



Overview
overview

10

Static
static

3

native.exe
windows7-x64

10

native.exe
windows10-2004-x64

Report

Analysis Logs

Download Sample

Download PCAP

Download PCAPNG

Feedback

Print to PDF

Analysis

max time kernel
150s

max time network
149s

platform
windows10-2004_x64

resource
win10v2004-20240226-en

resource tags

ARCH:X64

ARCH:X86

IMAGE:WIN10V2004-
20240226-EN

LOCALE:EN-US

OS:WINDOWS10-2004-X64

SYSTEM

submitted
01-03-2024 14:16

Sharing

Copy URL

Twitter

E-mail



General



Target

native.exe



Size

2.1MB



MD5

1a917a85dcbb1d3df5f4dd02e3a62873



SHA1

567f528fec8e7a4787f8c253446d8f1b6
20dc9d6



SHA256

217bf967c95d1359314fcd53ae8d044
89eb3c7bdc1f22110d5a8a476d1fc92e



SHA512

341acbd43efac1718c7f3e3795549acf2
9237a2675bdadcb7e52ce18aac6dcc6a
e628e1b6edfa2338ed6d9923c148cb4
322c75fad86d5c0e6f2327c2270563ec



SSDEEP

49152:/WlrpDXJLRxe123BMGwxB19y0
IEjaV/EC5O7pD:/apzJy1kMxt2R/ET



Score

10^{/10}

RHADAMANTHYS

ZGRAT

RAT

STEALER



Malware Config



Signatures



Discovery

Detect ZGRat V1 • 36 IoCs

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

Accept

ZGRAT

RAT

- Checks computer location settings • 2 TTPs 1 IoCs
Looks up country code configured in the registry, likely geofence.
- Executes dropped EXE • 5 IoCs
- Suspicious use of SetThreadContext • 5 IoCs
- Enumerates physical storage devices • 1 TTPs
Attempts to interact with connected storage/optical drive(s).
- Program crash • 2 IoCs
- Suspicious behavior: EnumeratesProcesses • 16 IoCs
- Suspicious use of AdjustPrivilegeToken • 9 IoCs
- Suspicious use of WriteProcessMemory • 56 IoCs



Processes



<div>C:\Windows\system32\sihost.exe</div> <div>sihost.exe</div>	PID:2528
<div>C:\Windows\SysWOW64\dialer.exe</div> <div>"C:\Windows\system32\dialer.exe"</div>	PID:3484
<div>C:\Users\Admin\AppData\Local\Temp\native.exe</div> <div>"C:\Users\Admin\AppData\Local\Temp\native.exe"</div>	PID:212
<div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div> <div>"C:\Users\Admin\AppData\Local\Temp\BBLb.exe"</div>	PID:1552
<div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div> <div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div>	PID:1940
<div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div> <div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div>	PID:2616
<div>C:\Users\Admin\AppData\Local\Temp\native.exe</div> <div>C:\Users\Admin\AppData\Local\Temp\native.exe</div>	PID:2052
<div>C:\Windows\SysWOW64\WerFault.exe</div> <div></div>	PID:4572
<div></div> <div></div>	PID:3172
<div>C:\Windows\SysWOW64\WerFault.exe</div> <div></div>	PID:1560

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

■	C:\Windows\SysWOW64\WerFault.exe -pss -s 436 -p 2052 -ip 2052	
■	C:\Windows\SysWOW64\WerFault.exe C:\Windows\SysWOW64\WerFault.exe -pss -s 504 -p 2052 -ip 2052	PID:3808
■	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe -ExecutionPolicy Bypass - WindowStyle Hidden -NoProfile -enc QQBkA GQALQBNAAUABYAGUAZgB1AHIAZQBAGMAZQAgA C0ARQB4AGMABAB1AHMAaQBvAG4AUABhAHQAaAAGA EMA0gBcAFUAcwB1AHIAcwbCAEEAZABtAGkAbgBcA EEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwA0wAgA EEAZABkAC0ATQBwAFAAcgB1AGYAZQBvAGUAbgBjA GUAIAAIAEUAEABjAGwAdQBzAGkAbwBuAFAAcgBvA GMAZQBzAHMAIABBAHQAdABYAGkAYgB1AHQAZQBTA HQAcbpAG4AZwAuAGUAeABlADsA	PID:548
■	C:\Users\Admin\AppData\Local\TypeId\muqnkbmby\AttributeString.exe C:\Users\Admin\AppData\Local\TypeId\muqnkbmby\AttributeString.exe	PID:468
■	C:\Users\Admin\AppData\Local\TypeId\muqnkbmby\AttributeString.exe C:\Users\Admin\AppData\Local\TypeId\muqnkbmby\AttributeString.exe	PID:1740
■	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	PID:3280
■	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	PID:2936
■	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	PID:1392
■	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe -ExecutionPolicy Bypass - WindowStyle Hidden -NoProfile -enc QQBkA GQALQBNAAUABYAGUAZgB1AHIAZQBAGMAZQAgA C0ARQB4AGMABAB1AHMAaQBvAG4AUABhAHQAaAAGA	PID:3864

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).




















