ID: 679299
Sample Name: s0VxndYXq0
Cookbook: default.jbs
Time: 14:59:08
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

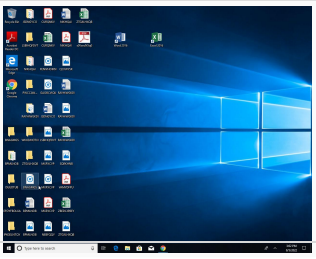
Windows Analysis Report

s0VxndYXq0

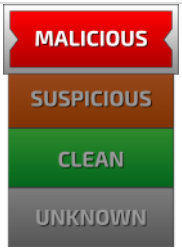
Overview

General Information

Sample Name:	s0VxndYXq0 (renamed file extension from none to exe)
Analysis ID:	679299
MD5:	de9784a4f56eaf8.
SHA1:	35c361a8bfdb89..
SHA256:	f384a96582763b..
Tags:	exe
Infos:	



Detection



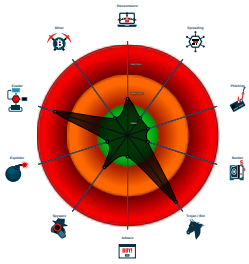
Remcos

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Remcos RAT
- Antivirus / Scanner detection for sub…
- Detected Remcos RAT
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Uses ping.exe to check the status o…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- s0VxndYXq0.exe (PID: 2732 cmdline: "C:\Users\user\Desktop\s0VxndYXq0.exe" MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
  - s0VxndYXq0.exe (PID: 3264 cmdline: C:\Users\user\Desktop\s0VxndYXq0.exe MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
    - cmd.exe (PID: 3704 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\install.bat" " MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 3708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - PING.EXE (PID: 5088 cmdline: PING 127.0.0.1 -n 2 MD5: 70C24A306F768936563ABDADB9CA9108)
      - remcos.exe (PID: 3908 cmdline: "C:\Users\user\remcos\remcos.exe" MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
        - remcos.exe (PID: 1924 cmdline: C:\Users\user\remcos\remcos.exe MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
        - remcos.exe (PID: 5456 cmdline: C:\Users\user\remcos\remcos.exe MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
        - remcos.exe (PID: 3572 cmdline: C:\Users\user\remcos\remcos.exe MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
- remcos.exe (PID: 5540 cmdline: "C:\Users\user\remcos\remcos.exe" MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
  - remcos.exe (PID: 5580 cmdline: C:\Users\user\remcos\remcos.exe MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
- remcos.exe (PID: 4776 cmdline: "C:\Users\user\remcos\remcos.exe" MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
  - remcos.exe (PID: 5832 cmdline: C:\Users\user\remcos\remcos.exe MD5: DE9784A4F56EAF8AFFC96754A15A5CD3)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "79.134.225.97:8600:123456|",
  "Assigned name": "Host",
  "Connect interval": "5",
  "Install flag": "Enable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "User Profile",
  "Copy file": "remcos.exe",
  "Startup value": "remcos",
  "Hide file": "Disable",
  "Mutex": "remcos_totevzugmgbhhbj",
  "Keylog flag": "0",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "1",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screens",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "audio",
  "Connect delay": "0",
  "Copy folder": "remcos",
  "Keylog folder": "remcos"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
s0VxndYXq0.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\remcos\remcos.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.351406709.0000000002FDB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0000000C.00000002.351406709.0000000002FDB000.00000004.00000800.00020000.00000000.sdmp	Remcos	detect Remcos in memory	JPCERT/CC Incident Response Group	• 0x1afb8:$remcos: Remcos • 0x1b82c:$remcos: Remcos • 0x1b864:$url: Breaking-Security.Net • 0x20086:$resource: SETTINGS
00000009.00000002.336989263.0000000002B77000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000009.00000002.336989263.0000000002B77000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000009.00000002.336989263.0000000002B77000.00000004.00000800.00020000.00000000.sdmp	Remcos	detect Remcos in memory	JPCERT/CC Incident Response Group	• 0x72b64:$remcos: Remcos • 0x733d8:$remcos: Remcos • 0x73410:$url: Breaking-Security.Net • 0x77c32:$resource: SETTINGS
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.s0VxndYXq0.exe.452e400.8.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.s0VxndYXq0.exe.452e400.8.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x10738:$s1: \Classes\mscfile\shell\open\command • 0x10720:$s2: eventvwr.exe
0.2.s0VxndYXq0.exe.452e400.8.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x11034:$name: Remcos • 0x118a8:$name: Remcos • 0x118fb:$name: REMCOS • 0x10688:$time: %02i:%02i:%02i:%03i • 0x11320:$time: %02i:%02i:%02i:%03i • 0x29fc:$crypto: 0F B6 96 08 04 00 00 89 10 8B 45 08 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F4 FB FF F F 30 06 47 3B 7D 0C 72
0.2.s0VxndYXq0.exe.452e400.8.unpack	Remcos	detect Remcos in memory	JPCERT/CC Incident Response Group	• 0x11034:$remcos: Remcos • 0x118a8:$remcos: Remcos • 0x118e0:$url: Breaking-Security.Net • 0x160ea:$resource: SETTINGS
0.2.s0VxndYXq0.exe.452e400.8.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x114dc:$funcs1: autogetofflinelogs • 0x114c0:$funcs2: clearlogins • 0x114f0:$funcs3: getofflinelogs • 0x11578:$funcs4: execcom • 0x114cc:$funcs5: deletekeylog • 0x11798:$funcs6: remscriptexecd • 0x115bc:$funcs7: getwindows • 0x10da0:$funcs8: fundlldata • 0x10d78:$funcs9: getfunlib • 0x107ec:$funcs10: autofflinelogs • 0x113b8:$funcs11: getclipboard • 0x114b4:$funcs12: getscrslist • 0x107e0:$funcs13: offlinelogs • 0x105c8:$funcs14: getcamsingleframe • 0x116e4:$funcs15: listfiles • 0x115e0:$funcs16: getproclist • 0x10828:$funcs17: onlinelogs • 0x11700:$funcs18: getdrives • 0x11784:$funcs19: remscriptsuccess • 0x10600:$funcs20: getcamframe • 0x1115c:$str_a1: C:\Windows\System32\cmd.exe
Click to see the 56 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Uses ping.exe to check the status of other devices and networks

