SECURITY ONION INCIDENT RESPONSE: REMCOS RAT

Group 1

Names	:	Abdur Rashid Firdaus
		Kheyral Sutan Dumas
Class	:	4CS1
Faculty	:	Ivan Firdaus, S.T

CEP CCIT

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

2025

SECURITY ONION INCIDENT RESPONSE:

REMCOS RAT

Batch Code : 4CS1

Start Date : 15th March, 2025

End Date : 24th , 2025

Name of Faculty : Ivan Firdaus, ST

Names of Developer :

1. Abdur Rashid Firdaus
2. Kheyral Sutan Dumas

Date of Submission: 24th March, 2025

ACKNOWLEDGEMENT

Authors would like to praise to Allah, Most Merciful bless and so authors can finish this Project 1 titled “Security Onion Incident Response: Remcos RAT”. Author would like to thank Mr. Ivan Firdaus, ST as Lecturer who has given useful suggestion which helps author in writing this paper.

The contents of this paper provide a detailed overview of a simple incident handling. The paper serves as a way of understanding cyber attack analysis as a subject for this final semester.

SYSTEM ANALYSIS

System Summary:

Incident Response (IR) is the structured approach used by organizations to detect, respond to, and recover from cybersecurity incidents. The goal is to minimize damage, reduce recovery time and costs, and prevent future incidents.

The purpose of this project is to identify any detail about the attack namely Remote Access Trojan attack. By utilizing tools such as sguil and kibana the goal is to find the details of the attack from the alerts provided.

Remcos or Remote Control and Surveillance, marketed as a legitimate software by a Germany-based firm Breaking Security for remotely managing Windows systems is now widely used in multiple malicious campaigns by threat actors. Remcos is a sophisticated remote access Trojan (RAT) that can be used to fully control and monitor any Windows computer from XP and onwards.

INDICATOR OF COMPROMISE

Indicators of Compromise (IoCs):

Remcos RAT Activity:

- **Source IP:** 10.0.90.215
- **C2 Communication:** 103.1.184.108
- **Alert Type:** ET TROJAN Remcos RAT Checkin 23

Dridex Trojan Activity:

- **Source IP:** 31.22.4.176, 203.45.1.75, 115.112.43.81
- **Destination IP:** 10.0.90.215
- **Alert Type:** ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)

Unauthorized Access to Domain Controller (10.0.90.9):

- **Host Identified:** LittleTigers-DC.littletigers.info
- **SMB Activity:**
    - **Source IP:** 10.0.90.215
    - **Destination IP:** 10.0.90.9
    - **Accessed Files:**
        - \LittleTigers-DC.littletigers.info\sysvol\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
        - \LittleTigers-DC\Shared\<share_root>
- **Possible Impact:** Modification of Group Policy Objects (GPOs) for persistence

Suspicious HTTP Requests:

- **Source IP:** 10.0.90.215
- **Destination IPs:** 217.23.14.81, 209.141.34.8
- **Files Requested:** test1.exe, f4.exe
- **Possible Purpose:** Additional malware payloads, secondary infections

ATTACK FLOW

Attack Flow:

Initial Infection via External Download (March 19, 01:45:03 UTC)

- **Source IP:** 10.0.90.215 (infected host)
- **Activity:** Download of executable files: test1.exe and f4.exe from external IPs:
  - test1.exe from 209.141.34.8 → Identified as a **TrojanSpy**.

Remcos RAT Check-in (March 19, 01:47:04 UTC)

- **Source:** 10.0.90.215 → **Destination:** 103.1.184.108
- **Activity:** Outbound connection indicating active **command-and-control (C2) communication**.

