ID: 756107
Sample Name: POv5Nk1dlu.exe
Cookbook: default.jbs
Time: 16:40:49
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

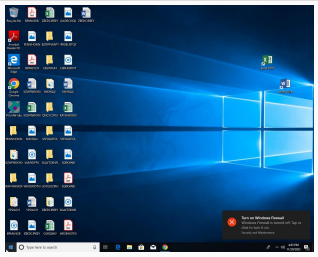
Windows Analysis Report

POv5Nk1dlu.exe

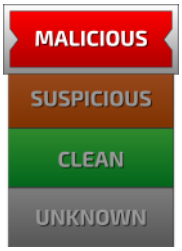
Overview

General Information

Sample Name:	POv5Nk1dlu.exe
Analysis ID:	756107
MD5:	14e2d1b23a0737.
SHA1:	000e55014fd096..
SHA256:	cd64bfd3940f7aa..
Tags:	exe
Infos:	



Detection

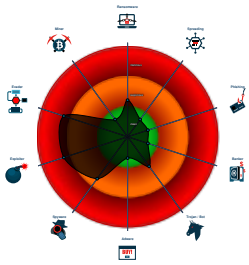


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Sigma detected: Drops script at sta…
- Binary is likely a compiled AutoIt sc…
- Found API chain indicative of debug…
- Uses schtasks.exe or at.exe to add…
- Uses 32bit PE files
- Yara signature match
- Contains functionality to check if a d…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- POv5Nk1dlu.exe (PID: 1408 cmdline: C:\Users\user\Desktop\POv5Nk1dlu.exe MD5: 14E2D1B23A073724D63CE5C9C89091CD)
- wscript.exe (PID: 4716 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\RDVGHelper\runas.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - at.exe (PID: 2848 cmdline: "C:\Users\user\RDVGHelper\at.exe" MD5: 8B5794337FDF61005D3F079A792B0AA1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\runas.url	Methodology_Suspicious_Shortcut_Local_URL	Detects local script usage for .URL persistence	@itsreallynick (Nick Carr), @QW5kcmV3 (Andrew Thompson)	• 0x13:$file: URL=file:/// • 0x56:$file: URL=file:/// • 0x0:$url_explicit: [InternetShortcut] • 0x43:$url_explicit: [InternetShortcut]

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

System Summary

Binary is likely a compiled AutoIt script file

Boot Survival

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

Anti Debugging

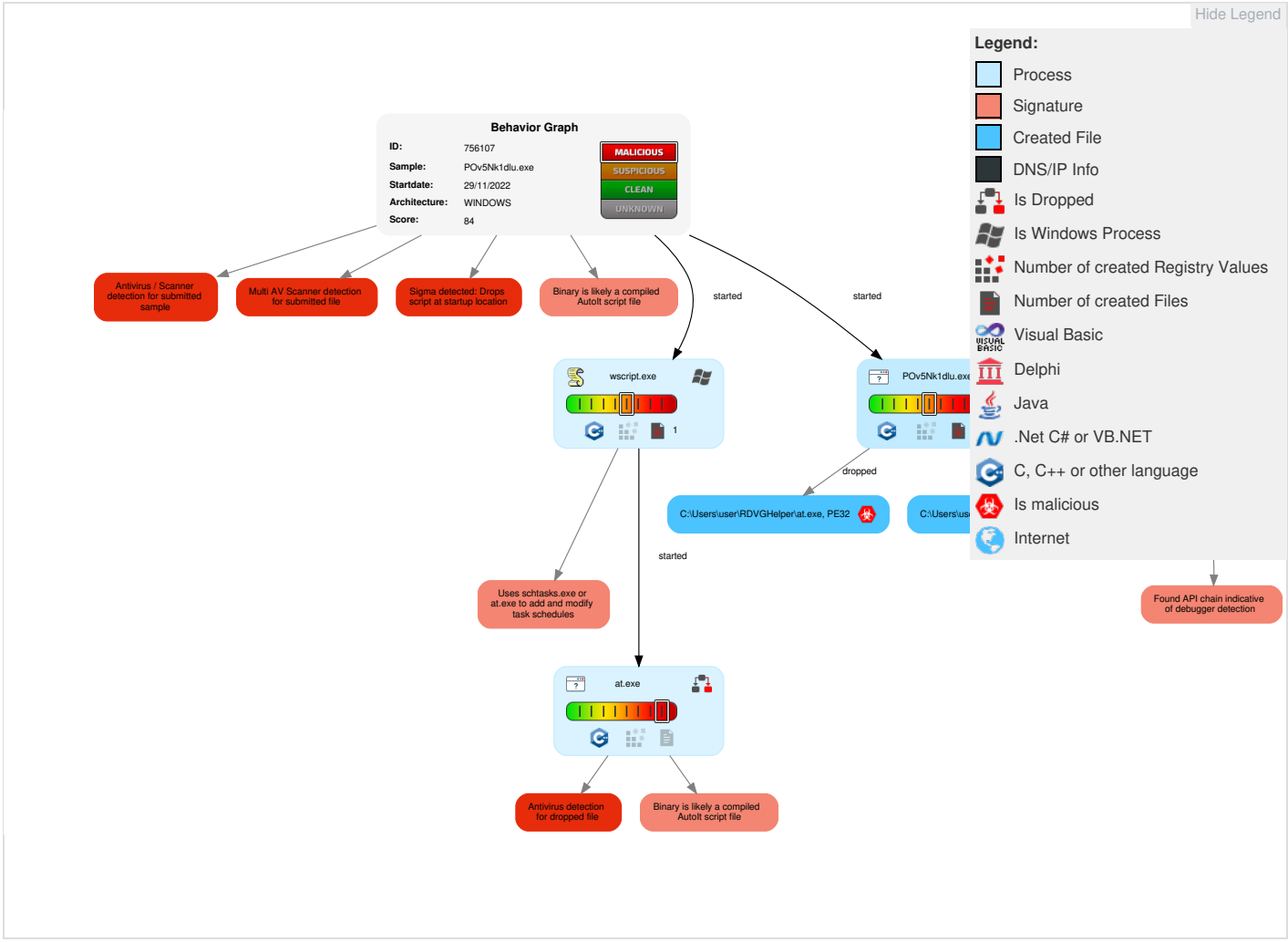
Found API chain indicative of debugger detection