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Remcos RAT

Remote Access Functionality

Yara detected Remcos RAT

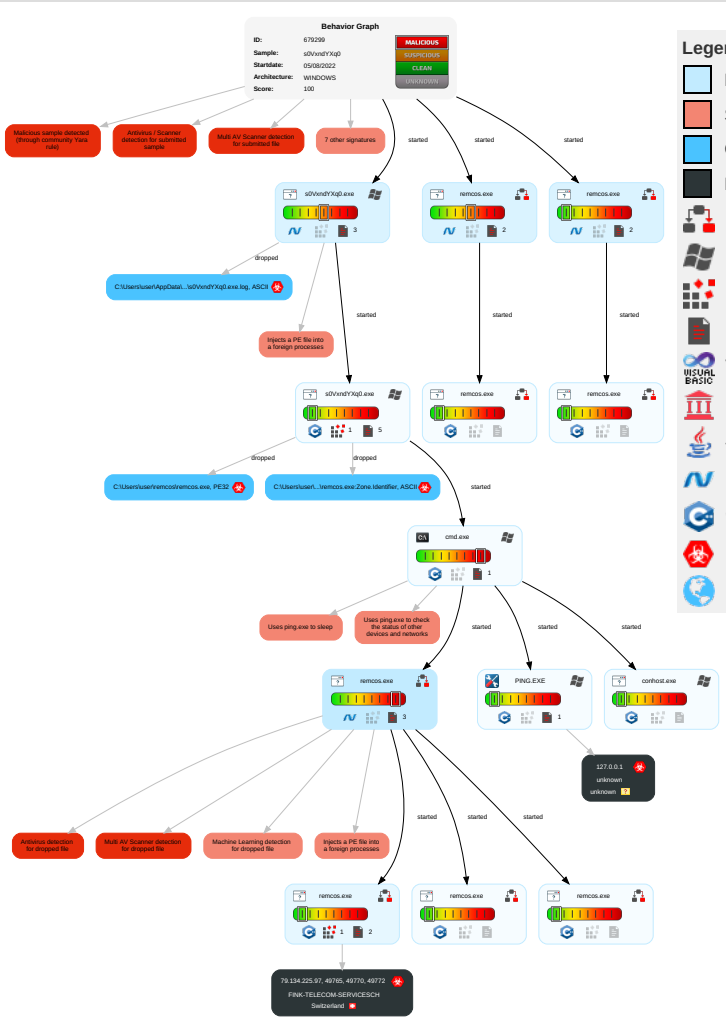
Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Masquerading	1 Input Capture	2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Scripting	LSA Secrets	1 System Network Configuration Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Software Packing	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