Network



Requests				TCP	UDP
	DNS	76.32.126.40.in-addr.arpa			
	DNS	9.228.82.20.in-addr.arpa			
	DNS	g.bing.com			
	GET	https://g.bing.com/neg/0?action=emptycreativeimpress...			
	GET	https://g.bing.com/neg/0?action=emptycreative&adUnit...			
	GET	https://g.bing.com/neg/0?action=emptycreativeimpress...			
	DNS	179.178.17.96.in-addr.arpa			
	DNS	41.110.16.96.in-addr.arpa			
	DNS	55.36.223.20.in-addr.arpa			
	DNS	86.23.85.13.in-addr.arpa			
	DNS	18.31.95.13.in-addr.arpa			
	DNS	18.134.221.88.in-addr.arpa			
	DNS	180.178.17.96.in-addr.arpa			
	DNS	nickshort.ug	MSBUILD.EXE		
	DNS	kodedea.ug	MSBUILD.EXE		
	DNS	kodedea.ug	MSBUILD.EXE		
	DNS	junks.ac.ug	MSBUILD.EXE		
	DNS	ugas.ug	MSBUILD.EXE		
	DNS	fillah.ac.ug	MSBUILD.EXE		
	DNS		MSBUILD.EXE		
	DNS		MSBUILD.EXE		
	DNS				
	DNS				

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

	DNS	ugas.ug	MSBUILD.EXE	▼
	DNS	fillah.ac.ug	MSBUILD.EXE	▼
	DNS	nickshort.ug	MSBUILD.EXE	▼
	DNS	kodedea.ug	MSBUILD.EXE	▼
	DNS	ugas.ug	MSBUILD.EXE	▼
	DNS	fillah.ac.ug	MSBUILD.EXE	▼
	DNS	nickshort.ug	MSBUILD.EXE	▼
	DNS	kodedea.ug	MSBUILD.EXE	▼
	DNS	ugas.ug	MSBUILD.EXE	▼
	DNS	ugas.ug	MSBUILD.EXE	▼
	DNS	fillah.ac.ug	MSBUILD.EXE	▼
	DNS	nickshort.ug	MSBUILD.EXE	▼
	DNS	nickshort.ug	MSBUILD.EXE	▼
	DNS	kodedea.ug	MSBUILD.EXE	▼
	DNS	kodedea.ug	MSBUILD.EXE	▼
	DNS	ugas.ug	MSBUILD.EXE	▼
	DNS	fillah.ac.ug	MSBUILD.EXE	▼

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).



MITRE ATT&CK Enterprise

v15



Replay Monitor



Downloads



C:\Users\Admin\AppData\Local\Microsoft\CLR_v4...

Filesize

2KB

Download

Submit

Download

Submit

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

SHA512 4617591400409e1930195795a55...

C:\Users\Admin\AppData\Local\Microsoft\Windo...

Filesize	944B
MD5	77d622bb1a5b250869a3238b9bc1...
SHA1	d47f4003c2554b9dfc4c16f22460...
SHA256	f97ff12a8abf4bf88bb6497bd2ac2d...
SHA512	d6789b5499f23c9035375a102271...

Download

Submit

C:\Users\Admin\AppData\Local\Temp\BBLb.exe

Filesize	1.2MB
MD5	71eb1bc6e6da380c1cb552d78b39...
SHA1	df3278e6e26d8c0bc878fe0a8c8a...
SHA256	cefa92ee6cc2fad86c49dd37d57ff...
SHA512	d6fab2c469924b8202f7964e864f...

Download

Submit

C:\Users\Admin\AppData\Local\Temp_PSScriptP...

Filesize	60B
MD5	d17fe0a3f47be24a6453e9ef58c94...
SHA1	6ab83620379fc69f80c0242105dd...
SHA256	96ad1146eb96877eab5942ae0736...
SHA512	5b592e58f26c264604f98f6aa1286...

Download

Submit

memory/212-44-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-0-0x00000000009E0000-0x0000...

Filesize	2.2MB
----------	-------

Download

memory/212-10-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-50-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-14-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-16-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-18-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-20-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-22-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-24-0x0000000005750000-0x0000...

