

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

567f528fec8e7a4787f8c253446d8f1b620dc9d6



SHA256

217fbf967c95d1359314fcd53ae8d04489eb3c7bdc1f22110d5a8a476d1fc92e



SHA512

341acbd43efac1718c7f3e3795549acf29237a2675bdadcb7e52ce18aac6dcc6ae628e1b6edfa2338ed6d9923c148cb4322c75fad86d5c0e6f2327c2270563ec



SSDEEP

49152:/WlrvpDXJLRxe123BMGwxB19y0IEjaV/EC5O7pD:/apzJy1kMxt2R/ET



Score

10^{/10}

RHADAMANTHYS

ZGRAT

RAT

STEALER



Malware Config



Signatures



Discovery

Detect ZGRat V1 • 36 IoCs

Rhadamanthys

Rhadamanthys is an info stealer written in C++ first seen in August 2022.

RHADAMANTHYS

STEALER

Suspicious use of NtCreateUserProcessOtherParentProcess • 1 IoCs

ZGRat

ZGRat is remote access trojan written in C#.

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

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

Suspicious use of WriteProcessMemory • 56 IoCs


























Processes



<div><div></div><div>C:\Windows\system32\sihost.exe</div></div> <div>sihost.exe</div>	PID:2528
<div><div></div><div>C:\Windows\SysWOW64\dialer.exe</div></div> <div>"C:\Windows\system32\dialer.exe"</div>	PID:3484
<div><div></div><div>C:\Users\Admin\AppData\Local\Temp\native.exe</div></div> <div>"C:\Users\Admin\AppData\Local\Temp\native.exe"</div>	PID:212
<div><div></div><div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div></div> <div>"C:\Users\Admin\AppData\Local\Temp\BBLb.exe"</div>	PID:1552
<div><div></div><div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div></div> <div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div>	PID:1940
<div><div></div><div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div></div> <div>C:\Users\Admin\AppData\Local\Temp\BBLb.exe</div>	PID:2616
<div><div></div><div>C:\Users\Admin\AppData\Local\Temp\native.exe</div></div> <div>C:\Users\Admin\AppData\Local\Temp\native.exe</div>	PID:2052
<div><div></div><div>C:\Windows\SysWOW64\WerFault.exe</div></div> <div>C:\Windows\SysWOW64\WerFault.exe -p 2052 -s 448</div>	PID:4572
<div><div></div><div>C:\Windows\SysWOW64\WerFault.exe</div></div> <div>C:\Windows\SysWOW64\WerFault.exe -p 2052 -s 444</div>	PID:3172
<div><div></div><div>C:\Windows\SysWOW64\WerFault.exe</div></div> <div>C:\Windows\SysWOW64\WerFault.exe -p 2052 -ip 2052</div>	PID:1560
<div><div></div><div>C:\Windows\SysWOW64\WerFault.exe</div></div> <div>C:\Windows\SysWOW64\WerFault.exe -p 2052 -ip 2052</div>	PID:3808
<div><div></div><div>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</div></div> <div>powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -enc QQBkAGQALQBNAHAUAByAGUAZgBIAHIAZQBAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAqAAgAEMA0gBcAFUAcwBIAHIAcwBcAEEAZABtAGkAbgBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwAOwAgAEEAZABkAC0ATQBwAFAAcgBIAGYAZQByAGUAbgBjAGUAIAtAEU AeABjAGwAdQBzAGkAbwBuAFAAcgBvAGMAZQBzAHMAIABBAHQAdABYAGkAYgB1AHQAZQBTAHQAcgBpAG4AZwAuAGUAeABlADsA</div>	PID:548
<div><div></div><div>C:\Users\Admin\AppData\Local\Temp\d\muqnkbmby\AttributeString.exe</div></div> <div></div>	PID:468
	PID:1740

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	175.178.17.96.in-addr.arpa		▼
	DNS	30.243.111.52.in-addr.arpa		▼
	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
MD5	d85ba6ff808d9e5444a4b369f5bc...
SHA1	31aa9d96590fff6981b315e0b391b...
SHA256	84739c608a73509419748e4e20e...
SHA512	8c414eb55b45212af385accc16d9...

Download

Submit

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

Filesize	927B
MD5	4a911455784f74e368a4c2c7876d...
SHA1	a1700a0849ffb4f26671eb76da248...

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](#).

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/212-44-0×0000000005750000-0×0000...

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

Download

memory/212-0-0×00000000009E0000-0×0000...

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

Download

memory/212-10-0×0000000005750000-0×0000...

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

Download

memory/212-50-0×0000000005750000-0×0000...

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

Download

memory/212-14-0×0000000005750000-0×0000...

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

Download

memory/212-16-0×0000000005750000-0×0000...

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

Download

memory/212-18-0×0000000005750000-0×0000...

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

Download

memory/212-20-0×0000000005750000-0×0000...

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

Download

memory/212-22-0×0000000005750000-0×0000...