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
2 Valid Accounts	1 1 Scripting	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	2 1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	2 Valid Accounts	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	2 Valid Accounts	1 1 Scripting	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	2 Registry Run Keys / Startup Folder	2 1 Access Token Manipulation	2 1 Obfuscated Files or Information	NTDS	1 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 2 Process Injection	1 Software Packing	LSA Secrets	1 3 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	1 Scheduled Task/Job	1 DLL Side-Loading	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	2 Registry Run Keys / Startup Folder	1 Masquerading	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Valid Accounts	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	2 1 Access Token Manipulation	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 2 Process Injection	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

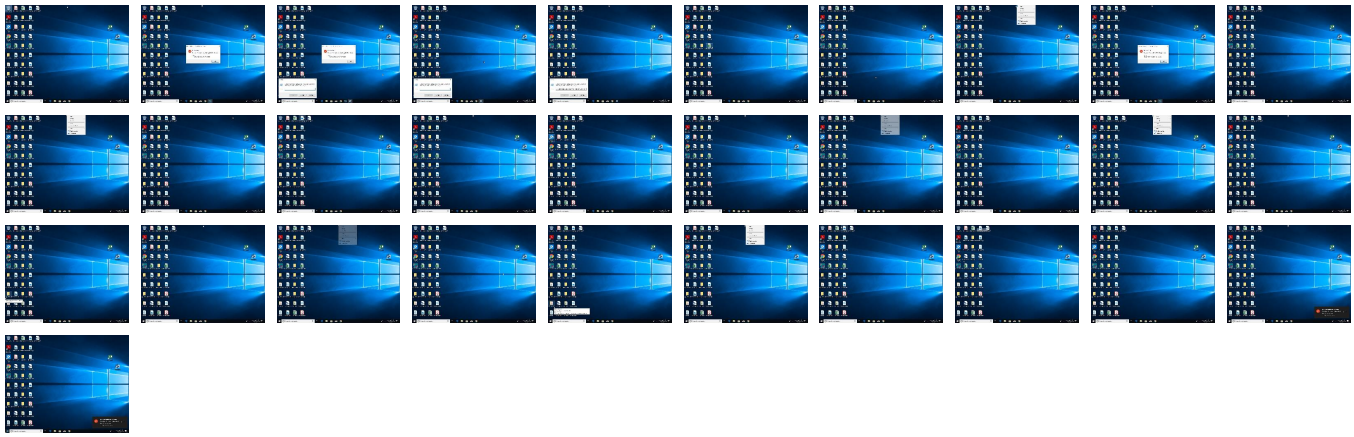
Behavior Graph



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
POv5Nk1dlu.exe	77%	ReversingLabs	Win32.Backdoor.NanoCore	
POv5Nk1dlu.exe	73%	Virustotal		Browse
POv5Nk1dlu.exe	100%	Avira	HEUR/AGEN.1245473	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\RDVGHelper\at.exe	100%	Avira	HEUR/AGEN.1245473	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.POv5Nk1dlu.exe.f50000.0.unpack	100%	Avira	HEUR/AGEN.1245473		Download File
2.0.at.exe.950000.0.unpack	100%	Avira	HEUR/AGEN.1245473		Download File
2.2.at.exe.950000.0.unpack	100%	Avira	HEUR/AGEN.1220844		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.POv5Nk1dlu.exe.f50000.0.unpack	100%	Avira	HEUR/AGEN.1220844		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.orgmTimed	0%	Avira URL Cloud	safe	
http://bot.whatismyipaddress.com6	0%	Avira URL Cloud	safe	
http://checkip.dyndns.orgmTime	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org	POv5Nk1dlu.exe, 00000000.00000002.316017878.0000000000DAD000.00000004.00000020.00020000.00000000.sdmp, at.exe, 00000002.00000002.358917443.00000000017B4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://checkip.dyndns.orgmTimed	at.exe, 00000002.00000002.358917443.00000000017B4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bot.whatismyipaddress.com	at.exe, 00000002.00000002.358917443.00000000017B4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://bot.whatismyipaddress.com6	POv5Nk1dlu.exe, 00000000.00000002.316065070.0000000000DEF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.myexternalip.com/raw	at.exe, 00000002.00000002.358917443.00000000017B4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://checkip.dyndns.orgmTime	POv5Nk1dlu.exe, 00000000.00000002.316065070.0000000000DEF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.myexternalip.com/raw/	POv5Nk1dlu.exe, 00000000.00000002.316065070.0000000000DEF000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756107
