Free Automated Malware Analysis Service - powered by Falcon Sandbox

Archived: 2026-04-02 11:31:02 UTC

Incident Response

Risk Assessment

Persistence

Grants permissions using icacls (DACL modification)

Spawns a lot of processes

Writes data to a remote process

Network Behavior

Contacts 1 domain and 5326 hosts. View all details

MITRE ATT&CK™ Techniques Detection

This report has 11 indicators that were mapped to 15 attack techniques and 6 tactics. View all details

Additional Context

OSINT

External References

https://hexcoderblog.wordpress.com/2018/04/17/honeypot-research-the-notable-speeds-of-malicious-targeting/

External User Tags

#honeypot #malware

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

- External Systems
  - Detected Suricata Alert

    details

    Detected alert "ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1" (SID: 2024298, Rev: 4, Severity: 1) categorized as "A Network Trojan was detected" (PUA/PUP/Adware)
    Detected alert "ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)" (SID: 2025649, Rev: 3, Severity: 1) categorized as "A Network Trojan was detected"
    Detected alert "ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)" (SID: 2025992, Rev: 2, Severity: 1) categorized as "A Network Trojan was detected"

    source

    Suricata Alerts

    relevance

    10/10
  - Sample was identified as malicious by a large number of Antivirus engines

    details

    64/70 Antivirus vendors marked sample as malicious (91% detection rate)

    source

    External System

    relevance

    10/10
  - Sample was identified as malicious by at least one Antivirus engine

    details

    64/70 Antivirus vendors marked sample as malicious (91% detection rate)

    source

    External System

    relevance

    8/10
- General
  - The analysis extracted a file that was identified as malicious

    details

58/67 Antivirus vendors marked dropped file "MSSECSVC.EXE.6038B8CC.bin" as malicious (classified as "CVE-2017-0147" with 86% detection rate)
66/71 Antivirus vendors marked dropped file "TASKSCHE.EXE.6038BB10.bin" as malicious (classified as "Trojan.Ransom.WannaCryptor" with 92% detection rate)
66/71 Antivirus vendors marked dropped file "tasksche.exe" as malicious (classified as "Trojan.Ransom.WannaCryptor" with 92% detection rate)
58/67 Antivirus vendors marked dropped file "mssecsvc.exe" as malicious (classified as "CVE-2017-0147" with 86% detection rate)
14/59 Antivirus vendors marked dropped file "m_dutch.wnry" as malicious (classified as "Trojan.Filecoder" with 23% detection rate)
15/60 Antivirus vendors marked dropped file "m_finnish.wnry" as malicious (classified as "Trojan.Filecoder" with 25% detection rate)
16/61 Antivirus vendors marked dropped file "m_vietnamese.wnry" as malicious (classified as "Trojan.Filecoder" with 26% detection rate)
12/59 Antivirus vendors marked dropped file "m_turkish.wnry" as malicious (classified as "Trojan.Filecoder" with 20% detection rate)
12/59 Antivirus vendors marked dropped file "m_russian.wnry" as malicious (classified as "Trojan.Filecoder" with 20% detection rate)
14/60 Antivirus vendors marked dropped file "m_indonesian.wnry" as malicious (classified as "Trojan.Filecoder" with 23% detection rate)
18/61 Antivirus vendors marked dropped file "m_italian.wnry" as malicious (classified as "Trojan.Filecoder" with 29% detection rate)
15/60 Antivirus vendors marked dropped file "m_french.wnry" as malicious (classified as "Trojan.Filecoder" with 25% detection rate)
17/61 Antivirus vendors marked dropped file "m_chinese _traditional_.wnry" as malicious (classified as "Trojan.Filecoder" with 27% detection rate)
14/60 Antivirus vendors marked dropped file "m_spanish.wnry" as malicious (classified as "Trojan.Filecoder" with 23% detection rate)
15/61 Antivirus vendors marked dropped file "m_portuguese.wnry" as malicious (classified as "Trojan.Filecoder" with 24% detection rate)