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

Download

memory/212-24-0×0000000005750000-0×0000...

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

Download

memory/212-26-0×0000000005750000-0×0000...

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

Download

memory/212-28-0×0000000005750000-0×0000...

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

Download

memory/212-30-0×0000000005750000-0×0000...

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

Download

memory/212-32-0×0000000005750000-0×0000...

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

Download

memory/212-34-0×0000000005750000-0×0000...

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

Download

memory/212-36-0×0000000005750000-0×0000...

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

Download

memory/212-38-0×0000000005750000-0×0000...

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

Download

memory/212-54-0×0000000005750000-0×0000...

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

Download

memory/212-42-0×0000000005750000-0×0000...

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

memory/212-48-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-12-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-8-0×0000000005750000-0×00000...	Download
Filesize2.0MB	
memory/212-40-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-56-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-58-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-60-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-62-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-64-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-66-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-935-0×0000000005740000-0×000...	Download
Filesize64KB	
memory/212-936-0×0000000001670000-0×000...	Download
Filesize4KB	
memory/212-937-0×0000000005960000-0×000...	Download
Filesize1.6MB	
memory/212-938-0×0000000005B00000-0×00...	Download
Filesize304KB	
memory/212-4-0×0000000005750000-0×00000...	Download
Filesize2.0MB	
memory/212-3-0×0000000005750000-0×00000...	Download
Filesize2.0MB	
memory/212-951-0×0000000007CF0000-0×000...	Download
Filesize5.6MB	
memory/212-2-0×0000000005750000-0×00000...	Download
Filesize2.0MB	
memory/212-1-0×0000000075130000-0×00000...	Download
Filesize7.7MB	
memory/212-52-0×0000000005750000-0×0000...	Download
Filesize2.0MB	
memory/212-961-0×0000000075130000-0×000...	Download
Filesize7.7MB	
memory/468-4146-0×0000000075130000-0×00...	Download
Filesize7.7MB	
memory/468-5079-0×0000000005300000-0×0...	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](#).

Filesize	10.8MB	Download
memory/548-4139-0x00000226F1BA0000-0x00...		
Filesize	64KB	Download
memory/548-4140-0x00000226F15F0000-0x00...		
Filesize	136KB	Download
memory/548-4137-0x00007FF872E50000-0x00...		
Filesize	10.8MB	Download
memory/1392-8228-0x00000000058B0000-0x...		
Filesize	64KB	Download
memory/1392-10447-0x00000000058B0000-0x...		
Filesize	64KB	Download
memory/1392-10446-0x0000000075130000-0x...		
Filesize	7.7MB	Download
memory/1392-8227-0x0000000075130000-0x0...		
Filesize	7.7MB	Download
memory/1552-1912-0x00000000053A0000-0x0...		
Filesize	768KB	Download
memory/1552-950-0x0000000000530000-0x0...		
Filesize	1.2MB	Download
memory/1552-952-0x0000000075130000-0x00...		
Filesize	7.7MB	Download
memory/1552-1919-0x0000000075130000-0x0...		
Filesize	7.7MB	Download
memory/1552-956-0x0000000005020000-0x0...		
Filesize	1.2MB	Download
memory/1552-955-0x0000000004E70000-0x00...		
Filesize	64KB	Download
memory/1552-1911-0x0000000004E50000-0x0...		
Filesize	4KB	Download
memory/1552-954-0x0000000004E80000-0x0...		
Filesize	1.2MB	Download
memory/1740-5084-0x0000000075130000-0x0...		
Filesize	7.7MB	Download
memory/1740-5085-0x0000000005650000-0x0...		
Filesize	64KB	Download
memory/1740-7290-0x0000000075130000-0x0...		
Filesize	7.7MB	Download
memory/2052-1274-0x0000000003A90000-0x0...		
Filesize	4.0MB	Download
memory/2052-963-0x000000000400000-0x0...		
Filesize	544KB	Download
memory/2052-1279-0x0000000003A90000-0x...		
Filesize	4.0MB	Download
memory/2052-1322-0x0000000003A90000-0x...		
		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](#).



Filesize	336KB	Download
memory/2616-4124-0x0000000005300000-0x0...		
Filesize	408KB	Download
memory/2616-4123-0x00000000050A0000-0x0...		
Filesize	344KB	Download
memory/2616-1922-0x0000000005020000-0x0...		
Filesize	64KB	Download
memory/2616-4127-0x00000000075130000-0x0...		
Filesize	7.7MB	Download
memory/2616-1918-0x0000000000400000-0x0...		
Filesize	624KB	Download
memory/2936-7288-0x00000000075130000-0x0...		
Filesize	7.7MB	Download
memory/2936-7289-0x00000000053E0000-0x...		
Filesize	64KB	Download
memory/2936-8223-0x0000000005550000-0x...		
Filesize	4KB	Download

© 2018-2024

[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](#).