Dridex Execution and Second Malicious Download (March 19, 01:49:46 UTC)

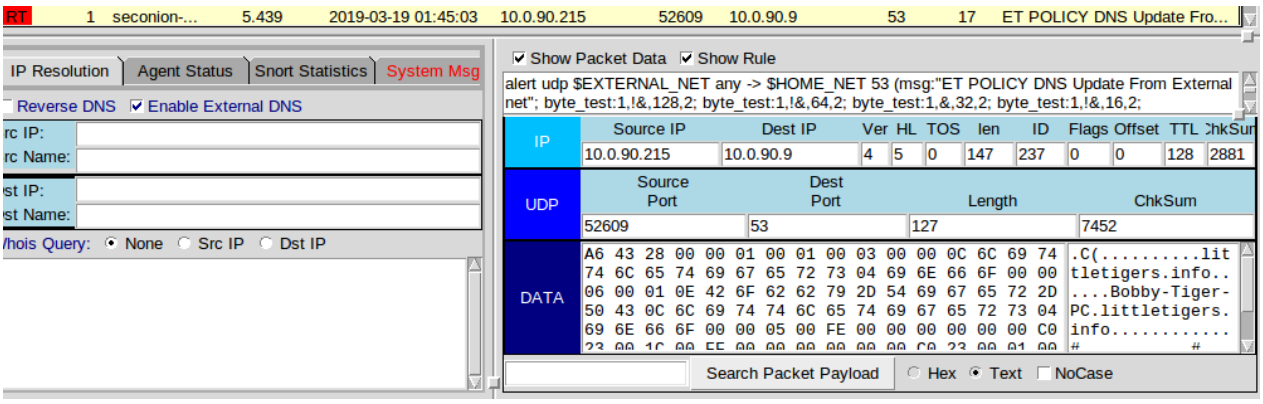
- **Source:** 10.0.90.215 → **Destination:** 217.23.14.81
- **Activity:** Download request for f4.exe, reinforcing the presence of Dridex.

Lateral Movement via SMB (March 19, 01:50 UTC and onward)

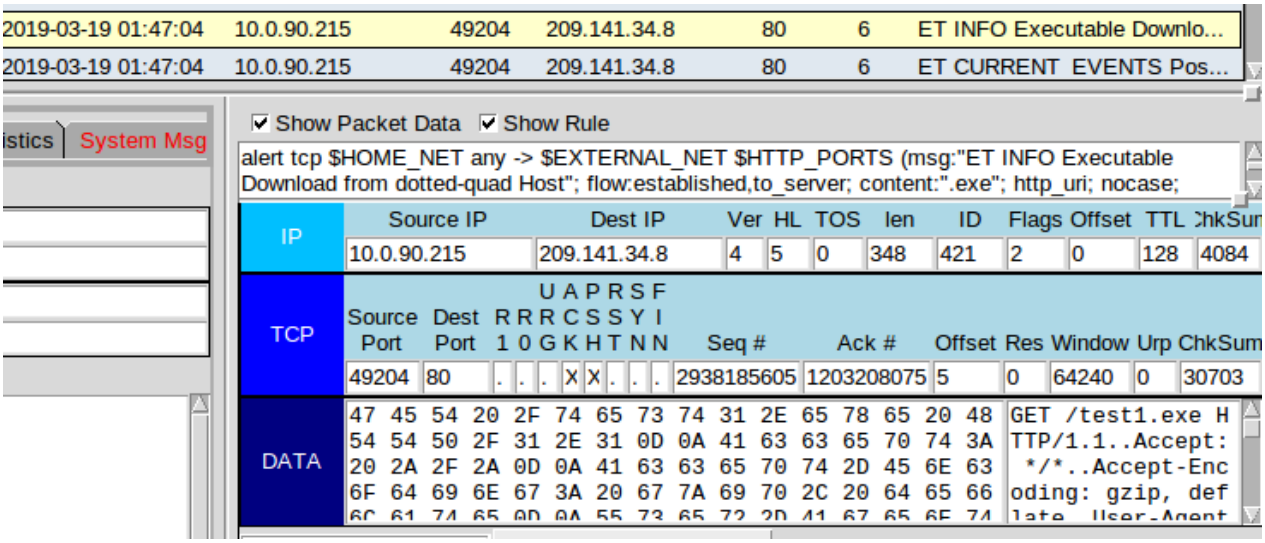
- **Infected host 10.0.90.215** accessed multiple SMB shares on **LittleTigers-DC**:
  - \LittleTigers-DC.littletigers.info\IPC$ (17 times)
  - \LittleTigers-DC.littletigers.info\sysvol (12 times)
  - \LittleTigers-DC\IPC$ (4 times)
  - \LittleTigers-DC\Shared (3 times)
- **Purpose of attack:** Possible **credential theft, reconnaissance, or malware propagation** via:
  - **Pass-the-Hash / Pass-the-Ticket attacks**
  - **Modifying Group Policy Objects (GPOs) in SYSVOL**
  - **Exfiltration of sensitive data from shared directories**

DOCUMENTATION

Initial Infection via External Download (March 19, 01:45:03 UTC)



Remcos RAT Check-in (March 19, 01:47:04 UTC)




```
SRC: GET /test1.exe HTTP/1.1
SRC: Accept: */*
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C;
.NET4.0E)
SRC: Host: 209.141.34.8
SRC: Connection: Keep-Alive
```

DOCUMENTATION

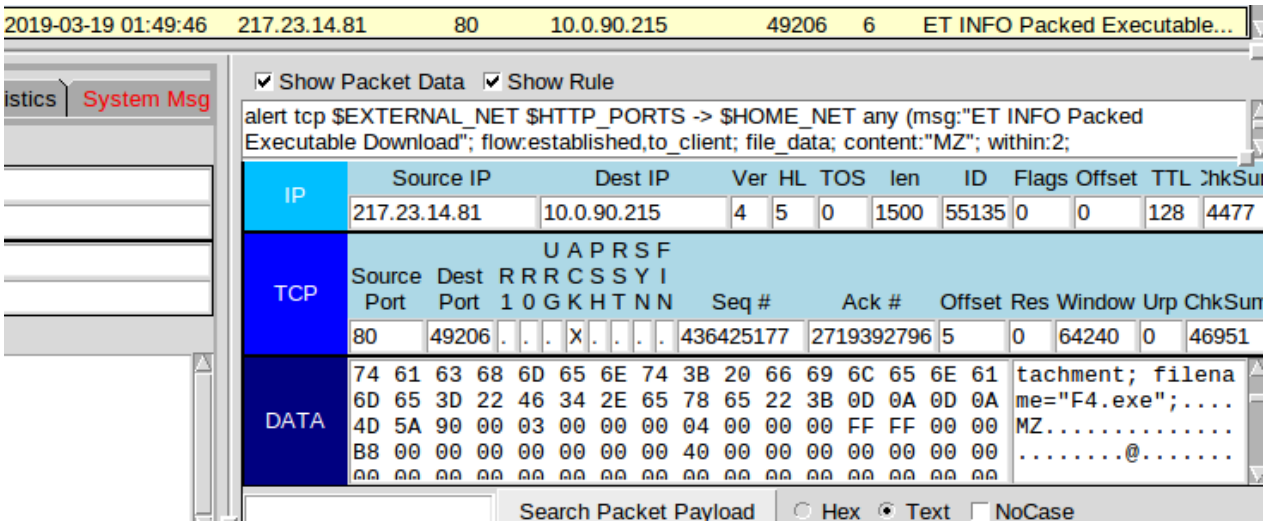
Security alert was triggered indicating a Remcos RAT infection on host 10.0.90.215

Alert	Source IP Address	Destination IP Address	Cou
ET TROJAN Remcos RAT Checkin 23	10.0.90.215	103.1.184.108	404
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	31.22.4.176	10.0.90.215	16
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	203.45.1.75	10.0.90.215	13
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	115.112.43.81	10.0.90.215	3

Additional alerts suggest possible Dridex activity due to SSL certificate detections from known malicious sources

