

JOINT CYBER SECURITY ADVISORY



National Cyber
Security Centre
a part of GCHQ

23 Nov 2023

DPRK state-linked cyber actors conduct software supply chain attacks



Overview

The National Intelligence Service (NIS) of the Republic of Korea (ROK) and the National Cyber Security Centre (NCSC) of the United Kingdom (UK) have identified Democratic People's Republic of Korea (DPRK) state-linked cyber actors targeting software supply chain products, widely used by government organisations, financial institutions and defence industry companies globally.

The NIS and the NCSC are releasing this joint Cybersecurity Advisory (CSA) to help prevent compromise and raise public awareness. It includes DPRK state-linked cyber actors' tactics, techniques and procedures (TTPs) used in their global supply chain attacks, as well as preventative measures to help avoid such attacks.

Further Details

In recent years, supply chain attacks from DPRK state-linked cyber actors have steadily increased in volume and have become more sophisticated. The malicious actors utilise tactics including zero-day attacks and multiple exploits to attack software supply chain products, used by a number of international organisations.

The NIS and the NCSC consider these supply chain attacks to align and considerably assist with the fulfilment of wider DPRK state priorities. This includes revenue generation and espionage, with the theft of advanced technologies across a range of sectors, including but not limited to defence.

Supply chain attacks are a highly effective means of compromising numerous well-protected, high-profile targets. Several elements of the supply chain have proved susceptible to compromise, including software vendors, managed service providers and cloud providers. From here, an actor can indiscriminately target a number of organisations and users, and their attacks can be expanded or shifted to a ransomware attack to demand money or cause a system disruption.

It can be hard to detect these attacks as the actors are using legitimate software and hardware.

With the level of the threat likely to increase, organisations should establish and put in place relevant security measures to safely manage the security of the products and to build resilience to attacks.



Technical Details

For software supply chain attacks, DPRK state-linked cyber actors have used zero-day exploits and newly published vulnerabilities and tools, as well as exploited multiple vulnerabilities in series, to precisely attack a specific target.

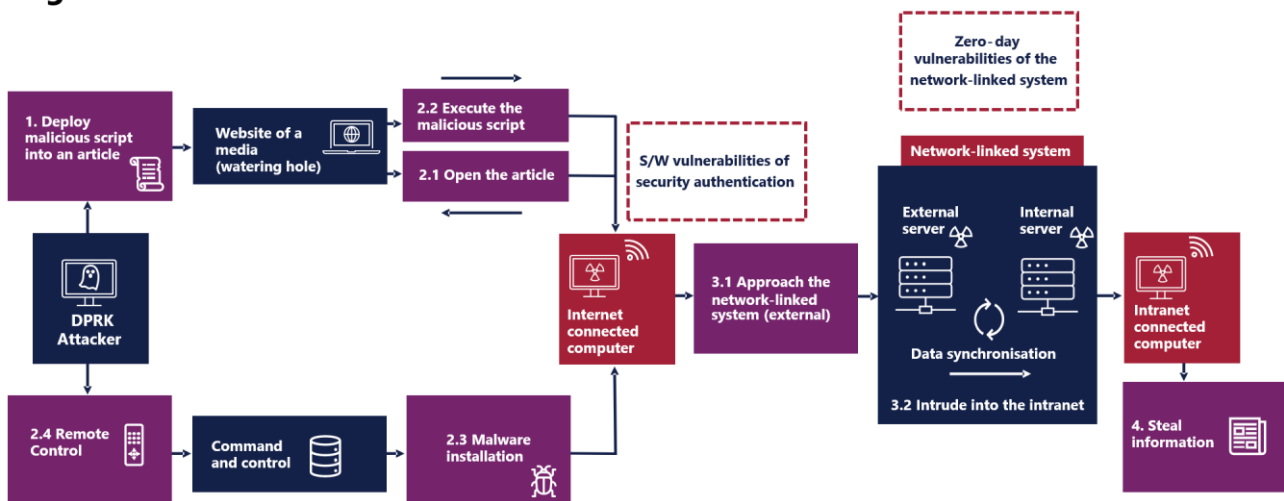
Below are recent supply chain attacks conducted by DPRK-based actors, detailing their attack flow and modi operandi.