source
Binary File

relevance
10/10

- The analysis spawned a process that was identified as malicious

details
58/67 Antivirus vendors marked spawned process "mssecsvc.exe" (PID: 3240) as malicious (classified as "CVE-2017-0147" with 86% detection rate)
58/67 Antivirus vendors marked spawned process "mssecsvc.exe" (PID: 2796) as malicious (classified as "CVE-2017-0147" with 86% detection rate)
66/71 Antivirus vendors marked spawned process "tasksche.exe" (PID: 2740) as malicious (classified as "Trojan.Ransom.WannaCryptor" with 92% detection rate)
66/71 Antivirus vendors marked spawned process "tasksche.exe" (PID: 3732) as malicious (classified as "Trojan.Ransom.WannaCryptor" with 92% detection rate)
66/71 Antivirus vendors marked spawned process "tasksche.exe" (PID: 1336) as malicious (classified as "Trojan.Ransom.WannaCryptor" with 92% detection rate)

source
Monitored Target

relevance
10/10

- Installation/Persistence
  - Writes data to a remote process

details
"rundll32.exe" wrote 32 bytes to a remote process "C:\Windows\mssecsvc.exe" (Handle: 212)
"rundll32.exe" wrote 52 bytes to a remote process "C:\Windows\mssecsvc.exe" (Handle: 212)
"rundll32.exe" wrote 4 bytes to a remote process "C:\Windows\mssecsvc.exe" (Handle: 212)
"mssecsvc.exe" wrote 32 bytes to a remote process "C:\Windows\tasksche.exe" (Handle: 720)
"mssecsvc.exe" wrote 52 bytes to a remote process "C:\Windows\tasksche.exe" (Handle: 720)
"mssecsvc.exe" wrote 4 bytes to a remote process "C:\Windows\tasksche.exe" (Handle: 720)
"tasksche.exe" wrote 32 bytes to a remote process "%ALLUSERSPROFILE%\tvzfcptuxgtlf819\tasksche.exe" (Handle: 140)
"tasksche.exe" wrote 52 bytes to a remote process "C:\ProgramData\tvzfcptuxgtlf819\tasksche.exe" (Handle: 140)
"tasksche.exe" wrote 4 bytes to a remote process "C:\ProgramData\tvzfcptuxgtlf819\tasksche.exe"

(Handle: 140)
"tasksche.exe" wrote 32 bytes to a remote process "C:\Windows\System32\icacls.exe" (Handle: 136)
"tasksche.exe" wrote 52 bytes to a remote process "C:\Windows\System32\icacls.exe" (Handle: 136)
"tasksche.exe" wrote 4 bytes to a remote process "C:\Windows\System32\icacls.exe" (Handle: 136)
"tasksche.exe" wrote 32 bytes to a remote process "C:\Windows\System32\attrib.exe" (Handle: 136)
"tasksche.exe" wrote 52 bytes to a remote process "C:\Windows\System32\attrib.exe" (Handle: 136)
"tasksche.exe" wrote 4 bytes to a remote process "C:\Windows\System32\attrib.exe" (Handle: 136)
"tasksche.exe" wrote 32 bytes to a remote process "C:\Windows\System32\attrib.exe" (Handle: 64)
"tasksche.exe" wrote 52 bytes to a remote process "C:\Windows\System32\attrib.exe" (Handle: 64)
"tasksche.exe" wrote 4 bytes to a remote process "C:\Windows\System32\attrib.exe" (Handle: 64)
"tasksche.exe" wrote 32 bytes to a remote process "C:\Windows\System32\icacls.exe" (Handle: 64)
"tasksche.exe" wrote 52 bytes to a remote process "C:\Windows\System32\icacls.exe" (Handle: 64)
"tasksche.exe" wrote 4 bytes to a remote process "C:\Windows\System32\icacls.exe" (Handle: 64)

source
API Call

relevance
6/10

ATT&CK ID
T1055 (Show technique in the MITRE ATT&CK™ matrix)