Start date and time:	2022-11-29 16:40:49 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	POv5Nk1dlu.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
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:	mal84.expl.evad.winEXE@4/3@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.9%) • Quality average: 78.5% • Quality standard deviation: 11.3%
HCA Information:	• Successful, ratio: 64% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:41:51	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\runas.url

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\runas.url

Process:	C:\Users\user\Desktop\POv5Nk1dlu.exe
File Type:	Generic INItialization configuration [InternetShortcut]
Category:	modified
Size (bytes):	134
Entropy (8bit):	4.778942459748406
Encrypted:	false
SSDEEP:	3:HRAbABGQVuOUVifX5XQw0ylyLABGQVuOUVifX5XQw0W:HRYF5OLX5XQw08YF5OLX5XQw0W
MD5:	A84D228A61B08792024FF4337CC606F6
SHA1:	92DD57483FFF604A9848EDF1B060EB9BD11D6C42
SHA-256:	8CA3F2A55F27D106D5521C66C109B98CF9A13EAD480A46AA8F3906E1DD645F9B
SHA-512:	13663A0862CD250CBB2AAF238A77A97F4528A5E0E200C79C3B16AF30076290F2338F4C5D14B7B7E390DC4B8D39A5C0BBA77C648D86F9023722EFEB9E15CF2F7 7
Malicious:	**true**
Yara Hits:	• Rule: Methodology_Suspicious_Shortcut_Local_URL, Description: Detects local script usage for .URL persistence, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\runas.url, Author: @itsreallynick (Nick Carr), @QW5kcmV3 (Andrew Thompson)
Reputation:	low
Preview:	[InternetShortcut].URL=file:///C:\Users\user\RDVGHelper\runas.vbs[InternetShortcut].URL=file:///C:\Users\user\RDVGHelper\runas.vbs

C:\Users\user\RDVGHelper\at.exe

Process:	C:\Users\user\Desktop\POv5Nk1dlu.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	1348112
Entropy (8bit):	5.849778682930291
Encrypted:	false
SSDEEP:	24576:4AHnh+eWsN3skA4RV1Hom2KXDuFLLJiEzeyG75B:/h+ZkldoPKT4L4Ez3G9B
MD5:	8B5794337FDF61005D3F079A792B0AA1
SHA1:	61FAEBE8AB40D8C124AC8A5D060964EB9AF877A8
SHA-256:	184491C39AC7E31E86978E965583BEB6D692885B27C91003EF497A53CED6D70C
SHA-512:	6515FF218949A2F2DA753430F9469B40A887906955D31905C730F5340480780673367CFEC7E72DFE09AE34EF045366C8A5F5A22C32ABE5E13ABABBD7DC2EC3AE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........s..R...R...R....C..P....;.S..._@#.a..._@......_@..g...[j..[...[jo.w...R ...r...........#.S..._@'.S...R.k.S....".S...RichR...................PE..L...H..\.........."......`...P...P.......`........@.......................................@...@.......@.........................\|........D...................@ ..4q.................................t...H...UPX0.....P.......P......................UPX1.....`...`...\...T.............@....rsrc....P.......J..................@....imports.0.......$...... ....@....reloc.......@...r..................@.. ....