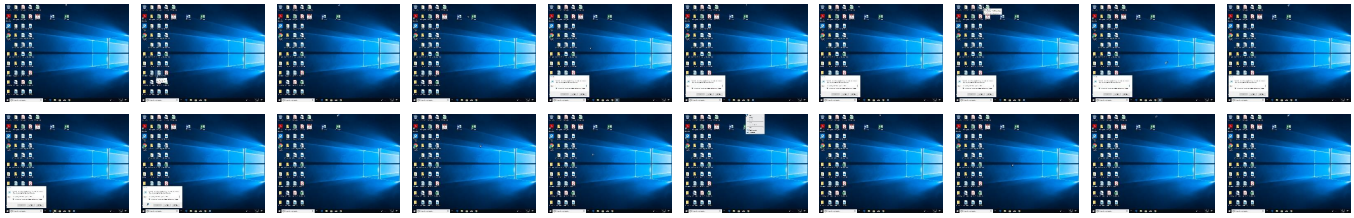
Behavior Graph



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
s0VxndYXq0.exe	54%	Virustotal		Browse
s0VxndYXq0.exe	54%	ReversingLabs	ByteCode-MSIL.Trojan.Worefl int	
s0VxndYXq0.exe	100%	Avira	TR/Kryptik.wodao	
s0VxndYXq0.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\remcos\remcos.exe	100%	Avira	TR/Kryptik.wodao	
C:\Users\user\remcos\remcos.exe	100%	Joe Sandbox ML		
C:\Users\user\remcos\remcos.exe	54%	ReversingLabs	ByteCode-MSIL.Trojan.Worefl int	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.s0VxndYXq0.exe.452e400.8.unpack	100%	Avira	HEUR/AGEN.1219514		Download File
5.0.s0VxndYXq0.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1219514		Download File
0.2.s0VxndYXq0.exe.4545420.9.unpack	100%	Avira	HEUR/AGEN.1219514		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://bladecoding.com/lolnotes/leagueofstats.php?name=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comalsR	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
79.134.225.97	3%	Virustotal		Browse
79.134.225.97	0%	Avira URL Cloud	safe	
http://www.agfamonotype.cw	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comictav	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.com7	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsk	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l-g	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.Wb	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.97	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

