranet.

Although there are many ways to cause an NTLM hash leak, fortunately, most of them cannot be exploited by hackers. In this study, we would discuss several NTLM hash leak methods, and focus on some of the most commonly used method of hacking: Office files, and dive

deeper to the possibility of extended application and under what circumstances will the existing protection mechanism be bypassed.

In the second section introduced background knowledge related to authentication, as well as traditional attack methods. In the third section, we will introduce our new discoveries and ways to bypass existing protections and combines past research and our findings to try to construct a method that can be used to automate large-scale attacks in real scenarios. Finally, the forth section will be our conclusion.

2. Background

In this section, we will introduce a common authentication method "NTLM". Besides, we will discuss the protocol and application using NTLM, and the past attacks on this authentication.

2.1. *NTLM Overview*

NTLM is a challenge-Response authentication mechanism. First, the client informs the server, the username and informs the server that it wants to log in. Then the server sends out a set of random number as a challenge and requires the client to hash it with its own password. Third, the client sent the hash result to the server, and then Server will verify whether the password is correct or not.

The NTLM protocol suite was first implemented in a Security Support Provider of Microsoft security protocols and been adopted in other protocols. Because NTLM has undergone many changes, We are not going to talk about its cryptography details here. If you are interested in the detailed, Microsoft official document could provide more information.

NTLM is mainly used for SMB, LDAP, MSSQL, HTTP, and other protocols, not only that, although it is not the preferred authentication method, in fact, NTLM is also used for wi-fi connection and remote desktop authentication. Although NTLM has been around for decades and has been updated many times, its security mechanism has often been challenged. MITRE ATT&CK has suggested that enterprises or institutions should not use NTLM for authentication but instead using Kerberos. However, Kerberos is more complicated to set up and there is downward compatibility and the third-party software requirement which does not support Kerberos as an authentication option, using NTLM for authentication is usually a necessary option.

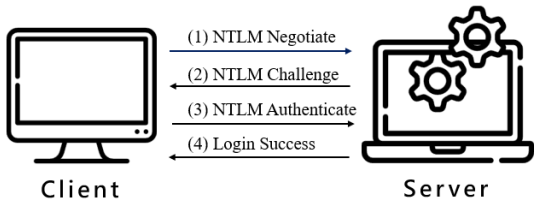

Fig. 1. The NTLM Challenge-Response Mechanism.

2.2. *Typical attack*

The security problems of the NTLM mechanism are reflected in two aspects. First, the NTLM hash can be cracked by rainbow tables or brute force. Common attack methods used Responder as a malicious server which answers to specific queries to receive the credentials sent by the victim to obtain the NTLM hash and then start the cracking process.

However, it is difficult to crack in a limited time, so there is another attack method called NTLM relay or so call pass the hash. The attack method is another variant of a man-in-the-middle attack as shown in Figure 2. Although there are some mitigations such as EPA (Enhanced Protection for Authentication), there are still ways to bypass those mechanisms such as “drop the mic”, and NTLM relay is still an indispensable step while implementing these attack. Through NTLM relay, an attacker can steal the victim’s credentials, and thus obtain confidential data that the victim could access or call the RPC service that is authorized to control the server, thereby affecting the entire operation of the organization or enterprise.

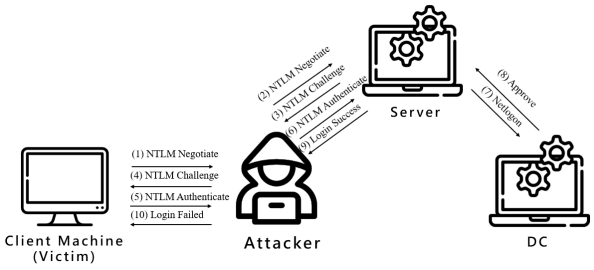

Fig. 2. The NTLM Relay Attack with Active Dictionary

2.3. *NTLM leak*

For the NTLM relay attack, the key relies on how to make the victims actively send a login request to the malicious server. through malicious file is one of the way.

In the article "Living on land: NETNTLM HASHES " introduced those penetrations such as HTML files, PDF,

Window media player, Office files, and others to cause NTLM leakage.

The principle is that when we click on these malicious files, the files actively request resources embedded in the UNC path through the SMB protocol. This sounds reasonable, but when the server located on this path asks for a certificate, the client will actively send the NTLM hash, which is the credential of the victim! Because of Windows integrated authentication, Windows integrated authentication is mainly suitable for users not to repeatedly enter account and password when accessing any resources. This is a great function to save users' time and reduce the possibility of Side-channel attack attacks, but when files need to access resources on a certain UNC path, the Windows operating system. It will consider that the security of these UNC paths has been verified when the file is made, so when the manufactured file is opened again, the file would automatically send the resource query and user credentials if needed.

Usually, those malicious files are sent through attachments in phishing emails. Fortunately, most people, rarely click on the extensions called .m3u .url .jnlp and other rare seen extensions. The most vulnerable types are PDF and office documents because these two file types are also the most common types in daily office work.

Table 1. File Type that Could Cause NTLM Leak.