Filesize	2.0MB
----------	-------

Download

memory/212-26-0x0000000005750000-0x0000...

Download

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

Download

Download

Download

Download

Filesize	2.0MB	
memory/212-34-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-36-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-38-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-54-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-42-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-6-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-46-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-48-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-12-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-8-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-40-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-56-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-58-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-60-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-62-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-64-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	
memory/212-66-0x0000000005750000-0x0000...		Download
Filesize	2.0MB	

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

Filesize	1.6MB	
memory/212-938-0×0000000005B00000-0×00...		Download
Filesize	304KB	
memory/212-4-0×0000000005750000-0×00000...		Download
Filesize	2.0MB	
memory/212-3-0×0000000005750000-0×00000...		Download
Filesize	2.0MB	
memory/212-951-0×0000000007CF0000-0×000...		Download
Filesize	5.6MB	
memory/212-2-0×0000000005750000-0×00000...		Download
Filesize	2.0MB	
memory/212-1-0×00000000075130000-0×00000...		Download
Filesize	7.7MB	
memory/212-52-0×0000000005750000-0×0000...		Download
Filesize	2.0MB	
memory/212-961-0×00000000075130000-0×000...		Download
Filesize	7.7MB	
memory/468-4146-0×00000000075130000-0×00...		Download
Filesize	7.7MB	
memory/468-5079-0×0000000005300000-0×0...		Download
Filesize	4KB	
memory/468-5086-0×00000000075130000-0×00...		Download
Filesize	7.7MB	
memory/548-4138-0×00000226F1BA0000-0×00...		Download
Filesize	64KB	
memory/548-4143-0×00007FF872E50000-0×00...		Download
Filesize	10.8MB	
memory/548-4139-0×00000226F1BA0000-0×00...		Download
Filesize	64KB	
memory/548-4140-0×00000226F15F0000-0×00...		Download
Filesize	136KB	
memory/548-4137-0×00007FF872E50000-0×00...		Download
Filesize	10.8MB	
memory/1392-8228-0×00000000058B0000-0×...		Download
Filesize	64KB	

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

Filesize	7.7MB	
memory/1552-1912-0x00000000053A0000-0x0...		Download
Filesize	768KB	
memory/1552-950-0x000000000530000-0x0...		Download
Filesize	1.2MB	
memory/1552-952-0x0000000075130000-0x00...		Download
Filesize	7.7MB	
memory/1552-1919-0x0000000075130000-0x0...		Download
Filesize	7.7MB	
memory/1552-956-0x0000000005020000-0x0...		Download
Filesize	1.2MB	
memory/1552-955-0x0000000004E70000-0x00...		Download
Filesize	64KB	
memory/1552-1911-0x0000000004E50000-0x0...		Download
Filesize	4KB	
memory/1552-954-0x0000000004E80000-0x0...		Download
Filesize	1.2MB	
memory/1740-5084-0x0000000075130000-0x0...		Download
Filesize	7.7MB	
memory/1740-5085-0x0000000005650000-0x0...		Download
Filesize	64KB	
memory/1740-7290-0x0000000075130000-0x0...		Download
Filesize	7.7MB	
memory/2052-1274-0x0000000003A90000-0x0...		Download
Filesize	4.0MB	
memory/2052-963-0x000000000400000-0x0...		Download
Filesize	544KB	
memory/2052-1279-0x0000000003A90000-0x...		Download
Filesize	4.0MB	
memory/2052-1322-0x0000000003A90000-0x...		Download
Filesize	4.0MB	
memory/2616-1921-0x0000000004F20000-0x0...		Download
Filesize	928KB	
memory/2616-1920-0x0000000075130000-0x0...		Download
Filesize	7.7MB	

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).



Filesize	344KB	
memory/2616-1922-0x0000000005020000-0x0...		Download
Filesize	64KB	
memory/2616-4127-0x0000000075130000-0x0...		Download
Filesize	7.7MB	
memory/2616-1918-0x0000000000400000-0x0...		Download
Filesize	624KB	
memory/2936-7288-0x0000000075130000-0x0...		Download
Filesize	7.7MB	
memory/2936-7289-0x00000000053E0000-0x...		Download
Filesize	64KB	
memory/2936-8223-0x0000000005550000-0x...		Download
Filesize	4KB	
memory/2936-8229-0x0000000075130000-0x0...		Download
Filesize	7.7MB	
© 2018-2024		
memory/3484-1297-0x0000000001F90000-0x0...		

[Terms](#) | [Privacy](#)

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).