

"SwimSnake (Silver Fox)" Black Market Intensely Counterfeits Various Popular Applications: WPS Download Station's Anti-Counterfeiting Special Report

2025/10/10

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

1 Overview

The "SwimSnake" attack group and other security enterprises, also known as "Silver Fox" and "Valley Gang Thieves," mainly target domestic users to carry out attacks and fraud activities. In the second half of 2022, Antiy has discovered and analyzed the early activities of the organization, including camouflage common software download station, SEO of search engine and phishing mail, and carry out the operation in the form of white and black. The instant messaging software (WeChat, Corporate WeChat, etc.) was used to further spread. Its main way of profit is through the instant messaging software pull the group to carry on the fraud, at the same time also forms to the infection host the ability to steal secret, possibly carries on the data to sell and so on other activities. The variety of malicious documents spread by it is very numerous, the method of avoiding killing is very frequent, and the influence of individuals and industries is extremely extensive.

Antiy CERT keeps track of the "SwimSnake" gang, and finds that the group uses a series of popular apps to fish and spread them, especially the phenomenon of swimming snake on Google and Bing search engines has become a major disaster area. Forged station and official website not only website content is highly similar, in domain name imitation is also extremely lifelike, once the user misbelieves and downloads the malicious installation package, "SwimSnake" remote control Trojan will implant the system. To achieve the remote control of the target equipment, theft of sensitive data and fraud operations.

This report sorts out the recent cases of phishing and spreading by the "SwimSnake" organization in imitation of the WPS website, and all the cases involved have survived, and each case has been classified and summarized through the attack method. Formation of WPS software download station anti-fake album. In daily office work, the user shall be alert to the phishing trap of all kinds of counterfeit software, be sure to download and update the software

through regular channels, carefully check the website address and certificate, and install terminal security protection software for system protection.

With enhanced download protection, Antiy IEP supports the management and control of browser, instant messaging software and email client portals to detect the receiving and downloading behaviors. So that the malware can not easily land on the local disk or boot, so that most malicious files are blocked in the load before execution.

Download Enhanced Protection Details: "IEP EDR" download enhanced protection, "so that the SwimSnake can not run up"

2 A Case of Imitation WPS Program of SwimSnake Black Production

Antiy CERT found in the daily tracking of the organization "snake swimming," that the organization phishing spread a large number of fake WPS software websites, and analyzed the documents downloaded from the fake websites and refined the attack methods. Form four groups of cases to share. Relevant methods have been disclosed in Antiy's historical release report. for further information, please visit the emergency response analysis module of Antiy's official website for reference. (https://www.antiy.cn/research/notice&report/research_report/index.html)

2.1 Case 1 of Copying WPS Website

Google search for "WPS download" shows that the 3rd, 5th and 6th digits of page 1 are all fake phishing websites created by the "SwimSnake" organization, and the result is as follows:



Figure 2-1 Google search engine results1

As shown in the figure of the page of the fishing website, it is difficult to distinguish whether the page is an official page from the page of the fishing website:

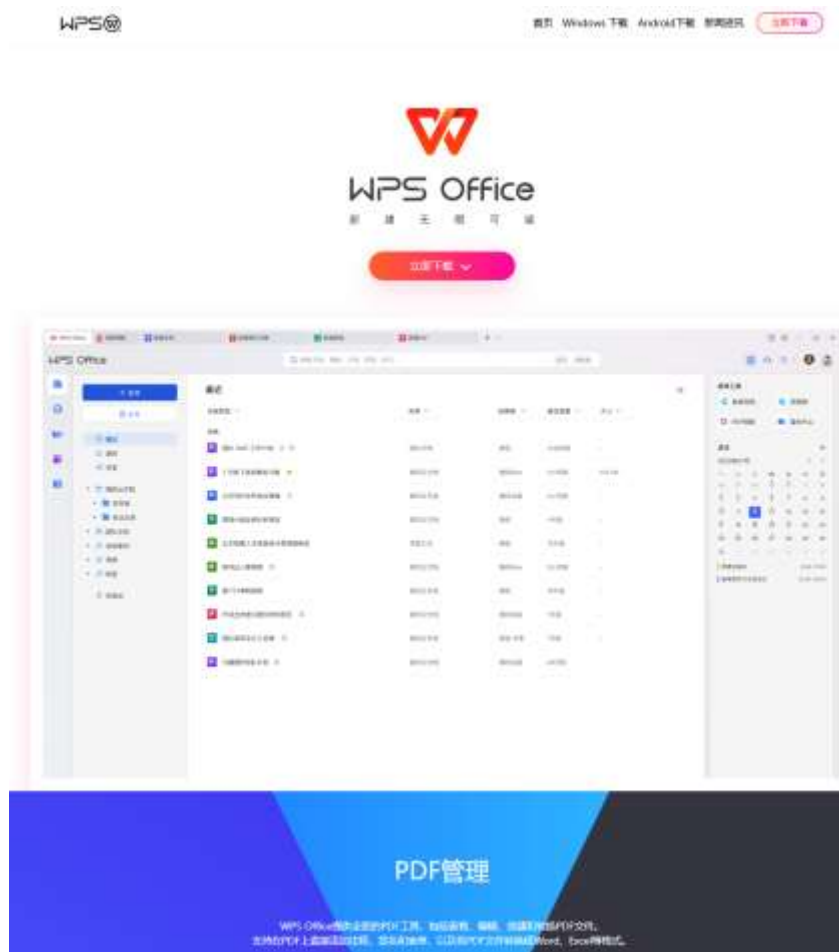


Figure 2-2 Page of a phishing website2

The following table shows an overview of the 3rd, 5th and 6th case filter re-analysis of Google's search engine results for fake WPS websites:

Table 2-1 Overview of Case 1 1

| | |
|--|--|
| Counterfeit applications | WPS |
| File name | Wgtfdhg (2) .exe WhxsaigWPSbn - 1.6.1.exe |
| Md5 | 395f257e1180ce2e7d13b80f716a3eae D07b929ce2c5ea59824c170ce6b755e1 |
| Introduction to the technique | The initial program is packaged using NSIS, which contains the command-line version of the RAR program, an encrypted jpg file that contains the "white plus black" file, and the normal WPS installer. |
| Link to corresponding reporting method | https://www.antiy.cn/research/notice&report/research_report/20230330.html |
| Phishing website domain name | https://www-wps.org/ https://www.wps1.com/ https://www.wps2.com/ https://cn-wps.com/ |

| | |
|-------------------------|---|
| | https[:]//zhs-wps.com/ |
| Malicious download link | https[:]//wsi.irdInc.top/Whotefjfsvo-1.6.7.zip https[:]//wsi.irdInc.top/whxsaigwpsbn-1.6.1.zip https[:]//honing.oss-ap-southeast-1.aliyuncs.com/Wp_s_BG.rar |
| Digital signature | Skutta, Kristjan Blizzard Entertainment, Inc. Guangzhou Tiger Teeth Information Technology Co., Ltd (Digital signature is invalid) |

2.2 Case 2 of Copying WPS Website

A bing search for "WPS" shows that the third digit on page 1 is a fake phishing website created by the "SwimSnake" organization, and the result is shown in the figure below:

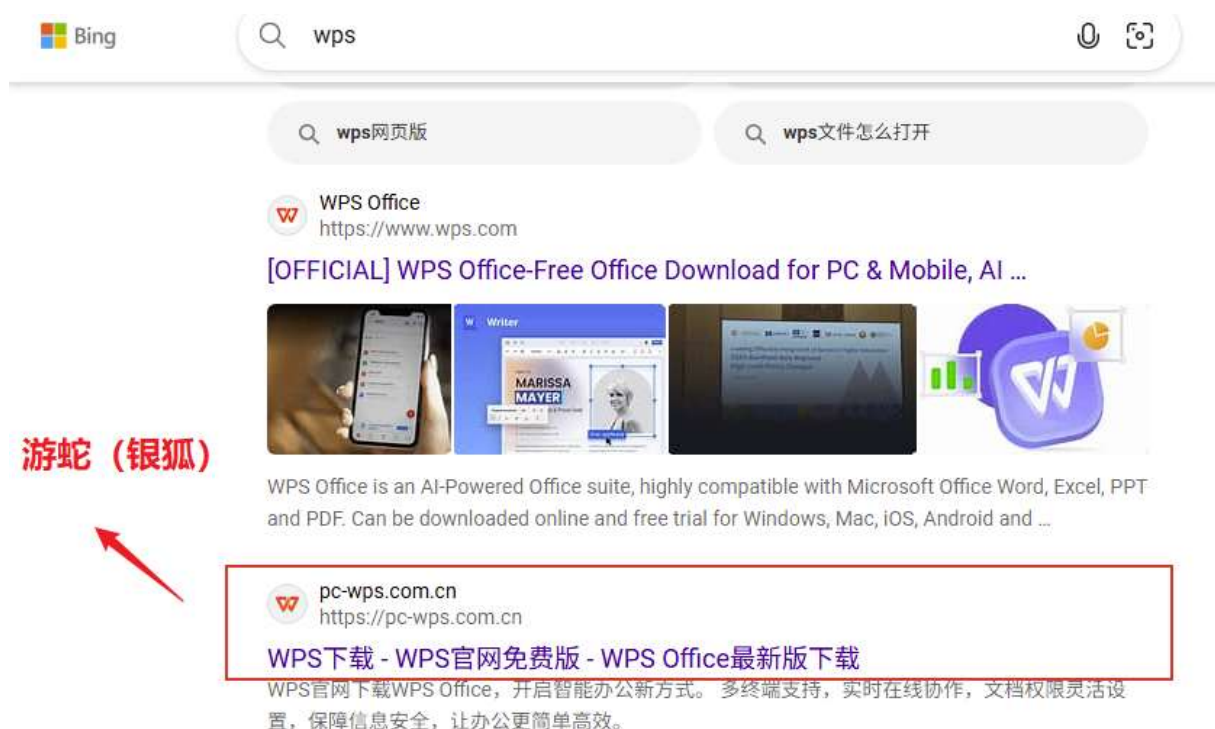


Figure 2-3 Results of the bing search engine3

As shown in the figure of the page of the fishing website, it is difficult to distinguish whether the page is an official page from the page of the fishing website:

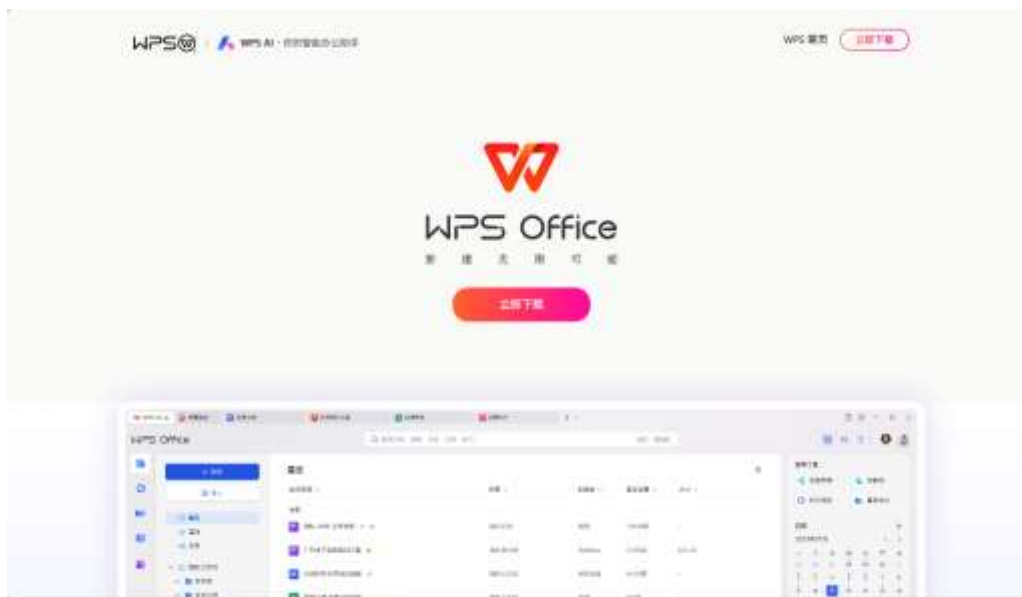


Figure 2-4 Page of a phishing website4

The following table shows an overview of cases of phishing of WPS websites:

Table 2-2 Overview of Case 2

| | |
|--|--|
| Counterfeit applications | WPS |
| File name | WPS _ Setup _ X64-43545.msi WPS _ Setup _ X64-953.msi |
| Md5 | 850cca9842ef88bdc9c3d6ef438416be D6978123f086d9e6fb825e7d5db65f16 |
| Brief Introduction to Attacking Techniques | The initial MSI program contains a normal WPS installer, as well as malicious components. The malicious component loads the malicious DLL file named "QQMusic.dll" by using the method of "white plus black," and realizes persistence through the registry, and reads the txt file and writes it into the applied memory. The txt file is Shellcode, and the final execution of Gh0st remote control Trojan. |
| Link to corresponding reporting method | https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202505.html |
| Phishing website domain name | https://pc-wps.com.cn https://wps-zh.com.cn |
| Malicious download link | https://1aad538cdb1479fb6921ff8ed872ab30.linkgodrive[.]icu/WPS_Setup_X64.zip https://a5f5e388a9033b039abc5145fbcd8f6c.ypio.icu/WPS_Setup_X64_2544.zip?skkey=a23b0dc3096bb68062343cde2a3eeb6035eea8eecd0de89db8ea6c256afe2b17 |
| Digital signature | None |

2.3 Case 3 of Copying WPS Website

A search for "WPS download" on Bing's web page shows that the 4th, 7th, 10th and 11th digits of Page 1 are all fake fishing websites created by the "SwimSnake" organization, and the result is shown as follows:

"SwimSnake (Silver Fox)" Black Market Intensely Counterfeits Various Popular Applications: WPS Download Station's Anti-Counterfeiting Special Report



Figure 2-5 Bing search engine results5

As shown in the figure of the page of the fishing website, it is difficult to distinguish whether the page is an official page from the page of the fishing website:



Figure 2-6 Page of a phishing website

The table below shows an overview of the 4th and 7th fake WPS websites of the Bing web search "WPS download" results:

Table 2-3 Overview of Case 32

| | |
|--|---|
| Counterfeit applications | WPS |
| File name | WPSsetup.exe |
| Md5 | 576f7f40cea79d1dbdfd4f0c08e79fa4 0b7c574e1503841c7eb2b1c5db8a6f3c |
| Brief Introduction to Attacking Techniques | The initial procedure is obfuscated to obtain malicious files from the attacker Alibaba Cloud OSS. The malicious file attempts to terminate the designated anti-virus product process and service, and obtains a group of "white plus black" malicious files from the attacker Alibaba Cloud OSS. The overall attack flow is similar to the sample in "The Spreading of Snake (Silver Fox) Black Products and the Continuous Tracking of Techniques and Tactics: Analysis of Attacks by Picking FinalShell Management |

| | |
|--|---|
| | Software." |
| Link to corresponding reporting method | https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202509.html |
| Phishing website domain name | https://www.kingsoftwps.com.cn/ https://wps-cn.net/ |
| Malicious download link | https://dowshfgfr5.s3.us-east-005.backblazeb2.com/WpsSetup.zip |
| Digital signature | None |

2.4 Case 4 of Copying WPS Website

As shown in the figure of the page of the fishing website, it is difficult to distinguish whether the page is an official page from the page of the fishing website:



Figure 2-7 Page of a phishing website

The following table shows an overview of the 10th spoofed WPS website of the Bing web search for "WPS downloads":

Table 2-4 Overview of Case 43

| | |
|--------------------------------------|---|
| Counterfeit applications | WPS |
| File name | Wjfrpsl.exe |
| Md5 | 05946b9848551eb738c9fdf748af0ff2 |
| Introduction to the technique | Package with InnoSetup, the package contains man100.dat, funzip.U, main.xml, Server. log, and is released to C:\ ProgramData\ Windows Data. Funzip.u is a 7za tool, which decompresses the main .xml file with the specified password "htLcenyRFYwXsHFUnqK," and executes the normal WPS installation program and malicious program. By executing UAC bypass tool, BYOVD attack component and powershell adding exclusion, the white plus black component is used to execute the final Winos remote control Trojan horse. |
| Phishing website domain name | https[:]//www.bg-wps.com/ |
| Malicious download link | https[:]//pub-3d7ecf8d8ed94374b9fb10d61138bd72.r2.dev/Wjfrpsl.zip |
| Digital signature | None |

3 Characteristics and Identification of Fishing Websites

Phishing sites masquerade as trusted services or institutions to steal user accounts, passwords, payment information or spread malware. They tend to be realistic in appearance, but there are hints of detail. Understanding common characteristics and grasping quick identification methods can reduce the risk of being cheated in the first time, and protect personal and enterprise information security.

