ID: 323808
Sample Name:
CoYUNxCu9sAz7iQ.exe
Cookbook: default.jbs
Time: 15:23:30
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

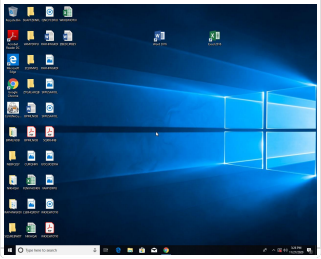
Analysis Report CoYUNxCu9sAz7iQ.exe

Overview

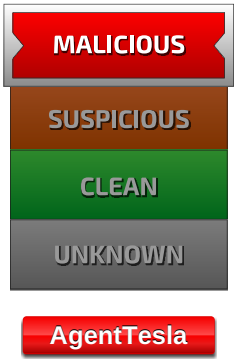
General Information

Sample Name:	CoYUNxCu9sAz7iQ.exe
Analysis ID:	323808
MD5:	4651a16a7a526e..
SHA1:	35c54c7553ceefc..
SHA256:	01818bdf9166323.
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

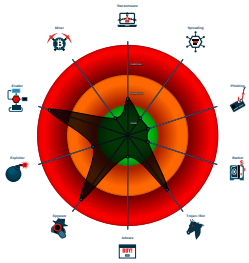


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- Contains functionality to register a lo…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- CoYUNxCu9sAz7iQ.exe (PID: 4532 cmdline: 'C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe' MD5: 4651A16A7A526EA71500C4E740D1B445)
  - schtasks.exe (PID: 3068 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FOPVbE' /XML 'C:\Users\user\AppData\Local\Temp\tmp7077.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - CoYUNxCu9sAz7iQ.exe (PID: 5956 cmdline: {path} MD5: 4651A16A7A526EA71500C4E740D1B445)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "OLNf4ayHpxAP",
  "URL: ": "http://Tu6Zp5Arx4D.com",
  "To: ": "laty.lambo101@yandex.com",
  "ByHost: ": "mail.nusatek.com:587",
  "Password: ": "uTERCX",
  "From: ": "salina@nusatek.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.610111498.000000000333 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.366830433.00000000036C 7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.365603212.000000000266 D000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.367073975.000000000384 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.609123676.000000000303 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 5 entries				

Unpacked PEs

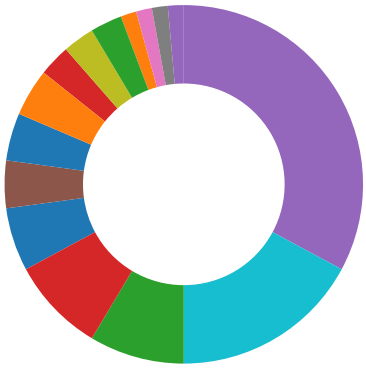
Source	Rule	Description	Author	Strings
3.2.CoYUNxCu9sAz7iQ.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