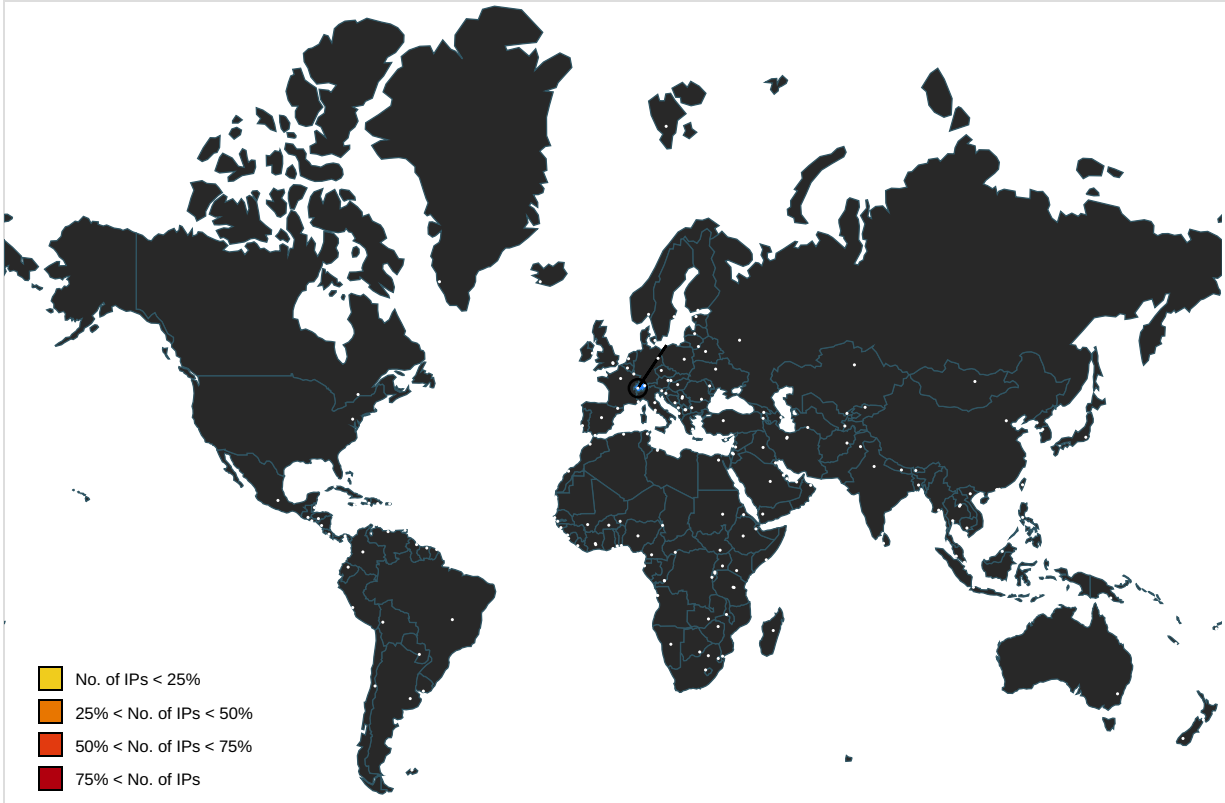
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://bladecoding.com/lolnotes/leagueofstats.php?name=	s0VxndYXq0.exe, remcos.exe.5.dr	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersF	s0VxndYXq0.exe, 00000000.00000003.237791179.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237771360.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237819421.0000000005B1E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.lolking.net/summoner/	s0VxndYXq0.exe, remcos.exe.5.dr	false		high
http://www.fontbureau.comalsR	s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	s0VxndYXq0.exe, 00000000.00000003.237525657.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.238027244.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersP	s0VxndYXq0.exe, 00000000.00000003.237710320.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.agfamonotype.cw	s0VxndYXq0.exe, 00000000.00000003.243809889.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.243932808.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.243586194.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244127013.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244021936.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.243771965.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.243848246.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244328823.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244234942.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.249288953.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000002.274138797.0000000005B2A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comalsF	s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersa	s0VxndYXq0.exe, 00000000.00000003.238476266.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.238443260.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designerse	s0VxndYXq0.exe, 00000000.00000003.244079552.0000000005B1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comictav	s0VxndYXq0.exe, 00000000.00000003.244188865.0000000005AEE000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244610211.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244375972.0000000005AED000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/%	s0VxndYXq0.exe, 00000000.00000003.236244264.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236102854.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com7	s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsk	s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerst	s0VxndYXq0.exe, 00000000.00000003.244112658.0000000005B1C000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244079552.0000000005B1C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/l-g	s0VxndYXq0.exe, 00000000.00000003.236244264.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236102854.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236394837.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y	s0VxndYXq0.exe, 00000000.00000003.236244264.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236102854.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236394837.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244188865.0000000005AEE000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000002.274032296.0000000005AEE000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244610211.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244375972.0000000005AED000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.264248405.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://raw.github.com/bladecoding/LoLNotes/master/General.txtO	s0VxndYXq0.exe, remcos.exe.5.dr	false		high
http://www.jiyu-kobo.co.jp/jp/	s0VxndYXq0.exe, 00000000.00000003.236244264.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236102854.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236394837.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	s0VxndYXq0.exe, 00000000.00000003.244188865.0000000005AEE000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244610211.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244375972.0000000005AED000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerses-es_tradnlw	s0VxndYXq0.exe, 00000000.00000003.237791179.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237910949.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237771360.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237851832.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237819421.0000000005B1E000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237952730.0000000005B1E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comd	s0VxndYXq0.exe, 00000000.00000003.238946519.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/high6/LoLNotes	s0VxndYXq0.exe, remcos.exe.5.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237981073.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.238107631.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.238027244.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.Wb	s0VxndYXq0.exe, 00000000.00000003.237033632.0000000005B1E000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.237070417.0000000005B20000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	s0VxndYXq0.exe, 00000000.00000003.244188865.0000000005AEE000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244610211.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.244375972.0000000005AED000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	s0VxndYXq0.exe, 00000000.00000003.236102854.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.236394837.0000000005AEC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://bit.ly/unCoIY?http://lolnotes-	s0VxndYXq0.exe, remcos.exe.5.dr	false		high
http://www.fontbureau.com/designers8	s0VxndYXq0.exe, 00000000.00000002.274487686.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp, s0VxndYXq0.exe, 00000000.00000003.238027244.0000000005B1D000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.97	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679299
Start date and time: 05/08/202214:59:08	2022-08-05 14:59:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	s0VxndYXq0 (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:	37
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@23/5@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:00:21	API Interceptor	2x Sleep call for process: s0VxndYXq0.exe modified