- Network Related
  - Contacts very many different hosts

  details
  Contacted 60 (or more) hosts in at least 19 different countries

  source
  Network Traffic

  relevance
  9/10
- Pattern Matching
  - YARA signature match

  details
  YARA signature "MS17_010_WanaCry_worm" classified file "22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "PC NETWORK PROGRAM 1.0,LANMAN1.0,Windows for Workgroups 3.1a,__TREEID__PLACEHOLDER__,__USERID__PLACEHOLDER__,h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j,h54WfF9cGigW (Reference: https://www.exploit-db.com/exploits/41987/, Author: Felipe Molina (@felmoltor))
  YARA signature "WannaDecryptor" classified file "22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "taskdl.exe,taskse.exe,r.wnry,s.wnry,t.wnry,u.wnry,msg/m_"
  YARA signature "WannaCry_RansomwareEx" classified file "22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "icacls . /grant Everyone:F /T /C /Q,taskdl.exe,tasksche.exe,Global\MsWinZonesCacheCounterMutexA,WNcry@2ol7,www.iuqerfsodp9ifjaposdfjhgosurijfaewrwerg Windows 10 --> ,cmd.exe /c "%s",msg/m_portuguese.wnry,5c005c003100390032002e003100360038002e00350036002e00320030005c00490050004300240 (Reference: https://goo.gl/HG2j5T, Author: Florian Roth (with the help of binar.ly))
  YARA signature "WannaDecryptor" classified file "tasksche.exe" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "taskdl.exe,taskse.exe,r.wnry,s.wnry,t.wnry,u.wnry,msg/m_"
  YARA signature "WannaCry_RansomwareEx" classified file "tasksche.exe" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "icacls . /grant Everyone:F /T /C /Q,taskdl.exe,tasksche.exe,Global\MsWinZonesCacheCounterMutexA,WNcry@2ol7, Windows 10 --> ,cmd.exe /c "%s",msg/m_portuguese.wnry,09ff763050ff562c5959473b7e0c7c,c1ea1dc1ee1e83e20183e6018d1456,8d48fff7d18d4410ff23f123c (Reference: https://goo.gl/HG2j5T, Author: Florian Roth (with the help of binar.ly))
  YARA signature "WannaDecryptor" classified file "TASKSCHE.EXE.6038BB10.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "taskdl.exe,taskse.exe,r.wnry,s.wnry,t.wnry,u.wnry,msg/m_"
  YARA signature "WannaCry_RansomwareEx" classified file "TASKSCHE.EXE.6038BB10.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "icacls . /grant Everyone:F /T /C /Q,taskdl.exe,tasksche.exe,Global\MsWinZonesCacheCounterMutexA,WNcry@2ol7, Windows 10 --> ,cmd.exe /c "%s",msg/m_portuguese.wnry,09ff763050ff562c5959473b7e0c7c,c1ea1dc1ee1e83e20183e6018d1456,8d48fff7d18d4410ff23f123c