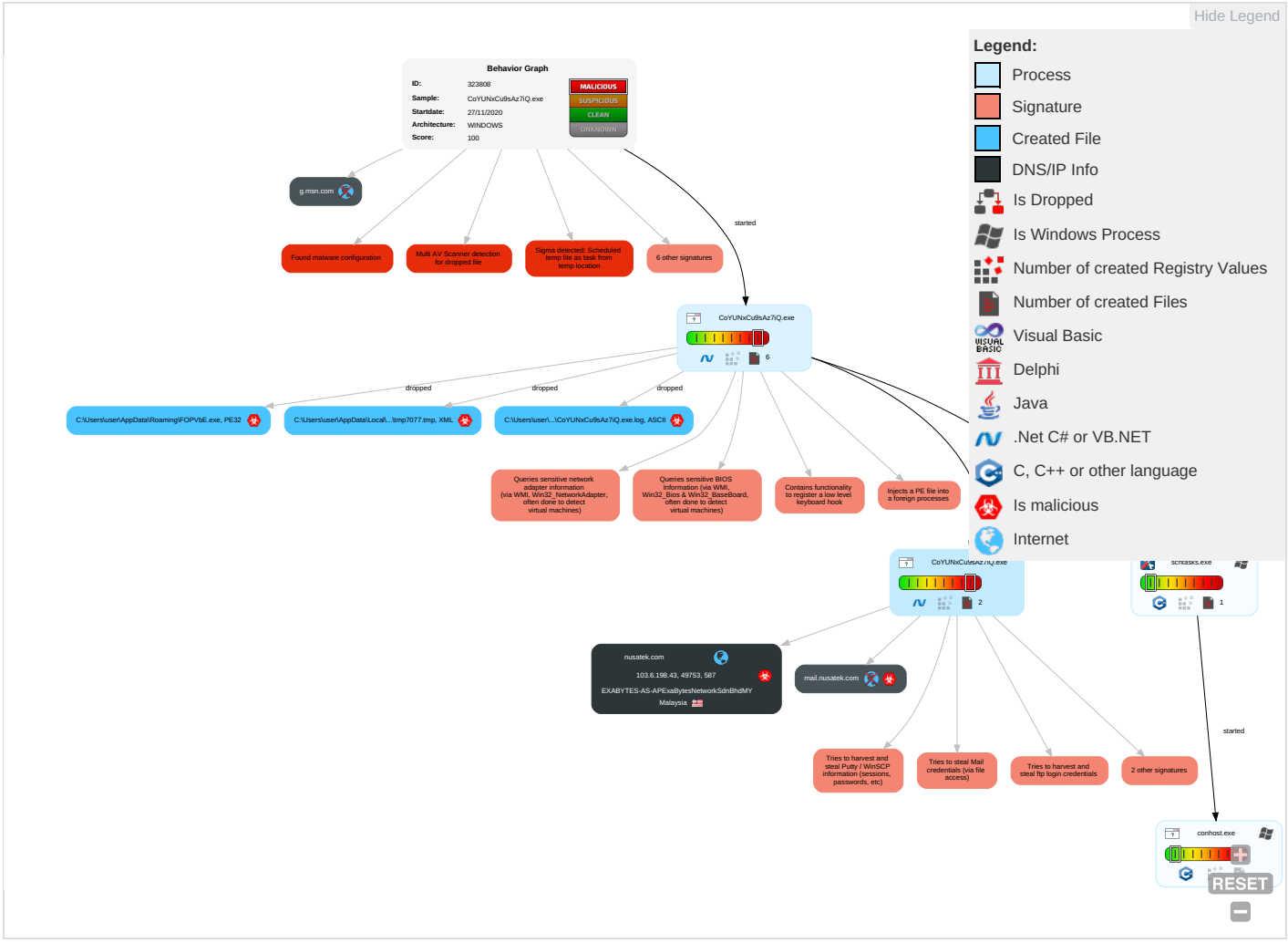
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Obfuscated Files or Information 3	Input Capture 2 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	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	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

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
CoYUNxCu9sAz7iQ.exe	60%	Virustotal		Browse
CoYUNxCu9sAz7iQ.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\FOPVbE.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.CoYUNxCu9sAz7iQ.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
nusatek.com	0%	Virustotal		Browse
mail.nusatek.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	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.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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	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.carterandcone.coml	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	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.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.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.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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.tiro.comn-u	0%	Avira URL Cloud	safe	
http://nusatek.com	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	
http://Tu6Zp5Arx4D.com	0%	Avira URL Cloud	safe	
http://mail.nusatek.com	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://xUHTrW.com	0%	Avira URL Cloud	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	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nusatek.com	103.6.198.43	true	true	• 0%, Virustotal, Browse	unknown
g.msn.com	unknown	unknown	false		high
mail.nusatek.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