C:\Users\user\RDVGHelper\runas.vbs

Process:	C:\Users\user\Desktop\POv5Nk1dlu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	106
Entropy (8bit):	4.736102681477269
Encrypted:	false
SSDEEP:	3:jaPcYonh3QBHoUVifX5EtACHn:jk+h8ILX5G1
MD5:	2372F2EE2222AB931284A8D08A10C318
SHA1:	C5DED8E64290FE4C74BC5FBADCCDF0BCAA5C6C7F
SHA-256:	E791FD8D094533E9CCA63CF23B8BEB8AB8F0E2F447BE2FDF1EE1B3B5A1DFD988
SHA-512:	B6EC56F1EC2ECE19C3370B8F53A92251D82D811AFEE9C202535AC565247236B76040D22A9EB7DDD77A2988E2C8BC4C42EE4A010558379D2A96B74BE109C460 D
Malicious:	false

Reputation:	low
Preview:	Set WshShell = WScript.CreateObject("WScript.Shell")..WshShell.Run """C:\Users\user\RDVGHelper\at.exe"""

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
Entropy (8bit):	5.8497727328429265
TrID:	• Win32 Executable (generic) a (10002005/4) 99.39% • UPX compressed Win32 Executable (30571/9) 0.30% • Win32 EXE Yoda's Crypter (26571/9) 0.26% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	POv5Nk1dlu.exe
File size:	1348104
MD5:	14e2d1b23a073724d63ce5c9c89091cd
SHA1:	000e55014fd09600275f5b394c5be51c2bf4dad9
SHA256:	cd64bfd3940f7aabd6a74ca47beba4ef1d19f6605dee0f64e5932765a3142fba
SHA512:	882164c258e762be8129ff85f1fcffe5c37df46931a2fcf7275673d0f982fbb6e2c0a7008ea6ddec5983e78162a2085f21f2d3f95f95e5f9e0b32462e7913a25
SSDEEP:	24576:4AHnh+eWsN3skA4RV1Hom2KXDuFLLJiEzeyG75Z:/h+ZkldoPKT4L4Ez3G9Z
TLSH:	4A558D02B3928035FEAE91739B59B20156BCFD64013385FF1298DD79BA701A11F2E66F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..R...R...R....C..P.....;.S..._@#.a..._@....._@..g...[j..[... [jo.w...R...r.....#.S..._@'.S...R.k.S.....".S...RichR..

File Icon

Icon Hash:	868c661b1d9cc4e6

Static PE Info

General

Entrypoint:	0x42800a
Entrypoint Section:	UPX0
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE, DEBUG_STRIPPED
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x5CCFBA48 [Mon May 6 04:38:32 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	bd3825b6e0410966f0c31f64b6c7644a

Entrypoint Preview

Instruction
call 00007F55550BFA3Dh
jmp 00007F55550B27F4h
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
push edi
push esi
mov esi, dword ptr [esp+10h]
mov ecx, dword ptr [esp+14h]
mov edi, dword ptr [esp+0Ch]
mov eax, ecx
mov edx, ecx
add eax, esi
cmp edi, esi
jbe 00007F55550B297Ah
cmp edi, eax
jc 00007F55550B2CDEh
bt dword ptr [004C41FCh], 01h
jnc 00007F55550B2979h
rep movsb
jmp 00007F55550B2C8Ch
cmp ecx, 00000080h
jc 00007F55550B2B44h
mov eax, edi
xor eax, esi
test eax, 0000000Fh
jne 00007F55550B2980h
bt dword ptr [004BF324h], 01h
jc 00007F55550B2E50h
bt dword ptr [004C41FCh], 00000000h
jnc 00007F55550B2B1Dh
test edi, 00000003h
jne 00007F55550B2B2Eh
test esi, 00000003h
jne 00007F55550B2B0Dh
bt edi, 02h
jnc 00007F55550B297Fh
mov eax, dword ptr [esi]
sub ecx, 04h
lea esi, dword ptr [esi+04h]
mov dword ptr [edi], eax
lea edi, dword ptr [edi+04h]
bt edi, 03h
jnc 00007F55550B2983h
movq xmm1, qword ptr [esi]
sub ecx, 08h
lea esi, dword ptr [esi+08h]
movq qword ptr [edi], xmm1
lea edi, dword ptr [edi+08h]
test esi, 00000007h
je 00007F55550B29D5h
bt esi, 03h