3.1 Common characteristics of phishing website domain names

1. Replace or add characters: A phishing website usually uses a domain name similar to a regular website, and a normal website domain name usually has the following structure: Xxx.software name .cn. Phishing sites that fake WPS use similar domain names such as "WPS1," "WPS2," "WPSkr," "kingsoftWPS."
2. Add prefixes: Add extra characters before and after the real domain name, such as "cn-WPS," "zhs-WPS," "WPS-cn" and similar domain names.
3. Subdomain name camouflage: Use subdomain names to confuse the public, for example, the domain name of the WPS website is "WPS.cn" and the attacker uses similar domain names such as "WPS.com.cn" (actually the subdomain name of com.cn).

Table 3-1 Summary of characteristics of domain names of fishing websites1

| Normal website domain name | Phishing website domain name | Techniques employed |
|-------------------------------|------------------------------|--|
| Platform.WPS.cn Www.WPS.cn | Www.WPSkr.com | Replace or add characters |
| | Www.WPS1.com | |
| | Www.WPS2.com | |
| | Www.bg-WPS.com | Add the prefix suffix |
| | Www.WPS.org | |
| | Cn-WPS.com | |
| | Zhs-WPS.com | |
| | WPS-cn.net | |
| | Www.kingsoftWPS.com.cn | Replace or add characters, subdomain name camouflage |
| | Pc-WPS.com.cn | Add presuffix, subdomain name camouflage |
| | WPS-zh.com.cn | |

3.2 Common Features of Pages on Fishing Websites

1. Interface imitation: When setting up a website, the organization will imitate the official website, so the interface setting will be very similar, almost the same as the page of the official website. It's hard to tell if it's a fishing site by the naked eye.
2. There are other problems with the web page: The organization of "SwimSnake" can only imitate the homepage of the official website, and it will not cost a lot to produce the website, and there will be many problems. For example, the response time of the download button is too slow, the page is not fully loaded, the jump link is invalid, and there are download links of other non-own products.







Figure 3-1 Identification of Fishing Web Page1

3.3 Common Features of Downloading Files from Fishing Websites

1. Whether the file name downloaded is correct or not: The file name of the file downloaded on the official website is generally "Name + Setup," most of which are executable files. And the file name of phishing website download mostly carries on the name with irregular way, and what download is "swim snake Trojan horse" the form that is compressed package mostly.
2. Download the file icon is correct: Phishing website download the icon of the file and our common software icon will exist some differences, mostly in imitation.
3. Whether the downloaded document has digital signature or not: The documents downloaded from the official website all bear the digital signature of the company, and the certificate is valid. Files downloaded by phishing websites generally do not carry digital signatures, and a few files with digital signatures are inconsistent with those of software companies, and the certificates are in an invalid state.

Table 3-2 Common characteristics of downloaded files from fishing websites2

| Common Features of Download Files | Formal website | Phishing websites |
|-----------------------------------|---|---|
| Download file name | WPS_Setup_22529.exe | tpoanse-x64.2.6.3.zip、Wjfrpsl.zip、WPS_Setup_X64-43545_msi.zip 、 WPS_Setup_X64_2544.zip 、 Wp_s_BG.rar |
| Icon |  |    |
| Digital signature | Zhuhai Kingsoft Office Software Co., Ltd. (Digital signature is invalid) | Skutta, Kristjan Blizzard Entertainment, Inc. (Digital signature is invalid) |

4 IoC

395f257e1180ce2e7d13b80f716a3eae
D07b929ce2c5ea59824c170ce6b755e1
850cca9842ef88bdc9c3d6ef438416be
D6978123f086d9e6fb825e7d5db65f16
0b7c574e1503841c7eb2b1c5db8a6f3c
576f7f40cea79d1dbdfd4f0c08e79fa4

| |
|---|
| 05946b9848551eb738c9fdf748af0ff2 |
| Www.WPS [.] org |
| Www.WPS1 [.] com |
| Www.WPS2 [.] com |
| Cn-WPS [.] com |
| Zhs-WPS [.] com |
| Pc-WPS.com [.] cn |
| WPS-zh.com [.] cn |
| WPS-cn [.] net |
| Www.WPSkr [.] com |
| Www.kingsoftWPS.com [.] cn |
| WPS-cn [.] net |
| Www.bg-WPS [.] com |
| Https [:] / / wsi.irdInc.top / Whotefjfsvo-1.6.7.zip |
| Https [:] / / wsi.irdInc.top / whxsaigWPSbn-1.6.1.zip |
| Https [:] / / honing.oss-ap-southeast-1.aliyuncs.com / Wp _ s _ BG.rar |
| Https [:] / / 1aad538cdb1479fb6921ff8ed872ab30.linkgodrive [.] icu / WPS _ Setup _ X64.zip |
| Https [:] / / a5f5e388a9033b039abc5145fbed8f6c.ypio.icu / WPS _ Setup _ X64 _ 2544.zip? Key = a23b0dc3096bb68062343cde3eeb 6035eea8eecd0de89db8ea6c256afe2b17 |
| Hxxps [:] / / dowshfgfr5.s3.us-east-005.backblazeb2 [.] com / WPSSetup.zip |
| Https [:] / / pub-3d7ecf8d8ed94374b9fb10d61138bd72.r2.dev / Wjfrpsl.zip |

List of Antiy's historical reports on the threat of "SwimSnake.

[1] Analysis of attacks on remote control Trojans placed by falsifying Chinese Telegram websites [R/OL]. (2022-10-24)

https://www.antiy.cn/research/notice&report/research_report/20221024.html

[2] Analysis of attacks on remote control Trojan delivered by cloud note-taking platform [R/OL]. (2023-03-24)

https://www.antiy.cn/research/notice&report/research_report/20230324.html

[3] Analysis of gangs using cloud note-taking platform to deliver remote-controlled Trojans [R/OL]. (2023-03-30)

https://www.antiy.cn/research/notice&report/research_report/20230330.html

[4] Analysis of large-scale attacks launched by "SwimSnake" gangs against domestic users [R/OL]. (2023-05-18)

https://www.antiy.cn/research/notice&report/research_report/20230518.html

[5] Analysis of recent fishing attacks by "SwimSnake" gangs [R/OL]. (2023-07-11)

https://www.antiy.cn/research/notice&report/research_report/TrojanControl_Analysis.html

[6] Analysis of the activities of the "SwimSnake" gang in using WeChat to spread malicious codes [R/OL]. (2023-08-22)

https://www.antiy.cn/research/notice&report/research_report/SnakeTrojans_Analysis.html

[7] Special Analysis Report on "SwimSnakes" and Black Producers [R/OL]. (2023-10-12)

https://www.antiy.cn/research/notice&report/research_report/SwimSnakeTrojans_Analysis.html

[8] Analysis of the new round of attacks against financial personnel and e-commerce customer service by the "SwimSnake" gang [R/OL]. (2023-11-11-11)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis.html

[9] Analysis of the recent attack activities of the "SwimSnake" black industry [R/OL]. (2024-04-07)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202404.html

[10] Analysis of phishing attacks by "SwimSnake" gangs using malicious documents [R/OL]. (2024-06-21)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202406.html

[11] The phishing download website spreads the threat of "SwimSnake," and the malicious installer hides the remote control Trojan [R/OL]. (2024-12-20)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202412.html

[12] Special inspection and handling of "SwimSnake" attacks on black products that are rampant and quickly activated [R/OL]. (2025-04-23)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202504.html

[13] The black production of "SwimSnake" uses fake WPS Office download stations to spread remote control Trojans [R/OL]. (2025-05-15)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202505.html

[14] "SwimSnake (Silver Fox)" attacks by the latest variety of black production [R/OL]. (2025-08-17)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202508.html

[15] The spreading of black products and continuous tracking of techniques and tactics of SwimSnake (silver fox): Analysis of attack methods of imitation FinalShell management software [R/OL]. (2025-09-19)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202509.html