Time	Type	Description
15:00:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run remcos "C:\Users\user\remcos\remcos.exe"
15:00:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run remcos "C:\Users\user\remcos\remcos.exe"
15:00:43	API Interceptor	6x Sleep call for process: remcos.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\remcos\remcos.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	high, 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\Microsoft\CLR_v4.0_32\UsageLogs\s0VxndYXq0.exe.log

Process:	C:\Users\user\Desktop\s0VxndYXq0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308

Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, 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\install.bat

Process:	C:\Users\user\Desktop\s0VxndYXq0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	83
Entropy (8bit):	4.660536268409599
Encrypted:	false
SSDEEP:	3:cQxCvfn9m1t+CQHovBkwbM2n:cQ2fE1wCSovKwo2n
MD5:	F153731DF7A038F42AAA8D34E873FF25
SHA1:	1C90ACC2243D0DBEDEB28A8F7F719E605D80894D
SHA-256:	BC24BC26EE03AE15EE552CADF887C9FC201D19D76944321883E5C818D0E8A4AF
SHA-512:	F16A79B8A04E90B7B8F43D3001D51FDDDDC07B8D117D1CF978C35C96DDFFD161E6901DA5446EB42758DC980FC79ADC8BCA1B5DA640AB294BD24A8944FF0D1CA
Malicious:	false
Preview:	PING 127.0.0.1 -n 2 ..start "" "C:\Users\user\remcos\remcos.exe"..del %0 ..exit ..

C:\Users\user\remcos\remcos.exe

Process:	C:\Users\user\Desktop\s0VxndYXq0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	950272
Entropy (8bit):	7.359178629458712
Encrypted:	false
SSDEEP:	12288:4Rb0kj3oTB2b2UVFdPBGjIKHfrLPVPf1cLlq+R3rU8weZd+ydGRuwJGdaTuM18N5:4RA0siGjIKHf/NH1eFR7U8wWkTRk
MD5:	DE9784A4F56EAF8AFFC96754A15A5CD3
SHA1:	35C361A8BFDB894E80FE99728E60AD7D08745AF1
SHA-256:	F384A96582763BE490EA4EEED6D3F10291D7DF964F64DB077B4D10697149A7DA
SHA-512:	8576E0ED22421F70350A1108129E6DFA0190335724561CA5093E22A8CEB2E6AD0D61DB77A86C4603C60F4627C091D576B9174DAA2C0545D9D1E032502BC19E3
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\remcos\remcos.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 54%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....G.b.....0..`.....n~... .....@.. .....@.....~..W..... ..... ..H.....text...t^... ..`..... ..`.rsrc.....b.....@..@.reloc.....~.....@..B.....P~.....H.....E..|8.....+...X...@E.....U.....U..`.E.f.8.u...3..f9H.u..@.....a.....0.....*....0.....(.....*.0.....(.....*.0..<.....(#.....(.....(.....(.....(.....(....*.0.....{....*..0.....}....*.0.....{....*..0.....}....*.0.....{....*..0.....}....*.0.....{....*..0.....}....*.0.....{....*..0.....}....*.0.....