Rich Headers

Programming Language:	• [ASM] VS2013 build 21005 • [C] VS2013 build 21005 • [C++] VS2013 build 21005 • [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [ASM] VS2013 UPD5 build 40629 • [RES] VS2013 build 21005 • [LNK] VS2013 UPD5 build 40629

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x141000	0x17c	.imports
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10c000	0x34414	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x144000	0x7134	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x10ba74	0x48	UPX1
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0xb5000	0xb5000	False	0.5158192334254144	data	6.647020934312938	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
UPX1	0xb6000	0x56000	0x55c00	False	0.07822749635568513	data	1.3367400085274173	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x10c000	0x35000	0x34a00	False	0.6905943809382423	data	6.924446867745964	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.imports	0x141000	0x3000	0x2400	False	0.3615451388888889	data	4.6777086279249716	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x144000	0x8000	0x7200	False	0.7617530153508771	data	6.783955557128661	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10c4e4	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	Great Britain
RT_ICON	0x10c610	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128, 16 important colors	English	Great Britain
RT_ICON	0x10c73c	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	Great Britain
RT_ICON	0x10c868	0xeac8	Device independent bitmap graphic, 300 x 600 x 4, image size 57600	English	Great Britain
RT_MENU	0x11b334	0x50	data	English	Great Britain
RT_STRING	0x11b388	0x48b8	data		
RT_STRING	0x11fc44	0x48b8	data		
RT_STRING	0x124500	0x594	data	English	Great Britain

Name	RVA	Size	Type	Language	Country
RT_STRING	0x124a98	0x68a	data	English	Great Britain
RT_STRING	0x125128	0x490	data	English	Great Britain
RT_STRING	0x1255bc	0x5fc	data	English	Great Britain
RT_STRING	0x125bbc	0x65c	data	English	Great Britain
RT_STRING	0x12621c	0x466	data	English	Great Britain
RT_STRING	0x126688	0x158	Matlab v4 mat-file (little endian) n, numeric, rows 0, columns 0	English	Great Britain
RT_RCDATA	0x1267e4	0x19560	data		
RT_GROUP_ICON	0x13fd48	0x14	data	English	Great Britain
RT_GROUP_ICON	0x13fd60	0x14	data	English	Great Britain
RT_GROUP_ICON	0x13fd78	0x14	data	English	Great Britain
RT_GROUP_ICON	0x13fd90	0x14	data	English	Great Britain
RT_VERSION	0x13fda8	0x278	data	English	United States
RT_MANIFEST	0x140024	0x3ef	ASCII text, with CRLF line terminators	English	Great Britain