(Reference: https://goo.gl/HG2j5T, Author: Florian Roth (with the help of binar.ly))
YARA signature "MS17_010_WanaCry_worm" classified file "MSSECSVC.EXE.6038B8CC.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "PC NETWORK PROGRAM 1.0,LANMAN1.0,Windows for Workgroups 3.1a,__TREEID__PLACEHOLDER__,__USERID__PLACEHOLDER__,h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j,h54WfF9cGigW
(Reference: https://www.exploit-db.com/exploits/41987/, Author: Felipe Molina (@felmoltor))
YARA signature "WannaDecryptor" classified file "MSSECSVC.EXE.6038B8CC.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "taskdl.exe,taskse.exe,r.wnry,s.wnry,t.wnry,u.wnry,msg/m_"
YARA signature "WannaCry_RansomwareEx" classified file "MSSECSVC.EXE.6038B8CC.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "icacls . /grant Everyone:F /T /C /Q,taskdl.exe,tasksche.exe,Global\MsWinZonesCacheCounterMutexA,WNcry@2ol7,www.iuqerfsodp9ifjaposdfjhgosurijfaewrwerg
Windows 10 --> ,cmd.exe /c "%s",msg/m_portuguese.wnry,5c005c003100390032002e003100360038002e00350036002e00320030005c004900500043002400,5c
(Reference: https://goo.gl/HG2j5T, Author: Florian Roth (with the help of binar.ly))
YARA signature "WannaCry_Ransomware_Gen" classified file "MSSECSVC.EXE.6038B8CC.bin" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "__TREEID__PLACEHOLDER__,__USERID__PLACEHOLDER__,Windows for Workgroups 3.1a,PC NETWORK PROGRAM 1.0,LANMAN1.0" (Reference: https://www.us-cert.gov/ncas/alerts/TA17-132A, Author: Florian Roth (based on rule by US CERT))
YARA signature "MS17_010_WanaCry_worm" classified file "mssecsvc.exe" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "PC NETWORK PROGRAM 1.0,LANMAN1.0,Windows for Workgroups 3.1a,__TREEID__PLACEHOLDER__,__USERID__PLACEHOLDER__,h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j,h54WfF9cGigW
(Reference: https://www.exploit-db.com/exploits/41987/, Author: Felipe Molina (@felmoltor))
YARA signature "WannaDecryptor" classified file "mssecsvc.exe" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "taskdl.exe,taskse.exe,r.wnry,s.wnry,t.wnry,u.wnry,msg/m_"
YARA signature "WannaCry_RansomwareEx" classified file "mssecsvc.exe" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "icacls . /grant Everyone:F /T /C /Q,taskdl.exe,tasksche.exe,Global\MsWinZonesCacheCounterMutexA,WNcry@2ol7,www.iuqerfsodp9ifjaposdfjhgosurijfaewrwerg
Windows 10 --> ,cmd.exe /c "%s",msg/m_portuguese.wnry,5c005c003100390032002e003100360038002e00350036002e00320030005c004900500043002400,5c
(Reference: https://goo.gl/HG2j5T, Author: Florian Roth (with the help of binar.ly))
YARA signature "WannaCry_Ransomware_Gen" classified file "mssecsvc.exe" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "__TREEID__PLACEHOLDER__,__USERID__PLACEHOLDER__,Windows for Workgroups 3.1a,PC NETWORK PROGRAM 1.0,LANMAN1.0" (Reference: https://www.us-cert.gov/ncas/alerts/TA17-132A, Author: Florian Roth (based on rule by US CERT))
YARA signature "MS17_010_WanaCry_worm" classified file "all.bstring" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "PC NETWORK PROGRAM 1.0,LANMAN1.0,Windows for Workgroups 3.1a,__TREEID__PLACEHOLDER__,__USERID__PLACEHOLDER__,h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j,h54WfF9cGigW
(Reference: https://www.exploit-db.com/exploits/41987/, Author: Felipe Molina (@felmoltor))
YARA signature "WannaDecryptor" classified file "all.bstring" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "taskdl.exe,taskse.exe,msg/m_"
YARA signature "WannaCry_Ransomware_Gen" classified file "all.bstring" as "ransomware,wcry,wannacry,wanacrypt0r" based on indicators: "__TREEID__PLACEHOLDER__,__USERID__PLACEHOLDER__,Windows for Workgroups 3.1a,PC NETWORK PROGRAM 1.0,LANMAN1.0" (Reference: https://www.us-cert.gov/ncas/alerts/TA17-132A, Author: Florian Roth (based on rule by US CERT))

source
YARA Signature

relevance
10/10

- System Security
  - Modifies the access control lists of files

  details
  Process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)
  Process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)

  source
  Monitored Target

  relevance
  5/10

ATT&CK ID

T1044 (Show technique in the MITRE ATT&CK™ matrix)

- Unusual Characteristics
  - Checks for a resource fork (ADS) file

  details

  "mssecsvc.exe" checked file "C:"

  source

  API Call

  relevance

  5/10
  - Spawns a lot of processes

  details

  Spawned process "mssecsvc.exe" (Show Process)
  Spawned process "mssecsvc.exe" with commandline "-m security" (Show Process)
  Spawned process "tasksche.exe" with commandline "/i" (Show Process)
  Spawned process "tasksche.exe" (Show Process)
  Spawned process "tasksche.exe" (Show Process)
  Spawned process "attrib.exe" with commandline "attrib +h ." (Show Process)
  Spawned process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)
  Spawned process "attrib.exe" with commandline "attrib +h ." (Show Process)
  Spawned process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)

  source

  Monitored Target

  relevance

  8/10
- Hiding 4 Malicious Indicators
  - All indicators are available only in the private webservice or standalone version
- Anti-Reverse Engineering
  - PE file has unusual entropy sections

  details

  .rsrc
  .rsrc with unusual entropies 7.71095306051
  7.72627063923

  source

  Static Parser

  relevance

  10/10
- External Systems
  - Found an IP/URL artifact that was identified as malicious by at least one reputation engine

  details

  4/84 reputation engines marked "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" as malicious (4% detection rate)

  source

  External System

  relevance

  10/10
- Installation/Persistence
  - Chained signature (with api-8701...). Detects file write then launch as EXE