C:\Users\user\remcos\remcos.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\s0VxndYXq0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.359178629458712
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	s0VxndYXq0.exe
File size:	950272
MD5:	de9784a4f56eaf8affc96754a15a5cd3
SHA1:	35c361a8bfdb894e80fe99728e60ad7d08745af1
SHA256:	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da
SHA512:	8576e0ed22421f70350a1108129e6dfa0190335724561ca5093e22a8ceb2e6ad0d61db77a86c4603c60f4627c091d576b9174daa2c0545d9d1e032502bc19e3e
SSDEEP:	12288:4Rb0kj3oTB2b2UVFdPBGjIKHfrLPVPf1cLlq+R3rU8weZd+ydGRuwJGdaTuM18N5:4RA0siGjIKHf/NH1eFR7U8wWkTRk
TLSH:	5D155A99369071EFC857C976CA682C50FB31B576930FD207A45322ADAE0D6ABDF101F2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....G.b.....0..`.....n~... .....@.. .....@.....

File Icon

Icon Hash:	397165848c36a18d

Static PE Info

General

Entrypoint:	0x4e7e6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62E047C2 [Tue Jul 26 20:00:02 2022 UTC]
TLS Callbacks:	
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:	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
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
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	0xe7e14	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe8000	0x1a90	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xea000	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	0xe5e74	0xe6000	False	0.7169316830842392	data	7.366377921746369	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x1a90	0x1c00	False	0.45717075892857145	data	5.558425499312093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe8160	0xd28	data		
RT_GROUP_ICON	0xe8e88	0x14	data		
RT_GROUP_ICON	0xe8e9c	0x14	data		
RT_VERSION	0xe8eb0	0x33c	data		
RT_MANIFEST	0xe91ec	0x8a3	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

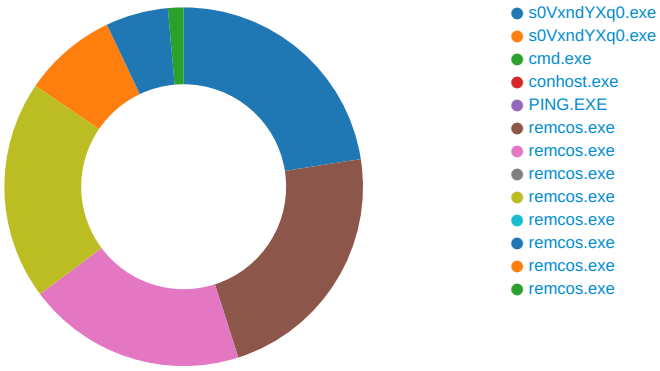
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 15:00:51.489784956 CEST	49765	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:00:51.547962904 CEST	8600	49765	79.134.225.97	192.168.2.4
Aug 5, 2022 15:00:52.065028906 CEST	49765	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:00:52.123380899 CEST	8600	49765	79.134.225.97	192.168.2.4
Aug 5, 2022 15:00:52.709264040 CEST	49765	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:00:52.767832994 CEST	8600	49765	79.134.225.97	192.168.2.4
Aug 5, 2022 15:00:57.773063898 CEST	49770	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:00:57.832314014 CEST	8600	49770	79.134.225.97	192.168.2.4
Aug 5, 2022 15:00:58.334733009 CEST	49770	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:00:58.393183947 CEST	8600	49770	79.134.225.97	192.168.2.4
Aug 5, 2022 15:00:59.022278070 CEST	49770	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:00:59.080661058 CEST	8600	49770	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:04.092365980 CEST	49772	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:04.150609970 CEST	8600	49772	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:04.710223913 CEST	49772	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:04.768486977 CEST	8600	49772	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:05.413645983 CEST	49772	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:05.472306967 CEST	8600	49772	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:10.476984978 CEST	49773	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:10.535494089 CEST	8600	49773	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:11.132644892 CEST	49773	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:11.191097975 CEST	8600	49773	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:11.835798979 CEST	49773	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:11.897294044 CEST	8600	49773	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:16.906243086 CEST	49774	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:16.964862108 CEST	8600	49774	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:17.602025032 CEST	49774	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:17.660366058 CEST	8600	49774	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:18.211484909 CEST	49774	8600	192.168.2.4	79.134.225.97