Imports

DLL	Import
KERNEL32.DLL	DuplicateHandle, CreateThread, WaitForSingleObject, HeapAlloc, GetProcessHeap, HeapFree, Sleep, GetCurrentThreadId, MultiByteToWideChar, MulDiv, GetVersionExW, IsWow64Process, GetSystemInfo, FreeLibrary, LoadLibraryA, GetProcAddress, SetErrorMode, GetModuleFileNameW, WideCharToMultiByte, lstrcpyW, lstrlenW, GetModuleHandleW, QueryPerformanceCounter, VirtualFreeEx, OpenProcess, VirtualAllocEx, WriteProcessMemory, ReadProcessMemory, CreateFileW, SetFilePointerEx, SetEndOfFile, ReadFile, WriteFile, FlushFileBuffers, TerminateProcess, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, SetFileTime, GetFileAttributesW, FindFirstFileW, SetCurrentDirectoryW, GetLongPathNameW, GetShortPathNameW, DeleteFileW, FindNextFileW, CopyFileExW, MoveFileW, CreateDirectoryW, RemoveDirectoryW, SetSystemPowerState, QueryPerformanceFrequency, FindResourceW, LoadResource, LockResource, SizeofResource, EnumResourceNamesW, OutputDebugStringW, GetTempPathW, GetTempFileNameW, DeviceIoControl, GetLocalTime, CompareStringW, GetCurrentProcess, EnterCriticalSection, LeaveCriticalSection, GetStdHandle, CreatePipe, InterlockedExchange, TerminateThread, LoadLibraryExW, FindResourceExW, CopyFileW, VirtualFree, FormatMessageW, GetExitCodeProcess, GetPrivateProfileStringW, WritePrivateProfileStringW, GetPrivateProfileSectionW, WritePrivateProfileSectionW, GetPrivateProfileSectionNamesW, FileTimeToLocalFileTime, FileTimeToSystemTime, SystemTimeToFileTime, LocalFileTimeToFileTime, GetDriveTypeW, GetDiskFreeSpaceExW, GetDiskFreeSpaceW, GetVolumeInformationW, SetVolumeLabelW, CreateHardLinkW, SetFileAttributesW, CreateEventW, SetEvent, GetEnvironmentVariableW, SetEnvironmentVariableW, GlobalLock, GlobalUnlock, GlobalAlloc, GetFileSize, GlobalFree, GlobalMemoryStatusEx, Beep, GetSystemDirectoryW, HeapReAlloc, HeapSize, GetComputerNameW, GetWindowsDirectoryW, GetCurrentProcessId, GetProcessIoCounters, CreateProcessW, GetProcessId, SetPriorityClass, LoadLibraryW, VirtualAlloc, IsDebuggerPresent, GetCurrentDirectoryW, lstrcmpiW, DecodePointer, GetLastError, RaiseException, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, InterlockedDecrement, InterlockedIncrement, GetCurrentThread, CloseHandle, GetFullPathNameW, EncodePointer, ExitProcess, GetModuleHandleExW, ExitThread, GetSystemTimeAsFileTime, ResumeThread, GetCommandLineW, IsProcessorFeaturePresent, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, SetLastError, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetStartupInfoW, GetStringTypeW, SetStdHandle, GetFileType, GetConsoleCP, GetConsoleMode, RtlUnwind, ReadConsoleW, GetTimeZoneInformation, GetDateFormatW, GetTimeFormatW, LCMapStringW, GetEnvironmentStringsW, FreeEnvironmentStringsW, WriteConsoleW, FindClose, SetEnvironmentVariableA
ADVAPI32.dll	GetAce, RegEnumValueW, RegDeleteValueW, RegDeleteKeyW, RegEnumKeyExW, RegSetValueExW, RegOpenKeyExW, RegCloseKey, RegQueryValueExW, RegConnectRegistryW, InitializeSecurityDescriptor, InitializeAcl, AdjustTokenPrivileges, OpenThreadToken, OpenProcessToken, LookupPrivilegeValueW, DuplicateTokenEx, CreateProcessAsUserW, CreateProcessWithLogonW, GetLengthSid, CopySid, LogonUserW, AllocateAndInitializeSid, CheckTokenMembership, RegCreateKeyExW, FreeSid, GetTokenInformation, GetSecurityDescriptorDacl, GetAclInformation, AddAce, SetSecurityDescriptorDacl, GetUserNameW, InitiateSystemShutdownExW
COMCTL32.dll	ImageList_ReplaceIcon, ImageList_Destroy, ImageList_Remove, ImageList_SetDragCursorImage, ImageList_BeginDrag, ImageList_DragEnter, ImageList_DragLeave, ImageList_EndDrag, ImageList_DragMove, InitCommonControlsEx, ImageList_Create
COMDLG32.dll	GetOpenFileNameW, GetSaveFileNameW
GDI32.dll	StrokePath, DeleteObject, GetTextExtentPoint32W, ExtCreatePen, GetDeviceCaps, EndPath, SetPixel, CloseFigure, CreateCompatibleBitmap, CreateCompatibleDC, SelectObject, StretchBlt, GetDIBits, LineTo, AngleArc, MoveToEx, Ellipse, DeleteDC, GetPixel, CreateDCW, GetStockObject, GetTextFaceW, CreateFontW, SetTextColor, PolyDraw, BeginPath, Rectangle, SetViewportOrgEx, GetObjectW, SetBkMode, RoundRect, SetBkColor, CreatePen, CreateSolidBrush, StrokeAndFillPath
IPHLPAPI.DLL	IcmpCreateFile, IcmpCloseHandle, IcmpSendEcho
MPR.dll	WNetUseConnectionW, WNetCancelConnection2W, WNetGetConnectionW, WNetAddConnection2W
ole32.dll	CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, ProgIDFromCLSID, CLSIDFromProgID, OleSetMenuDescriptor, MkParseDisplayName, OleSetContainedObject, CoCreateInstance, IIDFromString, StringFromGUID2, CreateStreamOnHGlobal, OleInitialize, OleUninitialize, CoInitialize, CoUninitialize, GetRunningObjectTable, CoGetInstanceFromFile, CoGetObject, CoSetProxyBlanket, CoCreateInstanceEx, CoInitializeSecurity