  details

  Chained signature (with api-8701...). Detects file write then launch as EXE

  source

  API Call

  relevance

  8/10
  - Creates new processes

  details

  "rundll32.exe" is creating a new process (Name: "%WINDIR%\mssecsvc.exe", Handle: 212)
  "mssecsvc.exe" is creating a new process (Name: "%WINDIR%\tasksche.exe", Handle: 720)
  "tasksche.exe" is creating a new process (Name: "%ALLUSERSPROFILE%\tvzfcptuxgtlf819\tasksche.exe", Handle: 140)
  "tasksche.exe" is creating a new process (Name: "%WINDIR%\System32\attrib.exe", Handle: 136)
  "tasksche.exe" is creating a new process (Name: "%WINDIR%\System32\icacls.exe", Handle: 136)
  "tasksche.exe" is creating a new process

"tasksche.exe" is creating a new process (Name: "%WINDIR%\System32\icacls.exe", Handle: 64)
"tasksche.exe" is creating a new process (Name: "%WINDIR%\System32\attrib.exe", Handle: 64)

source
API Call

relevance
8/10

- Drops executable files

details
"MSSECSVC.EXE.6038B8CC.bin" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"TASKSCHE.EXE.6038BB10.bin" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"tasksche.exe" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"mssecsvc.exe" has type "PE32 executable (GUI) Intel 80386 for MS Windows"

source
Binary File

relevance
10/10

- Network Related
  - Found potential IP address in binary/memory

details
Potential IP "192.168.56.20" found in string "\\192.168.56.20\IPC$"

source
File/Memory

relevance
3/10

  - Sends traffic on typical HTTP outbound port, but without HTTP header

details
TCP traffic to 104.16.173.80 on port 80 is sent without HTTP header

source
Network Traffic

relevance
5/10

ATT&CK ID
T1043 (Show technique in the MITRE ATT&CK™ matrix)

- System Security
  - Modifies proxy settings

details
"mssecsvc.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYENABLE"; Value: "00000000")
"mssecsvc.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYSERVER")
"mssecsvc.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYOVERRIDE")
"mssecsvc.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")
"mssecsvc.exe" (Access type: "DELETEVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")
"mssecsvc.exe" (Access type: "SETVAL"; Path: "HKU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYENABLE"; Value: "00000000")
"mssecsvc.exe" (Access type: "DELETEVAL"; Path: "HKU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYSERVER")
"mssecsvc.exe" (Access type: "DELETEVAL"; Path: "HKU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYOVERRIDE")
"mssecsvc.exe" (Access type: "DELETEVAL"; Path: "HKU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")

source

Registry Access

relevance

10/10

ATT&CK ID

T1112 (Show technique in the MITRE ATT&CK™ matrix)

- Unusual Characteristics
  - Imports suspicious APIs

    details

    CreateProcessA
    LockResource
    WriteFile
    CreateFileA
    FindResourceA
    CreateServiceA
    StartServiceA
    StartServiceCtrlDispatcherA
    GetModuleFileNameA
    GetStartupInfoA
    GetFileSize
    GetProcAddress
    GetModuleHandleA
    GetModuleHandleW
    Sleep
    GetTickCount
    InternetOpenUrlA
    InternetCloseHandle
    InternetOpenA
    socket
    recv
    send
    WSAStartup
    connect
    closesocket
    RegCloseKey
    RegCreateKeyW
    LoadLibraryA
    GetFileAttributesA
    CopyFileA
    VirtualProtect
    GetFileAttributesW
    CreateDirectoryA
    CreateDirectoryW
    GetComputerNameW
    GetFileSizeEx
    GetTempPathW
    TerminateProcess
    VirtualAlloc

    source

    Static Parser

    relevance

    1/10

  - Installs hooks/patches the running process

    details

    "rundll32.exe" wrote bytes "88eadc761656dd7681ecdc764557dc763105dc76ca9edc76cda6dc768220d876000000009498cd7651c1cd76ee9ccd76ec32d77654d3 to virtual address "0x10002000" (part of module "2A8EFBFADD798F6111340F7C1C956BEE.DLL")
    "mssecsvc.exe" wrote bytes "e7393577e1a639772e713977ee29397785e234776da03977906438773ad53f7726e43477d16d3977003d3777804b377700000000ad3 to virtual address "0x74C01000" (part of module "WSHIP6.DLL")
    "mssecsvc.exe" wrote bytes "f8110000" to virtual address "0x750D12CC" (part of module "SSPICLI.DLL")
    "mssecsvc.exe" wrote bytes "f8110d75" to virtual address "0x750E834C" (part of module "SSPICLI.DLL")
    "mssecsvc.exe" wrote bytes "f8110000" to virtual address "0x750D1408" (part of module

"SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "b89012036fffe0" to virtual address "0x750D1248" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "48120d75" to virtual address "0x750E8348" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "f8110d75" to virtual address "0x750E8368" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "68130000" to virtual address "0x75871680" (part of module "WS2_32.DLL")
"mssecsvc.exe" wrote bytes "f8110d75" to virtual address "0x750E83C4" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "48120d75" to virtual address "0x750E8364" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "fae63477e1a639772e713977ee29397785e234776da0397726e43477d16d3977003d3777804b377700000000ad3787758b2d8775b64 to virtual address "0x746B1000" (part of module "WSHTCPIP.DLL")
"mssecsvc.exe" wrote bytes "48120d75" to virtual address "0x750E83C0" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "f8110d75" to virtual address "0x750E83E0" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "b88011036fffe0" to virtual address "0x75871368" (part of module "WS2_32.DLL")
"mssecsvc.exe" wrote bytes "48120000" to virtual address "0x750D139C" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "48120000" to virtual address "0x750D12DC" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "a011036f" to virtual address "0x7715E324" (part of module "WININET.DLL")
"mssecsvc.exe" wrote bytes "48120d75" to virtual address "0x750E83DC" (part of module "SSPICLI.DLL")
"mssecsvc.exe" wrote bytes "b81015036fffe0" to virtual address "0x750D11F8" (part of module "SSPICLI.DLL")

source
Hook Detection
relevance
10/10
ATT&CK ID
T1179 (Show technique in the MITRE ATT&CK™ matrix)

- Hiding 2 Suspicious Indicators
  - All indicators are available only in the private webservice or standalone version

- External Systems
  - Detected Suricata Alert

    details
    Detected alert "ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection" (SID: 2001569, Rev: 15, Severity: 3) categorized as "Misc activity"

    source
    Suricata Alerts
    relevance
    10/10
- General
  - Contacts domains

    details
    "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"

    source
    Network Traffic
    relevance
    1/10
  - Contacts server

    details
    "104.16.173.80:80"
    "123.119.235.225:445"
    "171.243.141.156:445"
    "22.190.114.199:445"

"19.28.211.242:445"
"51.187.114.224:445"
"80.93.187.33:445"
"191.7.5.28:445"
"74.66.141.75:445"
"72.55.56.162:445"
"182.74.141.79:445"
"66.120.107.41:445"
"112.61.249.78:445"
"159.170.228.202:445"
"41.61.70.132:445"
"161.154.238.120:445"
"207.194.34.20:445"
"207.27.9.151:445"
"47.143.47.147:445"
"106.131.54.225:445"

source
Network Traffic

relevance
1/10

- Creates mutants

details
"\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex"
"Local\ZonesCacheCounterMutex"
"Local\ZonesLockedCacheCounterMutex"
"\BaseNamedObjects\Local\ZonesCacheCounterMutex"
"\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex"

source
Created Mutant

relevance
3/10

- GETs files from a webserver

details
"GET / HTTP/1.1
Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Cache-Control: no-cache"