File Type	File extension
Internet shortcut	url
Windows media player	m3u, asx, wax
Java external jar	jnlp
Microsoft Word	docx, xml
Chrome & IE & Edge	htm
Adobe Acrobat Reader	pdf

3. Our findings

3.1. *Office mitigation*

The NTFS file format supports using the named Zone: Identifier in the alternate data stream to mark files from the Internet. In order to avoid attacks similar to NTLM relay and other malicious code being executed while the file is opened, browsers and other internet clients such as email and chat programs utilize IAttachmentExecute interface's methods or write the Alternate Data Stream directly to mark files from the Internet. If this file happens to be an Office document while opening this Office file, we will see it open in Protected View, Similar to a sandbox to prevent malicious cities from being executed, noticed that the Enable all feature in Protected View is because the files is from the internet. It is different from the Enable Content seen by Macro in the file. In our study refers to the former, which is "Enable all feature".

3.2. *Bypassing Office mitigation*

Although there used to be browsers or Mail Desktop failed to check specific file types, and different determination on dragging downloadable files or double clicking to downloadable files. In other words, if the user dragged a file from Mail Desktop to a folder,the protect mode would be bypassed. However, this type of bypass technique has been patched by most software developers, therefore hackers started to focus on other problems: decompression. When compressed files are decompressing, the unzipped file should inherit the characteristics of Zone:identifer. Although most compression software has noticed this, different compression methods in the same decompress software will have different behaviors. Taking the most common 7zip as an example, it will propagate only when the compressed file is open in archive and double click the file. the article "Downloads and the Mark-of-the-Web" discuss it before, we re-experimented and organized, and found a little different result (Table 2)

Table 2. Popular Extractor List

Extractor	Double-click in Archive	Extract all
Windows Explorer	Not vulnerable	Not vulnerable
WinRar	Not vulnerable	Not vulnerable
7zip	vulnerable	Not vulnerable
WinZip	Not vulnerable	vulnerable
IZArc	Not vulnerable	Not vulnerable

3.3. *Is stealing NTLM hash over other protocol possible?*

The malicious files in table I steal the NTLM hash only through the SMB protocol. However, in the real world, experienced network administrators will prohibit SMB from connecting to the internet. Not only there is usually no related requirement, but to avoid NTLM hash through SMB. While hackers install Responder on the infected employee's computer is not possible to open rogue SMB servers, because that TCP port 445 has been bound by the Network Neighborhood or samba. The responder cannot bind the same port with an existed application. Because of those reasons, we try to insert the resource access path of the HTTP URL path in the Office document. Unfortunately, HTTP Request will be sent out successfully, but when the server responds with an access denied and requested, it uses NTLM for authentication

The client-side usually does not respond in the default settings, but when the client-side computer is set to "Automatic logon with current username and password" In an intranet or trusted site, HTTP will take the initiative to issue an NTLM hash and complete the entire authentication process.

This means that once the hacker hijack a host, and the internal network environment is set to Automatic logon with the current username and password in the intranet, Hackers can steal the credential of the entire intranet by sending spearing fishing e-mail attachments with an HTTP URL path pointing to the infected server through the investigation of the group personnel in the intranet.(Figure 3)

4. Conclusion

IoT devices not only appear in our lives but also enter our work environment. They all make the working environment more convenient and improve the work efficiency of employees. These IoT devices often support NTLM as an identity verification method. Furthermore, to prevent employees from constantly entering account passwords, the device automatically sends the user's identity verification information. Although this saves the user's time to enter the account and password, hackers can also use this authentication method to steal user identity verification information, and use the identity verification information to log in to other devices, This article combines past research results to present our new findings, and further, organize them into a complete attack architecture.

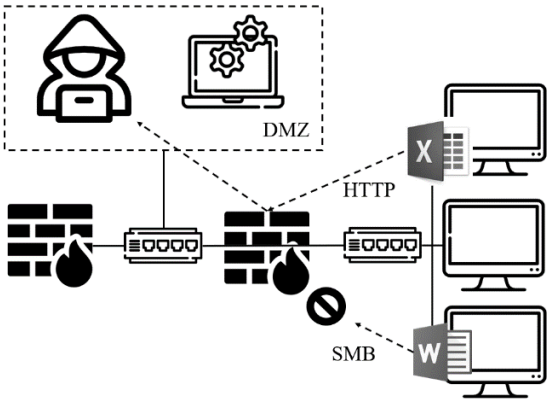

Fig. 3. The Attack Simulation Scenario

Acknowledgements

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract numbers MOST 109-2218-E-006-014- and MOST 109-2218-E-006-510-.

References

1. Jianing Wang and Junyu Zhou, NTLM Relay is dead, Long Live the NTLM Relay, HITBSecConf, 2018.
2. William Mattin, *One-Click to OWA*, DEF CON 26, 2018.
3. Marina Simakov and Yaron Zinar, Relaying Credentials Has Never Been Easier: How To Easily Bypass The Latest NTLM Mitigation, DEF CON 27, 2019.
4. Downloads and the Mark-of-the-Web, 2016
5. I. Ghafir and V. Prenosil and M. Hammoudeh, Dsguised executable files in spear-phishing emails: detecting the point of entry in advanced persistent threat, ICFNDS '18, 2018
6. Mohammed M. Alani, IoT Lotto: Utilizing IoT Devices in Brute-Force Attacks, ICIT 2018: Proceedings of the 6th International Conference on Information Technology: IoT and Smart, pp 140–144, 2018