DLL	Import
OLEAUT32.dll	LoadTypeLibEx, VariantCopyInd, SysReAllocString, SysFreeString, SafeArrayDestroyDescriptor, SafeArrayDestroyData, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayAllocData, SafeArrayAllocDescriptorEx, SafeArrayCreateVector, RegisterTypeLib, CreateStdDispatch, DispCallFunc, VariantChangeType, SysStringLen, VariantTimeToSystemTime, VarR8FromDec, SafeArrayGetVartype, VariantCopy, VariantClear, OleLoadPicture, QueryPathOfRegTypeLib, RegisterTypeLibForUser, UnRegisterTypeLibForUser, UnRegisterTypeLib, CreateDispTypeInfo, SysAllocString, VariantInit
PSAPI.DLL	GetProcessMemoryInfo
SHELL32.dll	DragQueryPoint, ShellExecuteExW, DragQueryFileW, SHEmptyRecycleBinW, SHGetPathFromIDListW, SHBrowseForFolderW, SHCreateShellItem, SHGetDesktopFolder, SHGetSpecialFolderLocation, SHGetFolderPathW, SHFileOperationW, ExtractIconExW, Shell_NotifyIconW, ShellExecuteW, DragFinish
USER32.dll	AdjustWindowRectEx, CopyImage, SetWindowPos, GetCursorInfo, RegisterHotKey, ClientToScreen, GetKeyboardLayoutNameW, IsCharAlphaW, IsCharAlphaNumericW, IsCharLowerW, IsCharUpperW, GetMenuStringW, GetSubMenu, GetCaretPos, IsZoomed, MonitorFromPoint, GetMonitorInfoW, SetWindowLongW, SetLayeredWindowAttributes, FlashWindow, GetClassLongW, TranslateAcceleratorW, IsDialogMessageW, GetSysColor, InflateRect, DrawFocusRect, DrawTextW, FrameRect, DrawFrameControl, FillRect, PtInRect, DestroyAcceleratorTable, CreateAcceleratorTableW, SetCursor, GetWindowDC, GetSystemMetrics, GetActiveWindow, CharNextW, wsprintfW, RedrawWindow, DrawMenuBar, DestroyMenu, SetMenu, GetWindowTextLengthW, CreateMenu, IsDlgButtonChecked, DefDlgProcW, CallWindowProcW, ReleaseCapture, SetCapture, CreateIconFromResourceEx, mouse_event, ExitWindowsEx, SetActiveWindow, FindWindowExW, EnumThreadWindows, SetMenuDefaultItem, InsertMenuItemW, IsMenu, TrackPopupMenuEx, GetCursorPos, DeleteMenu, SetRect, GetMenuItemID, GetMenuItemCount, SetMenuItemInfoW, GetMenuItemInfoW, SetForegroundWindow, IsIconic, FindWindowW, MonitorFromRect, keybd_event, SendInput, GetAsyncKeyState, SetKeyboardState, GetKeyboardState, GetKeyState, VkKeyScanW, LoadStringW, DialogBoxParamW, MessageBeep, EndDialog, SendDlgItemMessageW, GetDlgItem, SetWindowTextW, CopyRect, ReleaseDC, GetDC, EndPaint, BeginPaint, GetClientRect, GetMenu, DestroyWindow, EnumWindows, GetDesktopWindow, IsWindow, IsWindowEnabled, IsWindowVisible, EnableWindow, InvalidateRect, GetWindowLongW, GetWindowThreadProcessId, AttachThreadInput, GetFocus, GetWindowTextW, ScreenToClient, SendMessageTimeoutW, EnumChildWindows, CharUpperBuffW, GetParent, GetDlgCtrlID, SendMessageW, MapVirtualKeyW, PostMessageW, GetWindowRect, SetUserObjectSecurity, CloseDesktop, CloseWindowStation, OpenDesktopW, SetProcessWindowStation, GetProcessWindowStation, OpenWindowStationW, GetUserObjectSecurity, MessageBoxW, DefWindowProcW, SetClipboardData, EmptyClipboard, CountClipboardFormats, CloseClipboard, GetClipboardData, IsClipboardFormatAvailable, OpenClipboard, BlockInput, GetMessageW, LockWindowUpdate, DispatchMessageW, TranslateMessage, PeekMessageW, UnregisterHotKey, CheckMenuRadioItem, CharLowerBuffW, MoveWindow, SetFocus, PostQuitMessage, KillTimer, CreatePopupMenu, RegisterWindowMessageW, SetTimer, ShowWindow, CreateWindowExW, RegisterClassExW, LoadIconW, LoadCursorW, GetSysColorBrush, GetForegroundWindow, MessageBoxA, DestroyIcon, SystemParametersInfoW, LoadImageW, GetClassNameW
USERENV.dll	DestroyEnvironmentBlock, UnloadUserProfile, CreateEnvironmentBlock, LoadUserProfileW
UxTheme.dll	IsThemeActive
VERSION.dll	GetFileVersionInfoW, GetFileVersionInfoSizeW, VerQueryValueW
WININET.dll	InternetQueryDataAvailable, InternetCloseHandle, InternetOpenW, InternetSetOptionW, InternetCrackUrlW, HttpQueryInfoW, InternetQueryOptionW, HttpOpenRequestW, HttpSendRequestW, FtpOpenFileW, FtpGetFileSize, InternetOpenUrlW, InternetReadFile, InternetConnectW
WINMM.dll	timeGetTime, waveOutSetVolume, mciSendStringW
WSOCK32.dll	WSACleanup, socket, inet_ntoa, setsockopt, ntohs, recvfrom, ioctlsocket, htons, WSAStartup, __WSAFDIsSet, select, accept, listen, bind, closesocket, WSAGetLastError, recv, sendto, send, inet_addr, gethostbyname, gethostname, connect