source
Network Traffic

relevance
5/10

- Process launched with changed environment

details
Process "mssecsvc.exe" (Show Process) was launched with modified environment variables: "Path, LOCALAPPDATA, USERDOMAIN, TEMP, APPDATA, USERPROFILE, TMP"
Process "mssecsvc.exe" (Show Process) was launched with missing environment variables: "LOGONSERVER, HOMEPATH, HOMEDRIVE"
Process "tasksche.exe" (Show Process) was launched with new environment variables: "LOGONSERVER="\\HAPUBWS-PC", HOMEPATH="\Users\BoXuzF2", HOMEDRIVE="C:""
Process "tasksche.exe" (Show Process) was launched with modified environment variables: "Path, LOCALAPPDATA, USERDOMAIN, TEMP, APPDATA, USERPROFILE, TMP"
Process "tasksche.exe" (Show Process) was launched with new environment variables: "PROMPT="PG""
Process "tasksche.exe" (Show Process) was launched with modified environment variables: "Path, LOCALAPPDATA, USERDOMAIN, TEMP, APPDATA, USERPROFILE, TMP"
Process "tasksche.exe" (Show Process) was launched with missing environment variables: "LOGONSERVER, HOMEPATH, HOMEDRIVE"
Process "tasksche.exe" (Show Process) was launched with new environment variables: "LOGONSERVER="\\HAPUBWS-PC", HOMEPATH="\Users\BoXuzF2", HOMEDRIVE="C:""
Process "tasksche.exe" (Show Process) was launched with modified environment variables: "Path, LOCALAPPDATA, USERDOMAIN, TEMP, APPDATA, USERPROFILE, TMP"
Process "tasksche.exe" (Show Process) was launched with missing environment variables: "PROMPT"

source
Monitored Target

relevance
10/10

- Spawns new processes

details
Spawned process "rundll32.exe" with commandline ""C:\2a8efbfadd798f6111340f7c1c956bee.dll",#1" (Show Process)
Spawned process "mssecsvc.exe" (Show Process)
Spawned process "mssecsvc.exe" with commandline "-m security" (Show Process)
Spawned process "tasksche.exe" with commandline "/i" (Show Process)
Spawned process "tasksche.exe" (Show Process)
Spawned process "tasksche.exe" (Show Process)
Spawned process "attrib.exe" with commandline "attrib +h ." (Show Process)
Spawned process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)
Spawned process "attrib.exe" with commandline "attrib +h ." (Show Process)
Spawned process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)

source
Monitored Target

relevance
3/10

- Spawns new processes that are not known child processes

details
Spawned process "rundll32.exe" with commandline ""C:\2a8efbfadd798f6111340f7c1c956bee.dll",#1" (Show Process)
Spawned process "mssecsvc.exe" (Show Process)
Spawned process "mssecsvc.exe" with commandline "-m security" (Show Process)
Spawned process "tasksche.exe" with commandline "/i" (Show Process)
Spawned process "tasksche.exe" (Show Process)
Spawned process "tasksche.exe" (Show Process)
Spawned process "attrib.exe" with commandline "attrib +h ." (Show Process)
Spawned process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)
Spawned process "attrib.exe" with commandline "attrib +h ." (Show Process)
Spawned process "icacls.exe" with commandline "icacls . /grant Everyone:F /T /C /Q" (Show Process)

source
Monitored Target

relevance
3/10

- The input sample possibly contains the RDTSCP instruction

details
Found VM detection artifact "RDTSCP trick" in "22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6.bin" (Offset: 774762)

source
Binary File

relevance
5/10

ATT&CK ID
T1497 (Show technique in the MITRE ATT&CK™ matrix)

- Installation/Persistence
  - Dropped files

details
"MSSECSVC.EXE.6038B8CC.bin" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"TASKSCHE.EXE.6038BB10.bin" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"tasksche.exe" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"mssecsvc.exe" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"m_dutch.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_finnish.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_vietnamese.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_turkish.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_russian.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_indonesian.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_italian.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_french.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_chinese _traditional_.wnry" has type "Rich Text Format data version 1 unknown character set"
"m_spanish.wnry" has type "Rich Text Format data version 1 unknown character set"

"m_portuguese.wnry" has type "Rich Text Format data version 1 unknown character set"
"c.wnry" has type "data"

source
Binary File

relevance
3/10

- Touches files in the Windows directory

details
"rundll32.exe" touched file "%WINDIR%\AppPatch\sysmain.sdb"
"rundll32.exe" touched file "%WINDIR%\System32\rundll32.exe"
"rundll32.exe" touched file "%WINDIR%\AppPatch\AcLayers.dll"
"rundll32.exe" touched file "%WINDIR%\mssecsvc.exe"
"rundll32.exe" touched file "%WINDIR%\System32\en-US\rundll32.exe.mui"
"mssecsvc.exe" touched file "%APPDATA%\Microsoft\Windows\Cookies"
"mssecsvc.exe" touched file "%APPDATA%\Microsoft\Windows\Cookies\FZD0P3G2.txt"
"mssecsvc.exe" touched file "%WINDIR%\tasksche.exe"
"mssecsvc.exe" touched file "%WINDIR%\AppPatch\sysmain.sdb"