Attacks on various supply chain products, using zero-day vulnerabilities:

In March 2023, cyber actors used the software vulnerabilities of security authentication and network-linked systems in series to gain unauthorised access to the intranet of a target organisation. It used a software vulnerability of the MagicLine4NX security authentication program for the initial intrusion into an internet-connected computer of the target, and exploited a zero-day vulnerability of the network-linked system to move laterally and gain unauthorised access to information.

The attack flow below shows the procedure of serial complex attacks on two supply chain products:

Figure 1.



Attack Flow:

1. The cyber actors compromised the website of a media outlet, deployed malicious scripts into an article and created a watering hole. The malicious scripts were implemented to work when certain IP ranges were connected.
2. When victims opened the infected article from an internet-connected computer,

which was installed with the vulnerable security authentication software, the vulnerable software executed the malicious code. The victim computer then connected to the command and control (C2), and the attackers used the C2 to achieve remote control over the infected computer.

3. The actors were able to access an internet-side server from an internet-connected PC without permission through a network-linked system vulnerability, and exploit the data synchronisation function of the network-linked system to spread malicious code to the business side server. The actors then compromised the business PC with malicious code to steal information.
4. Malicious code installed on the business PC had two C2 servers, the first of which was the business side server of the network-linked system, which acts as a gateway in the middle, while the second C2 is located on the external internet. This malicious code was able to exfiltrate initial beacon data and download and execute encrypted payloads. The malicious code then attempted to move from the internal server of the network-linked solution to the external server to send the initial beacon to the C2 server, but was blocked by the security policy of the solution. If it hadn't been blocked, large amounts of information stored in the internal network could have been leaked.

See the IoC section for C2 server, MD5 hashes, encryption algorithms, and file certificates. Further detailed information on the security authentication software attack can be found on the [English](#) and [Korean](#) language blogs by Ahnlab.

Summary and Preventative Measures

The cyber actors initially employed a watering-hole attack to secure target groups, and conducted additional attacks on specific targets. The compromise of one supply chain led to the infection of another supply chain, which was a targeted attack against a specific target. The malicious actors used highly sophisticated modus operandi by exploiting an undisclosed vulnerability of the network-linked system and a legitimate function for intrusion into the intranet.

System owners should check whether a vulnerable version of software is on the list of installed programs, and update the software to the latest version.

MagicLine4NX 1.0.0.1 ~ 1.0.0.26 were vulnerable.

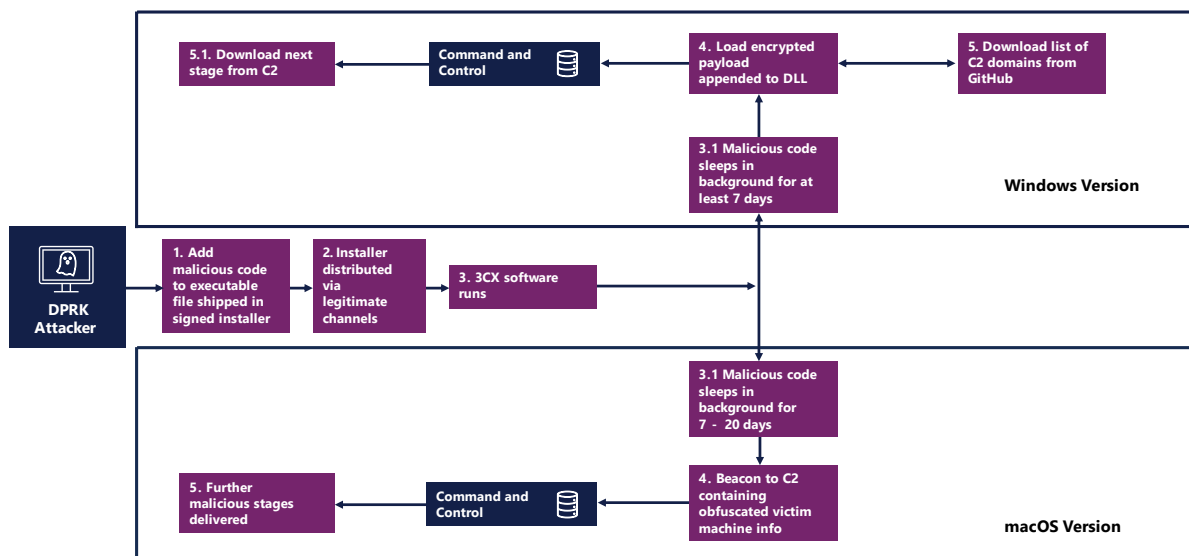
Organisations should make sure they control access to the administrator page of the network-linked system, and identify any unauthorised services or communications.

Further detailed information about how to check the vulnerable version can be found on the [ROK NCSC website](#).

The compromise of 3CX

In March 2023, it was widely reported by both [SentinelOne](#) and [Sophos](#) that the Desktop App software distributed by 3CX had been compromised and contained malware affecting both macOS and Windows operating systems. This constituted a significant global supply chain attack. The security incident was later confirmed by [3CX](#).

Figure 2.



In June 2023 the UK NCSC published a [malware analysis report](#) on the macOS malware used in the 3CX supply chain attack, named Smooth Operator

Attack Flow Windows version

1. The cyber actors added malicious code to an executable file that shipped within a signed installer for 3CX software.
2. The application was distributed to customers via legitimate channels. It is now known that the cyber actors had compromised the 3CX network and therefore were in a position to compromise the build process of the 3CX software.
3. When the 3CX software was run, the malicious code would sleep in the background for at least 7 days and the 3CX software would continue to run as normal.
4. After the sleep period, the malicious code loaded an encrypted payload which is

appended to a DLL also packaged within the 3CX software.

5. This payload is responsible for downloading a list of actor-controlled C2 domains from a GitHub repository, then reaching out to one of them to download the next stage.

The only observed onward stage was a browser stealer, which would extract and exfiltrate basic victim system data, victim 3CX account information and browser history from the Brave, Chrome, Edge and Firefox browsers.

Further detailed information on the Windows attack can be found in the industry from [ESET](#) and [Sophos](#).

Attack Flow macOS version

1. The cyber actors added malicious code to an executable file that shipped within the signed and notarised 3CX application.
2. The application was distributed to customers via legitimate channels. It is now known that the cyber actors had compromised the 3CX network and were therefore in a position to compromise the build process of the 3CX software.
3. When the 3CX software was run, the malicious code slept in the background for between 7 and 20 days, while the 3CX software continued to run as normal.
4. After the sleep period, the malicious code beamed to an actor-controlled C2 server using a customised obfuscation method. The beacon contained basic victim machine information.

5. The C2 server can deliver further malicious stages to be run by the victim machine, but the only observed additional stage collects 3CX account information from a configuration file on the victim machine and exfiltrates this to an actor-controlled C2 server.

Further detail about the macOS attack can be found in the [NCSC malware analysis report](#)

Summary and Preventative Measures

In April 2023 the NCSC published advice on its website regarding the [3CX Desktop App security issue](#).

The negative impact was limited because the malicious update was quickly detected by endpoint detection and response solutions.

This advisory encourages organisations to follow the advice published by the vendor to uninstall the software if you are running an affected version.

Mitigation

As supply chain attacks can happen at any scale and any point, a wide range of measures should be established. The NIS and the NCSC recommend implementing the mitigations below, relating to the supply chain life cycle, as well as management and technical security measures, to deter supply chain threats.

Management Security Measures

- Raise your organisation's awareness of supply chain cyber security, and promote understanding of the issue.
- Provide training on cyber security on a regular basis to help members of your organisation spot malicious tactics and attacks, and report them.
- Identify threats to your organisation's supply chain. Determine threat priorities, and assess impacts when malicious cyber activity occurs, in order to eliminate the blind spot.
- Check the access point to critical data and identify members and supply entities who have the authority to access to minimise access privileges.

Technical Security Measures

- Make sure you install security updates to maintain the most recent version of software, operating systems and anti-virus, to mitigate threats from known vulnerabilities.
- Adopt two-factor authentication for the administration and operation login policies, to prevent unauthorised logins from unauthorised users. The UK NCSC articles [Multi-factor authentication for online services](#) and [Device Security Guidance](#) provide relevant advice.
- Monitor network infrastructure so that traffic from supply chain software applications is trusted but any anomalous traffic can be detected.
- Refer to the following articles in order to mitigate security threats posed to the

supply chain.

1. [Understand of Supply Chain Attack](#) by the ROK NCSC
2. [Assess Supply Chain Cyber Security](#) by the UK NCSC
3. [Principles of Supply Chain Security](#) by the UK NCSC
4. [Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption](#) by the US CISA and NSA
5. [Cyber Supply Chain Risk Management \(C-SCRM\)](#) by the US NIST
6. [The Minimum Elements for a Software Bill of Materials \(SBOM\)](#) by the US NTIA

Reporting Incidents

If you suspect your organisation has been compromised:

Organisations in the ROK should contact the National Intelligence Service (NIS) (<https://www.nis.go.kr>; Contact number 111)

Organisations in the UK should contact the National Cyber Security Centre (NCSC) via
- Report a Cyber Incident (<https://report.ncsc.gov.uk>)

 **Indicators of Compromise (IoC)**

Attacks on various supply chain products, using zero-day vulnerabilities

Section	IoC	Note
C2	[C2 URL]/search/sch-result3.asp	HTTPS communicaiton
Decryption key	0x0c2a351837454a2661026f162530361a394e1d143334	ChaCha20 Key1
	0x0102350423062f085c000e02	ChaCha20 Key2
MD5 hashes	316c088874a5dfb8b8c1c4b259329257	Downloader (SamsungDeviceControl.exe)
	33ca34605e8077047e30e764f5182df0	Downloader (SamsungDevicePanel.exe)
Rogue certificate	Samsung SDS Co., Ltd.	Entity
	0139981ad983bf73e9514d2d4237929e	Serial no.
	2022.12.13 ~ 2023.07.20	Start date to expiration date

The compromise of 3CX, macOS version

Section	IoC	Note
C2	https://msstorageazure[.]com/analysis	
	https://officestoragebox[.]com/api/biosync	
	https://visualstudiofactory[.]com/groupcore	
	https://azuredeploystore[.]com/cloud/images	
	https://msstorageboxes[.]com/xbox	
	https://officeaddons[.]com/quality	
	https://sourcelabs[.]com/status	
	https://zacharryblogs[.]com/xmlquery	
	https://pbxcloudeservices[.]com/network	

	https://pbxphonenetwork[.]com/phone	
	https://akamaitechcloudservices[.]com/v2/fileapi	
	https://azureonlinestorage[.]com/google/storage	
	https://msedgepackageinfo[.]com/ms-webview	
	https://glcloudservice[.]com/v1/status	
	https://pbxsources[.]com/queue	
	https://sbmsa[.]wiki/blog/_insert	Exfiltration URL
	msstorageazure[.]com	
	officestoragebox[.]com	
	visualstudiofactory[.]com	
	azuredeploystore[.]com	
	msstorageboxes[.]com	
	officeaddons[.]com	
	sourceslabs[.]com	
	zacharryblogs[.]com	
	pbxcloudeservices[.]com	
	pbxphonenetwork[.]com	
	akamaitechcloudservices[.]com	
	azureonlinestorage[.]com	
	msedgepackageinfo[.]com	
	glcloudservice[.]com	
	pbxsources[.]com	
	sbmsa[.]wiki	Exfiltration domain
Malicious Code (MD5)	d5101c3b86d973a848ab7ed79cd11e5a	3CX DMG
	660ea9b8205fbd2da59fef26ae5115c	3CX dylib, libffmpeg.dylib
	5faf36ca90f6406a78124f538a03387a	Smooth Operator second-stage payload, UpdateAgent

Malicious Code (SHA1)	3dc840d32ce86ceb6f657b17cef62814646ba8e98	3CX DMG
	769383fc65d1386dd141c960c9970114547da0c2	3CX dylib, libffmpeg.dylib
	9e9a5f8d86356796162cee881c843cde9eaedfb3	Smooth Operator second-stage payload, UpdateAgent
Malicious Code (SHA-256)	e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	3CX DMG
	a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67	3CX dylib, libffmpeg.dylib
	6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59	Smooth Operator second-stage payload, UpdateAgent
Etc.	.main_storage	Victim ID and sleep time file
	UpdateAgent	Second-stage payload