Possible Origin

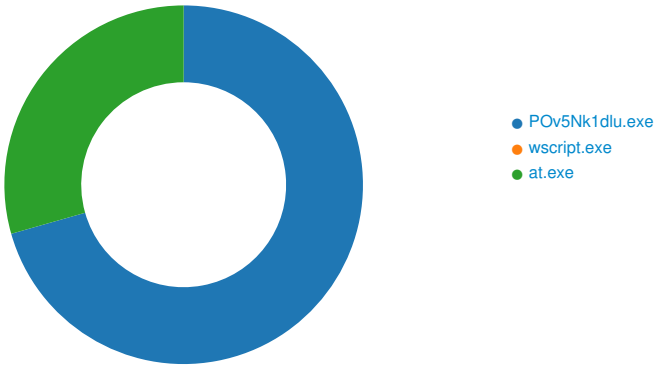
Language of compilation system	Country where language is spoken	Map
English	Great Britain	
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: POv5Nk1dlu.exe PID: 1408, Parent PID: 3324

General

Target ID:	0
Start time:	16:41:46
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\POv5Nk1dlu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\POv5Nk1dlu.exe
Imagebase:	0xf50000
File size:	1348104 bytes
MD5 hash:	14E2D1B23A073724D63CE5C9C89091CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: wscript.exe PID: 4716, Parent PID: 3324

General

Target ID:	1
Start time:	16:41:59
Start date:	29/11/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\RDVGHelper\runas.vbs"
Imagebase:	0x7ff6caef0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: at.exe PID: **2848**, Parent PID: **4716**

General

Target ID:	2
Start time:	16:42:07
Start date:	29/11/2022
Path:	C:\Users\user\RDVGHelper\at.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\RDVGHelper\at.exe"
Imagebase:	0x950000
File size:	1348112 bytes
MD5 hash:	8B5794337FDF61005D3F079A792B0AA1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira
Reputation:	low

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\runas.url	67	67	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 55 52 4c 3d 66 69 6c 65 3a 2f 2f 2f 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 52 44 56 47 48 65 6c 70 65 72 5c 72 75 6e 61 73 2e 76 62 73	[InternetShortcut]URL=file:///C:\Users\user\RDVGHelper\runas.vbs	success or wait	1	9B36B6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\RDVGHelper\at.exe	unknown	65536	success or wait	21	955D7C	ReadFile
C:\Users\user\RDVGHelper\at.exe	unknown	65536	success or wait	21	955D7C	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\runas.url	unknown	65536	success or wait	1	955D7C	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\runas.url	unknown	65536	end of file	1	955D7C	ReadFile

Disassembly

No disassembly