source
API Call

relevance
7/10

- Network Related
  - Found potential URL in binary/memory

details
Pattern match: "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
Pattern match: "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
Pattern match: "http://schemas.microsoft.com/o"
Pattern match: "http://schemas.microsoft.com/office/word/2003/wordml}}\paperw12240\paperh15840\margl1501\margr1502\margt1701\margb144
Pattern match: "http://schemas.microsoft.com/office/word/2003/wordml}}\paperw12240\paperh15840\margl1034\margr1034\margt1701\margb144
Pattern match: "http://schemas.microsoft"

source
File/Memory

relevance
10/10

- Unusual Characteristics
  - Matched Compiler/Packer signature

details
"22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6.bin" was detected as "Microsoft visual C++ 6.0 DLL"
"MSSECSVC.EXE.6038B8CC.bin" was detected as "Microsoft visual C++ 5.0"
"TASKSCHE.EXE.6038BB10.bin" was detected as "Microsoft visual C++ 5.0"

source
Static Parser

relevance
10/10

ATT&CK ID
T1045 (Show technique in the MITRE ATT&CK™ matrix)

File Details

All Details:

2a8efbfadd798f6111340f7c1c956bee

File Sections

Details	Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5
Name .text Entropy	.text	1.44299712447	0x1000	0x28c	0x1000	8de9a2cb31e4c74bd008b871

Details	Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5
1.44299712447 Virtual Address 0x1000 Virtual Size 0x28c Raw Size 0x1000 MD5 8de9a2cb31e4c74bd008b871d14bfafc						
Name .rdata Entropy 0.734601813362 Virtual Address 0x2000 Virtual Size 0x1d8 Raw Size 0x1000 MD5 3dd394f95ab218593f2bc8eb65184db4	.rdata	0.734601813362	0x2000	0x1d8	0x1000	3dd394f95ab218593f2bc8eb6
Name .data Entropy 0.0852386864133 Virtual Address 0x3000 Virtual Size 0x154 Raw Size 0x1000 MD5 fe5022c5b5d015ad38b2b77fc437a5cb	.data	0.0852386864133	0x3000	0x154	0x1000	fe5022c5b5d015ad38b2b77fc
Name .rsrc Entropy 6.10865289671 Virtual Address 0x4000 Virtual Size 0x500060 Raw Size 0x501000 MD5 f016d5edc700b1685a0bdcec7c83cea4	.rsrc	6.10865289671	0x4000	0x500060	0x501000	f016d5edc700b1685a0bdcec7
Name .reloc Entropy 0 Virtual Address 0x505000 Virtual Size 0x2ac Raw Size	.reloc	0	0x505000	0x2ac	0x1000	620f0b67a91f7f74151bc5be7

Details	Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5
0x1000 MD5 620f0b67a91f7f74151bc5be745b7110						

File Resources

File Imports

- KERNEL32.dll
- MSVCRT.dll

File Exports

Screenshots

Data couldn't be loaded. Please try again.

- CPU Usage
- Committed Bytes
- Disk Read Bytes/sec
- Disk Write Bytes/sec
- Network Packets/sec
- Page File Bytes

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 10 processes in total (System Resource Monitor).

Network Analysis

This report was generated with enabled TOR analysis

DNS Requests

HTTP Traffic

Suricata Alerts

ET rules applied using Suricata. Find out more about proofpoint ET Intelligence here.

Extracted Files

Displaying 24 extracted file(s). The remaining **47** file(s) are available in the full version and XML/JSON reports.

Warnings

- A process crash was detected during the runtime analysis
- Enforcing malicious verdict, as a reliable source indicates high confidence
- Network whitenoise filtering was applied
- Not all sources for indicator ID "api-55" are available in the report
- Not all sources for indicator ID "binary-0" are available in the report
- Not all sources for indicator ID "hooks-8" are available in the report
- Not all sources for indicator ID "mutant-0" are available in the report
- Not all sources for indicator ID "network-1" are available in the report
- Not all sources for indicator ID "network-17" are available in the report
- Some low-level data is hidden, as this is only a slim report

---