DOCUMENTATION

Dridex Execution and Second Malicious Download (March 19, 01:49:46 UTC)




```
Sensor Name: seconion-import-1
Timestamp: 2019-03-19 01:49:46
Connection ID: .seconion-import-1_482
Src IP:          10.0.90.215
Dst IP:          217.23.14.81
Src Port:        49206
Dst Port:        80
OS Fingerprint: 10.0.90.215:49206 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 217.23.14.81:80 (distance 0, link: ethernet/modem)

SRC: GET /f4.exe HTTP/1.1
SRC: Accept: */*
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C;
.NET4.0E)
SRC: Host: 217.23.14.81
SRC: Connection: Keep-Alive
SRC:
SRC:
```

DOCUMENTATION

The test1.exe revealed to be a spyware trojan

talosintelligence.com/sha_searches

FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256

2A9B0ED40F1F0BC0C13FF35D304689E9CADD633781CBCAD1C2D2B92CED3F1C85

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	811520 bytes
SAMPLE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
CISCO SECURE ENDPOINT DETECTION NAME*	Remcos::gravity::Win.Dropper.Vbkryjetor::in03.talos

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

[TROJAN] Trojan/Win32.Generic.C3113109

detected

Win32:Evo-gen [Trj]

Trojan.GenericKD.42036511

win/malicious_confidence_100

malware.confidence_100

Trojan.Siggen8.18466

The f4.exe revealed to be a dridex

FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256

5865E801E6324166D6D05B39A14F2A8A798C6EB652831F78C2634F2B7A400EAF

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	176128 bytes
SAMPLE TYPE	PE32 executable (console) Intel 80386, for MS Windows
CISCO SECURE ENDPOINT DETECTION NAME*	Win.Dropper.Cridex::1201

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

[TROJAN] Trojan/Win.Generic.R457226

detected

Win32:Trojan-gen

Trojan.Downloader.JUPC

win/malicious_confidence_100

malware.confidence_100

Trojan.Siggen8.19138

malicious (high confidence)

Detected

DOCUMENTATION

10.0.90.215 accessed 10.0.90.9 via SMB, interacting with critical SYSVOL files.

SMB - Source IP Address

IP Address	Count
10.0.90.215	36

SMB - Destination IP Address

IP Address	Count
10.0.90.9	36

SMB - File/Path Summary

File Path	File Name	Action	Source IP Address	Destination IP Address	Count
\\LittleTigers-DC.littletigers.info\sysvol	littletigers.info\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini	SMB::FILE_OPEN	10.0.90.215	10.0.90.9	6
\\LittleTigers-DC\Shared	<share_root>	SMB::FILE_OPEN	10.0.90.215	10.0.90.9	1

SMB - File Path

File Path	Count
\\LittleTigers-DC.littletigers.info\IPC$	17
\\LittleTigers-DC.littletigers.info\sysvol	12
\\LittleTigers-DC\IPC$	4
\\LittleTigers-DC\Shared	3

SMB - Destination Port

Destination Port	Count
445	36

SUMMARY

This attack leveraged multiple infection techniques, including malware downloads, RAT-based persistence, and lateral movement through SMB exploitation. The ultimate goal appears to be credential theft and data exfiltration. Immediate action is required to contain and remediate the breach while enhancing security controls to prevent future incidents.

This attack is targeting a Windows-based corporate network with an Active Directory infrastructure. The attackers are likely aiming to:

- Steal credentials (possibly domain admin access).
- Exfiltrate sensitive data (especially financial info).
- Spread further in the network via Dridex and SMB.

Mitigation Recommendations

- Isolate 10.0.90.215 from the network immediately.
- Reset all potentially compromised credentials, especially domain admin accounts.
- Deploy endpoint detection scans on 10.0.90.9 and other high-risk machines.

CONFIGURATION

Hardware: ASUS Laptop

Operating System: Windows 11, Security Onion VM

Software: Microsoft Word, Google Chrome

PROJECT FILE DETAILS

No	File Name	Remarks
1	Project 2 Group 1.pdf	Abdur Rashid Firdaus
2	Project 2 Group 1.pkt (Powerpoint)	Kheyral Sutan Dumas