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 15:01:18.269845963 CEST	8600	49774	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:23.275614977 CEST	49776	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:23.334021091 CEST	8600	49776	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:23.914994955 CEST	49776	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:23.973387957 CEST	8600	49776	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:24.602653980 CEST	49776	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:24.661000013 CEST	8600	49776	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:29.691310883 CEST	49801	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:29.749579906 CEST	8600	49801	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:30.337486982 CEST	49801	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:30.395963907 CEST	8600	49801	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:31.024995089 CEST	49801	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:31.083328009 CEST	8600	49801	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:36.541906118 CEST	49819	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:36.600670099 CEST	8600	49819	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:37.135059118 CEST	49819	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:37.193582058 CEST	8600	49819	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:37.838089943 CEST	49819	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:37.896397114 CEST	8600	49819	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:42.902713060 CEST	49827	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:42.961273909 CEST	8600	49827	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:43.463576078 CEST	49827	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:43.522169113 CEST	8600	49827	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:44.026073933 CEST	49827	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:44.084547043 CEST	8600	49827	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:49.099905968 CEST	49836	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:49.158422947 CEST	8600	49836	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:49.667279005 CEST	49836	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:49.725716114 CEST	8600	49836	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:50.229877949 CEST	49836	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:50.288291931 CEST	8600	49836	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:56.090359926 CEST	49844	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:56.148978949 CEST	8600	49844	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:56.652179956 CEST	49844	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:56.710563898 CEST	8600	49844	79.134.225.97	192.168.2.4
Aug 5, 2022 15:01:57.214720964 CEST	49844	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:01:57.273039103 CEST	8600	49844	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:02.278929949 CEST	49861	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:02.337223053 CEST	8600	49861	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:02.840158939 CEST	49861	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:02.898443937 CEST	8600	49861	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:03.402717113 CEST	49861	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:03.460984945 CEST	8600	49861	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:09.368092060 CEST	49865	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:09.426564932 CEST	8600	49865	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:10.090811968 CEST	49865	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:10.149149895 CEST	8600	49865	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:10.700218916 CEST	49865	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:10.758519888 CEST	8600	49865	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:15.763689041 CEST	49866	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:15.821871996 CEST	8600	49866	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:16.325689077 CEST	49866	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:16.384908915 CEST	8600	49866	79.134.225.97	192.168.2.4
Aug 5, 2022 15:02:16.888501883 CEST	49866	8600	192.168.2.4	79.134.225.97
Aug 5, 2022 15:02:16.946827888 CEST	8600	49866	79.134.225.97	192.168.2.4

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: s0VxndYXq0.exe PID: **2732**, Parent PID: **2256**

General

Target ID:	0
Start time:	15:00:07
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\s0VxndYXq0.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\s0VxndYXq0.exe"
Imagebase:	0x550000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.271680078.0000000004513000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Remcos, Description: detect Remcos in memory, Source: 00000000.00000002.271680078.0000000004513000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.268436636.0000000002CD7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.268436636.0000000002CD7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Remcos, Description: detect Remcos in memory, Source: 00000000.00000002.268436636.0000000002CD7000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: s0VxndYXq0.exe PID: **3264**, Parent PID: **2732**

General

Target ID:	5
Start time:	15:00:23
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\s0VxndYXq0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\s0VxndYXq0.exe