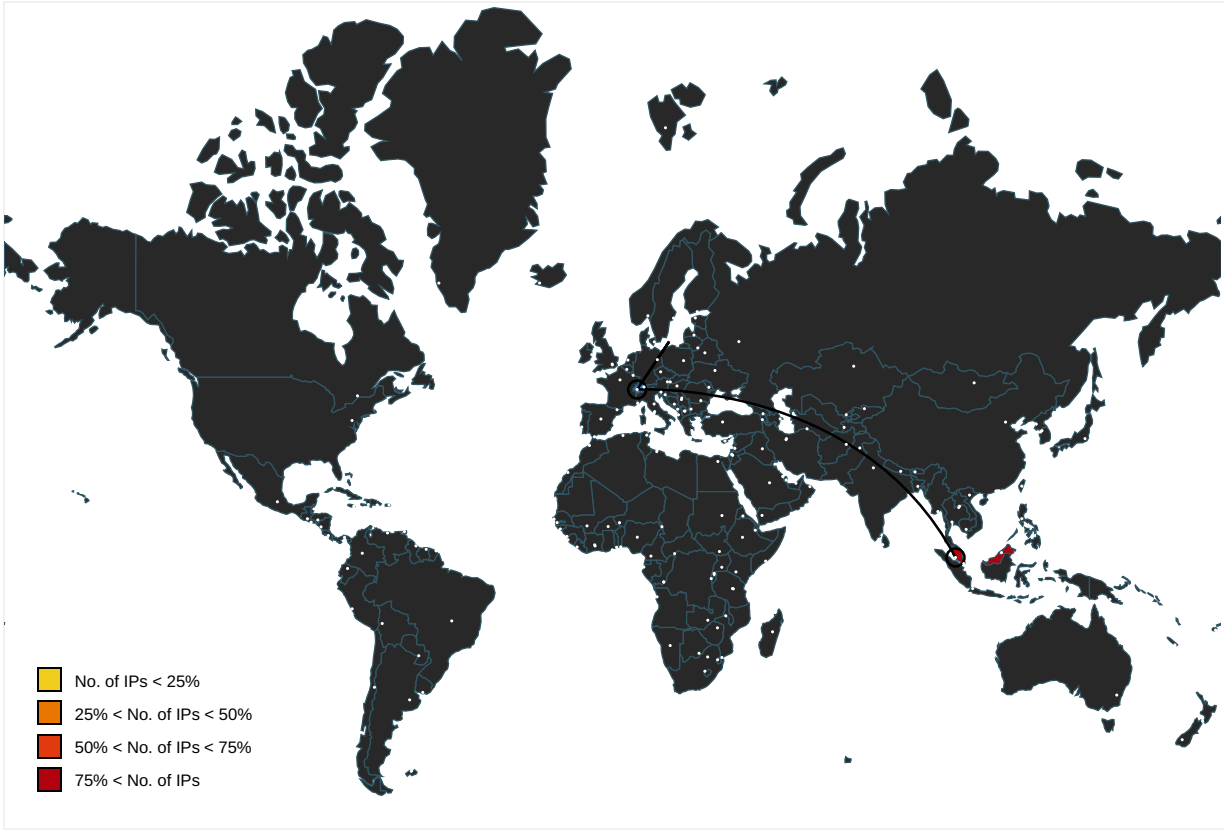
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.609123676.0000000003031000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000005570000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000005570000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000005570000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.609123676.0000000003031000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.613928909.0000000006440000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.609123676.000000000331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false		high
http://www.tiro.com	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.365389915.0000000000CC7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.come.com	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.365389915.0000000000CC7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.609123676.000000000331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.000000000570000.00000002.00000001.sdmp	false		high
http://www.tiro.comn-u	CoYUNxCu9sAz7iQ.exe, 00000000.00000003.344294408.0000000000CCC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.366830433.000000000036C7000.00000004.00000001.sdmp, CoYUNxCu9sAz7iQ.exe, 00000003.00000002.606845898.000000000402000.00000040.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://nusatek.com	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.610420870.0000000033 93000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Tu6Zp5Arx4D.com	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.610111498.0000000033 35000.00000004.00000001.sdmp, CoYUNxCu9sAz7iQ.exe, 00000003.00000002.610550515.0000000033 BF000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://mail.nusatek.com	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.610420870.0000000033 93000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false		high
http://www.fonts.com	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://xUHTrW.com	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.609123676.0000000030 31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.365603212.0000000026 6D000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.369526004.0000000055 70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	CoYUNxCu9sAz7iQ.exe, 00000003.00000002.609123676.0000000030 31000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	CoYUNxCu9sAz7iQ.exe, 00000000.00000002.366830433.0000000036 C7000.00000004.00000001.sdmp, CoYUNxCu9sAz7iQ.exe, 00000003.00000002.606845898.0000000004 02000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.6.198.43	unknown	Malaysia		46015	EXABYTES-AS-APExaBytesNetworkSdnBhdMY	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323808
Start date:	27.11.2020
Start time:	15:23:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CoYUNxCu9sAz7iQ.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:	24
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.spyw.evad.winEXE@6/3@3/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, wermgr.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 51.104.144.132, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 40.67.251.132, 52.147.198.201, 52.142.114.176, 92.122.213.247, 92.122.213.194, 52.154.66.52, 52.154.67.2, 52.154.67.48, 52.154.66.239, 52.224.75.92, 52.154.67.56, 104.79.90.110 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, blu-eap-main-ips-v4only.b.lg.prod.aadmsa.trafficmanager.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, db5p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:24:33	API Interceptor	777x Sleep call for process: CoYUNxCu9sAz7iQ.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.6.198.43	JRN7EZAZ.EXE	Get hash	malicious	Browse	
	zGyEJygJdB9gQUU.exe	Get hash	malicious	Browse	
	SGVVGTQI.EXE	Get hash	malicious	Browse	
	DQ0lO8gVkO.exe	Get hash	malicious	Browse	
	5GVTZR5R.EXE	Get hash	malicious	Browse	
	gHw9MlUsKBbvwaP.exe	Get hash	malicious	Browse	
	JpzOOD0oTm.exe	Get hash	malicious	Browse	
	l9Z33XjGakOIOoH.exe	Get hash	malicious	Browse	
	4Yn6GnIPrbXA7vi.exe	Get hash	malicious	Browse	
	4Yn6GnIPrbXA7vi.exe	Get hash	malicious	Browse	
	XG8UDAIJ.EXE	Get hash	malicious	Browse	
	Y6HpqlElKD0lLoa.exe	Get hash	malicious	Browse	
	f5l39y4FB2DX7aM.exe	Get hash	malicious	Browse	
	UPWQTZDV.EXE	Get hash	malicious	Browse	
	bPlvM3WldzoADDa.exe	Get hash	malicious	Browse	
	QIVUQCMF.EXE	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EXABYTES-AS-APExaBytesNetworkSdnBhdMY	2281.xls	Get hash	malicious	Browse	• 103.6.196.179
	2281.xls	Get hash	malicious	Browse	• 103.6.196.179
	Invoice_Payment Form_163142.xlsm	Get hash	malicious	Browse	• 110.4.45.148
	Original Shipment Document.exe	Get hash	malicious	Browse	• 110.4.45.145
	JRN7EZAZ.EXE	Get hash	malicious	Browse	• 103.6.198.43
	7nFOggQ2PE.exe	Get hash	malicious	Browse	• 103.6.196.121
	8zQf02MJSy.exe	Get hash	malicious	Browse	• 103.6.196.156
	j470QOQdWq.exe	Get hash	malicious	Browse	• 103.6.196.121
	zGyEJygJdB9gQUU.exe	Get hash	malicious	Browse	• 103.6.198.43
	SGVVGTQI.EXE	Get hash	malicious	Browse	• 103.6.198.43
	G4lV5bMc0l.exe	Get hash	malicious	Browse	• 103.6.196.156
	DQ0lO8gVkO.exe	Get hash	malicious	Browse	• 103.6.198.43
	HoQ00lJBmx.exe	Get hash	malicious	Browse	• 103.6.196.121
	D5rekL72q0.exe	Get hash	malicious	Browse	• 103.6.196.156
	Information du octobre 2020.doc	Get hash	malicious	Browse	• 110.4.47.219
	5GVTZR5R.EXE	Get hash	malicious	Browse	• 103.6.198.43
	egskZqWRhqoU0fJ.exe	Get hash	malicious	Browse	• 103.6.196.156
	eJQspuSPzUmj5H4.exe	Get hash	malicious	Browse	• 103.6.196.156
	Sztuis104rOKP2P.exe	Get hash	malicious	Browse	• 103.6.196.156
	http://https://www.rehdainstitute.com/.well-known/RFT/c2xvbmdpbkByZXZlbnVld2VsbC5jb20=	Get hash	malicious	Browse	• 110.4.43.99

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CoYUNxCu9sAz7iQ.exe.log

Process:	C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CoYUNxCu9sAz7iQ.exe.log

Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp7077.tmp

Process:	C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.158412337470319
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3pHtn:cbha7JlNQV/rydbz9l3YODOLNdq3DN
MD5:	CC524AE00308E9D28F7C17F0C3BEA972
SHA1:	7AC144F6B5E1E3B6A3D9854A311BDBC2306BE70D
SHA-256:	09F7B20150CAB3275EB9AFB58441190D324730F5345A8F2E22F0F2513E3DD997
SHA-512:	9A609CDF5516D201EDD641402CA5BB556A8E31421445799C68202B239B31583A9AE0FC94C3E19D3C6291E13BEA5F23EDB4C3E63DCBEDED405B66B8D0B17BA24A
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\FOPVbE.exe

Process:	C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	526848
Entropy (8bit):	7.727874815455438
Encrypted:	false
SSDEEP:	12288:V+b4KO3VrN2iNUPzvUuFxrNso8E7osJRkq3rat8LF:gb4KO3BN1WPzdFEozlvrG8
MD5:	4651A16A7A526EA71500C4E740D1B445
SHA1:	35C54C7553CEEFC195DA495916D063C0D0B78429
SHA-256:	01818BDF91663237419FAE1F1C7613108A4321D9E354478DF9A90D091126AD92
SHA-512:	607A15A9D550AED91712EE852F3B1B955BAABDAFB276FF302C64AB7DA81065059EB7411E24159FC16ACB5F559DE28D69ADBADCD283496E10AB34F03DA6525F61
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 48%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O._.....0.....D.....f.... .....@.. ....@.....O.....A.....`..... ..... ..H.....text...l.... ..... ..`.rsrc....A.....B.....@..@.rel oc.....`.....@..B.....H.....H.....r...c.....x...L.....0..G.....}.....(.....(.....s....}.....{.....o.....(.....{....{....o....*..0.....(.....{....{....(.... ...(....~....vl.....,{....{....o.....{....{....o....o.....{....(....}.....o.....3..{....{....o.....+....,@..{....{....o....s.....{....{....{....o.....{....{....o.....*...{....(...o!.....{....~....o"....*...{....(#...o!.....{.... ~....o"....*...0..+.....,..{.....+....,...{.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.727874815455438
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	CoYUNxCu9sAz7iQ.exe
File size:	526848
MD5:	4651a16a7a526ea71500c4e740d1b445
SHA1:	35c54c7553ceefc195da495916d063c0d0b78429
SHA256:	01818bdf91663237419fae1f1c7613108a4321d9e354478df9a90d091126ad92
SHA512:	607a15a9d550aed91712ee852f3b1b955baabdafb276ff302c64ab7da81065059eb7411e24159fc16acb5f559de28c69adbadcd283496e10ab34f03da6525f61
SSDEEP:	12288:V+b4KO3VrN2iNUPzvUuFxrNso8E7osJRkq3rat8LF:gb4KO3BN1WPzdFEozlvrG8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O._.....0.....D.....f.... .....@.. .....@.....

File Icon

Icon Hash:	061b331d55675307

Static PE Info

General

Entrypoint:	0x47e266
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBF4FA6 [Thu Nov 26 06:48:06 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

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7e214	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x80000	0x418c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7c26c	0x7c400	False	0.837456378898	data	7.7396642698	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x418c	0x4200	False	0.596117424242	data	5.50871998012	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x80190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x805f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967039, next used block 4294967295		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x816a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0x83c48	0x30	data		
RT_VERSION	0x83c78	0x328	data		
RT_MANIFEST	0x83fa0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

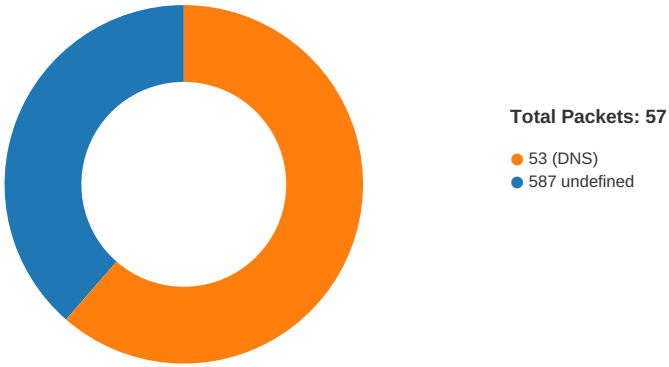
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 - 2020
Assembly Version	1.0.0.0
InternalName	8S.exe
FileVersion	1.0.0.0
CompanyName	Vendetta Inc.
LegalTrademarks	
Comments	
ProductName	Aku Form
ProductVersion	1.0.0.0
FileDescription	Aku Form
OriginalFilename	8S.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/27/20-15:25:11.692530	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:26:22.669672012 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:22.992970943 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:22.993104935 CET	49753	587	192.168.2.6	103.6.198.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:26:23.815403938 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:23.816065073 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:24.139399052 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:24.140218019 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:24.469810009 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:24.523279905 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:24.553596973 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:24.892113924 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:24.892149925 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:24.892168045 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:24.892180920 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:24.892271042 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:24.892318010 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:24.896862030 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:24.945151091 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:24.953711033 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:25.277616024 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:25.320189953 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:25.598146915 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:25.922080040 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:25.926378965 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:26.250798941 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:26.253868103 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:26.616332054 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:26.620827913 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:26.622385025 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:26.945966959 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:26.946738005 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:27.272370100 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:27.273055077 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:27.596244097 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:27.598881960 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:27.599049091 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:27.599800110 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:27.599934101 CET	49753	587	192.168.2.6	103.6.198.43
Nov 27, 2020 15:26:27.922245979 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:27.922281981 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:27.922611952 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:27.923075914 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:27.936120987 CET	587	49753	103.6.198.43	192.168.2.6
Nov 27, 2020 15:26:27.976623058 CET	49753	587	192.168.2.6	103.6.198.43

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:24:20.468957901 CET	60261	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:24:20.496216059 CET	53	60261	8.8.8.8	192.168.2.6
Nov 27, 2020 15:24:21.285037994 CET	56061	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:24:21.312120914 CET	53	56061	8.8.8.8	192.168.2.6
Nov 27, 2020 15:24:22.102268934 CET	58336	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:24:22.129487991 CET	53	58336	8.8.8.8	192.168.2.6
Nov 27, 2020 15:24:25.155627012 CET	53781	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:24:25.191222906 CET	53	53781	8.8.8.8	192.168.2.6
Nov 27, 2020 15:24:48.007899046 CET	54064	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:24:48.035337925 CET	53	54064	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:06.875039101 CET	52811	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:06.914865971 CET	53	52811	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:07.471039057 CET	55299	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:07.506573915 CET	53	55299	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:07.952738047 CET	63745	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:07.979890108 CET	53	63745	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:08.282535076 CET	50055	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:08.317938089 CET	53	50055	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:08.662797928 CET	61374	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:25:08.678622961 CET	50339	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:08.698225975 CET	53	61374	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:08.705697060 CET	53	50339	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:08.719943047 CET	63307	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:08.757446051 CET	53	63307	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:09.097336054 CET	49694	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:09.132934093 CET	53	49694	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:09.583522081 CET	54982	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:09.619036913 CET	53	54982	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:10.249325037 CET	50010	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:11.244841099 CET	50010	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:11.690782070 CET	53	50010	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:11.692442894 CET	53	50010	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:12.285501003 CET	63718	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:12.321007013 CET	53	63718	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:13.031722069 CET	62116	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:13.051517010 CET	63816	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:13.067358017 CET	53	62116	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:13.078581095 CET	53	63816	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:13.498667955 CET	55014	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:13.534315109 CET	53	55014	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:13.707174063 CET	62208	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:13.734375954 CET	53	62208	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:14.789650917 CET	57574	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:14.816862106 CET	53	57574	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:15.560677052 CET	51818	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:15.596460104 CET	53	51818	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:16.248910904 CET	56628	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:16.292251110 CET	53	56628	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:17.457845926 CET	60778	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:17.485085964 CET	53	60778	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:20.056134939 CET	53799	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:20.083307981 CET	53	53799	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:21.494687080 CET	54683	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:21.531594038 CET	53	54683	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:22.015125990 CET	59329	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:22.042256117 CET	53	59329	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:22.669127941 CET	64021	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:22.704682112 CET	53	64021	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:40.696990013 CET	56129	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:40.724000931 CET	53	56129	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:41.276238918 CET	58177	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:41.303311110 CET	53	58177	8.8.8.8	192.168.2.6
Nov 27, 2020 15:25:51.543215036 CET	50700	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:25:51.580598116 CET	53	50700	8.8.8.8	192.168.2.6
Nov 27, 2020 15:26:12.316112995 CET	54069	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:26:12.343128920 CET	53	54069	8.8.8.8	192.168.2.6
Nov 27, 2020 15:26:21.706056118 CET	61178	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:26:22.053304911 CET	53	61178	8.8.8.8	192.168.2.6
Nov 27, 2020 15:26:22.377428055 CET	57017	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:26:22.532567978 CET	53	57017	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 27, 2020 15:25:11.692529917 CET	192.168.2.6	8.8.8.8	d077	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:25:16.248910904 CET	192.168.2.6	8.8.8.8	0x617	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:21.706056118 CET	192.168.2.6	8.8.8.8	0xab5b	Standard query (0)	mail.nusatek.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:26:22.377428055 CET	192.168.2.6	8.8.8.8	0x67b	Standard query (0)	mail.nusatek.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:25:16.292251110 CET	8.8.8.8	192.168.2.6	0x617	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:26:22.053304911 CET	8.8.8.8	192.168.2.6	0xab5b	No error (0)	mail.nusatek.com	nusatek.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:26:22.053304911 CET	8.8.8.8	192.168.2.6	0xab5b	No error (0)	nusatek.com		103.6.198.43	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:22.532567978 CET	8.8.8.8	192.168.2.6	0x67b	No error (0)	mail.nusatek.com	nusatek.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:26:22.532567978 CET	8.8.8.8	192.168.2.6	0x67b	No error (0)	nusatek.com		103.6.198.43	A (IP address)	IN (0x0001)

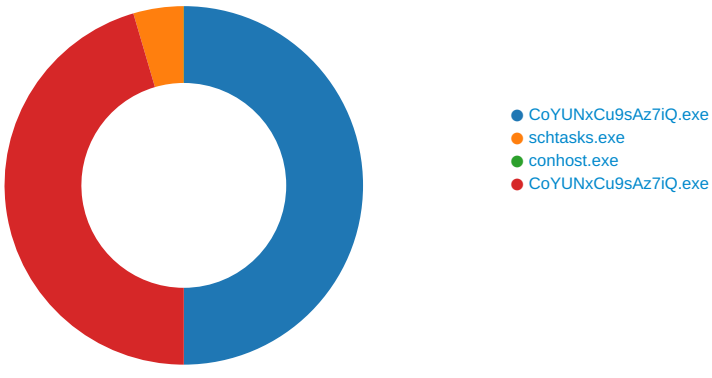
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 15:26:23.815403938 CET	587	49753	103.6.198.43	192.168.2.6	220-sambal.mschosting.com ESMTP Exim 4.93 #2 Fri, 27 Nov 2020 22:26:22 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 15:26:23.816065073 CET	49753	587	192.168.2.6	103.6.198.43	EHLO 468325
Nov 27, 2020 15:26:24.139399052 CET	587	49753	103.6.198.43	192.168.2.6	250-sambal.mschosting.com Hello 468325 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 15:26:24.140218019 CET	49753	587	192.168.2.6	103.6.198.43	STARTTLS
Nov 27, 2020 15:26:24.469810009 CET	587	49753	103.6.198.43	192.168.2.6	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: CoYUNxCu9sAz7iQ.exe PID: 4532 Parent PID: 4604

General

Start time:	15:24:25
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe'
Imagebase:	0x210000
File size:	526848 bytes
MD5 hash:	4651A16A7A526EA71500C4E740D1B445
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.366830433.00000000036C7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.365603212.000000000266D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.367073975.0000000003840000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	unknown
C:\Users\user\AppData\Roaming\FOPVbE.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF11E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp7077.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CoYUNxCu9sAz7iQ.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7077.tmp	success or wait	1	6CF16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FOPVbE.exe	unknown	526848	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 a6 4f bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 c4 07 00 00 44 00 00 00 00 00 00 66 e2 07 00 00 20 00 00 00 00 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....O._..... ....0.....D.....f.... .....@.. ....@.....	success or wait	1	6CF11B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp7077.tmp	unknown	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registratio	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CoYUNxCu9sAz7iQ.exe.log	unknown	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe	unknown	526848	success or wait	1	6CF11B4F	ReadFile

Analysis Process: schtasks.exe PID: 3068 Parent PID: 4532

General

Start time:	15:24:34
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FOPVbE' /XML 'C:\Users\user\AppData\Local\Temp\tmp7077.tmp'
Imagebase:	0x13c0000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7077.tmp	unknown	2	success or wait	1	13CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7077.tmp	unknown	1652	success or wait	1	13CABD9	ReadFile

Analysis Process: conhost.exe PID: 3528 Parent PID: 3068

General

Start time:	15:24:35
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: CoYUNxCu9sAz7iQ.exe PID: 5956 Parent PID: 4532

General

Start time:	15:24:35
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\CoYUNxCu9sAz7iQ.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xca0000
File size:	526848 bytes
MD5 hash:	4651A16A7A526EA71500C4E740D1B445
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.610111498.0000000003335000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.609123676.0000000003031000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.606845898.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ddd58f9c-e25a-4366-ba96-8d423210d7dd	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF11B4F	ReadFile

Disassembly

Code Analysis