Imagebase:	0x930000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000000.261466626.0000000000410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000002.269857625.0000000002CD0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40653B	CreateDirectoryA
C:\Users\user\remcos\remcos.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	40662B	CopyFileA
C:\Users\user\remcos\remcos.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	40662B	CopyFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\remcos\remcos.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 47 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 60 0e 00 00 1e 00 00 00 00 00 00 6e 7e 0e 00 00 20 00 00 00 fd 0e 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 fd 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELGb0`n~ @ @	success or wait	4	40662B	CopyFileA
C:\Users\user\remcos\remcos.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	40662B	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	remcos	unicode	"C:\Users\user\remcos\remcos.exe"	success or wait	1	409019	RegSetValueExA

Analysis Process: cmd.exe PID: **3704**, Parent PID: **3264**

General

Target ID:	6
Start time:	15:00:27
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\install.bat" "
Imagebase:	0x1190000
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

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\install.bat	unknown	8191	success or wait	3	119FB07	ReadFile

Analysis Process: conhost.exe PID: **3708**, Parent PID: **3704**

General

Target ID:	7
Start time:	15:00:28
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7338d0000
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: PING.EXE PID: **5088**, Parent PID: **3704**

General

Target ID:	8
Start time:	15:00:29
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true

Commandline:	PING 127.0.0.1 -n 2
Imagebase:	0x13b0000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: remcos.exe PID: **3908**, Parent PID: **3704**

General

Target ID:	9
Start time:	15:00:30
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\remcos\remcos.exe"
Imagebase:	0x530000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.336989263.0000000002B77000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000009.00000002.336989263.0000000002B77000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Remcos, Description: detect Remcos in memory, Source: 00000009.00000002.336989263.0000000002B77000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\remcos\remcos.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 54%, ReversingLabs
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	6CF2CF06	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	6CF2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\remcos.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D23C78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\remcos.exe.log	0	1308	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D23C907	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	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD71B4F	ReadFile

Analysis Process: remcos.exe PID: **5540**, Parent PID: **3616**

General

Target ID:	12
Start time:	15:00:39
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\remcos\remcos.exe"
Imagebase:	0x950000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000C.00000002.351406709.0000000002FDB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Remcos, Description: detect Remcos in memory, Source: 0000000C.00000002.351406709.0000000002FDB000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
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	6CF2CF06	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	6CF2CF06	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	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD71B4F	ReadFile

Analysis Process: remcos.exe PID: **1924**, Parent PID: **3908**

General

Target ID:	21
Start time:	15:00:47
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\remcos\remcos.exe
Imagebase:	0x1b0000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: remcos.exe PID: **4776**, Parent PID: **3616**

General

Target ID:	22
Start time:	15:00:47
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\remcos\remcos.exe"
Imagebase:	0xb70000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6CF2CF06	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	6CF2CF06	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	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD71B4F	ReadFile

Analysis Process: remcos.exe PID: **5456**, Parent PID: **3908**

General

Target ID:	23
Start time:	15:00:48
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\remcos\remcos.exe
Imagebase:	0x80000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3

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

Analysis Process: remcos.exe PID: 3572, Parent PID: 3908

General

Target ID:	24
Start time:	15:00:49
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\remcos\remcos.exe
Imagebase:	0x850000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000018.00000002.493007691.00000000029B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40653B	CreateDirectoryA
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	407A7F	CreateDirectoryA

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\remcos_totevzugmgbhhbj\	success or wait	1	408FED	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\remcos_totevzugmgbhhbj	EXEpath	unicode	6.F....s>:i....,...St d.....`e.	success or wait	1	409019	RegSetValueExA

Analysis Process: remcos.exe PID: 5580, Parent PID: 5540

General

Target ID:	26
Start time:	15:01:00
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\remcos\remcos.exe

Imagebase:	0xbe0000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000002.342391067.0000000002F00000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: remcos.exe PID: **5832**, Parent PID: **4776**

General

Target ID:	28
Start time:	15:01:11
Start date:	05/08/2022
Path:	C:\Users\user\remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\remcos\remcos.exe
Imagebase:	0x650000
File size:	950272 bytes
MD5 hash:	DE9784A4F56EAF8AFFC96754A15A5CD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001C.00000002.365233653.0000000000DF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly