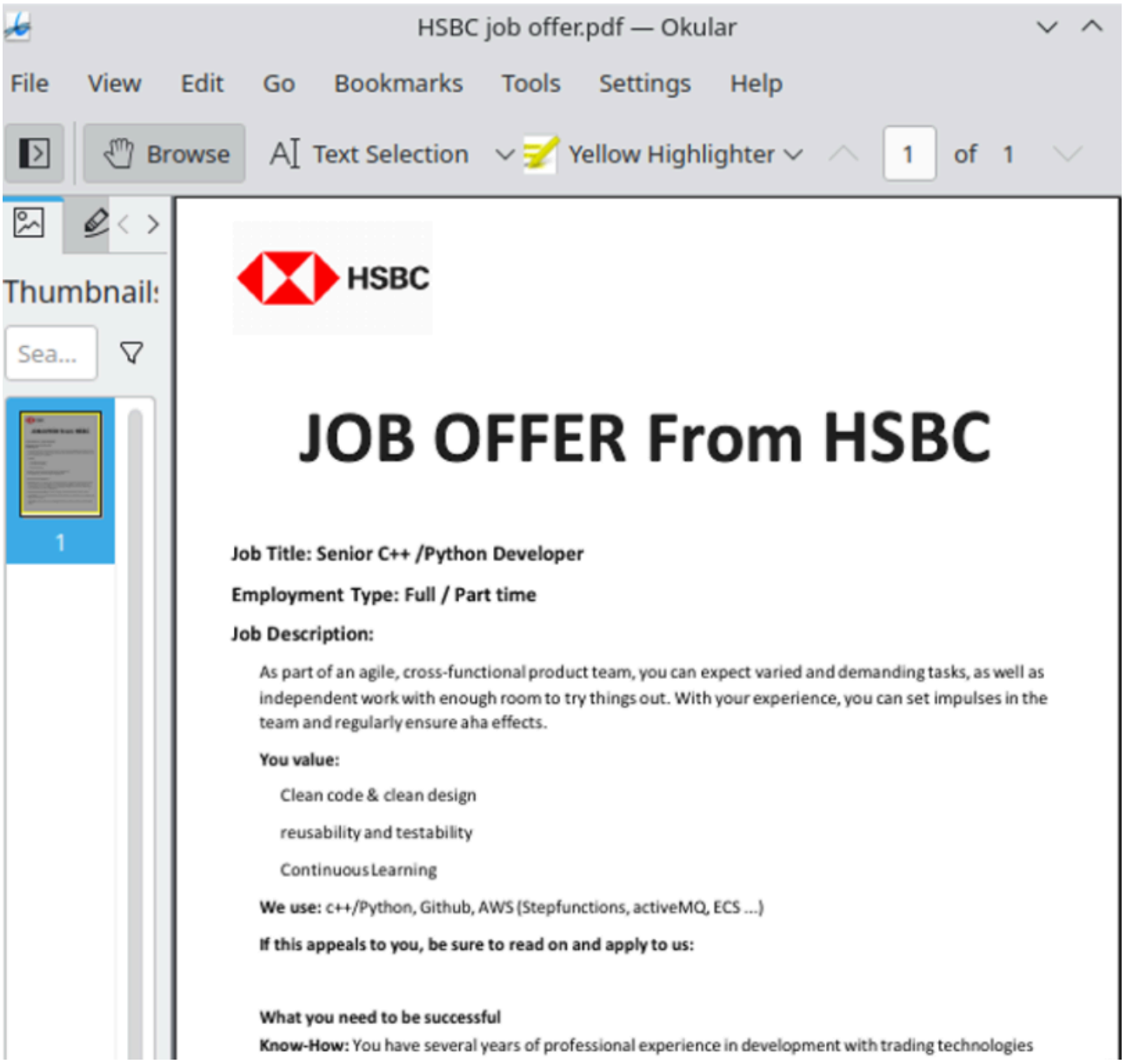
3CX Breach Was a Double Supply Chain Compromise

Published: 2023-04-21 · Archived: 2026-04-02 11:48:22 UTC

We learned some remarkable new details this week about the recent supply-chain attack on VoIP software provider **3CX.** The lengthy, complex intrusion has all the makings of a cyberpunk spy novel: North Korean hackers using legions of fake executive accounts on **LinkedIn** to lure people into opening malware disguised as a job offer; malware targeting **Mac** and **Linux** users working at defense and cryptocurrency firms; and software supply-chain attacks nested within earlier supply chain attacks.



Researchers at ESET say this job offer from a phony HSBC recruiter on LinkedIn was North Korean malware masquerading as a PDF file.

In late March 2023, 3CX disclosed that its desktop applications for both **Windows** and **macOS** were compromised with malicious code that gave attackers the ability to download and run code on all machines where the app was installed. 3CX says it has more than 600,000 customers and 12 million users in a broad range of industries, including aerospace, healthcare and hospitality.

3CX hired incident response firm **Mandiant**, which released a report on Wednesday that said the compromise began in 2022 when a 3CX employee installed a malware-laced software package distributed via an earlier software supply chain compromise that began with a tampered installer for **X_TRADER**, a software package provided by **Trading Technologies**.

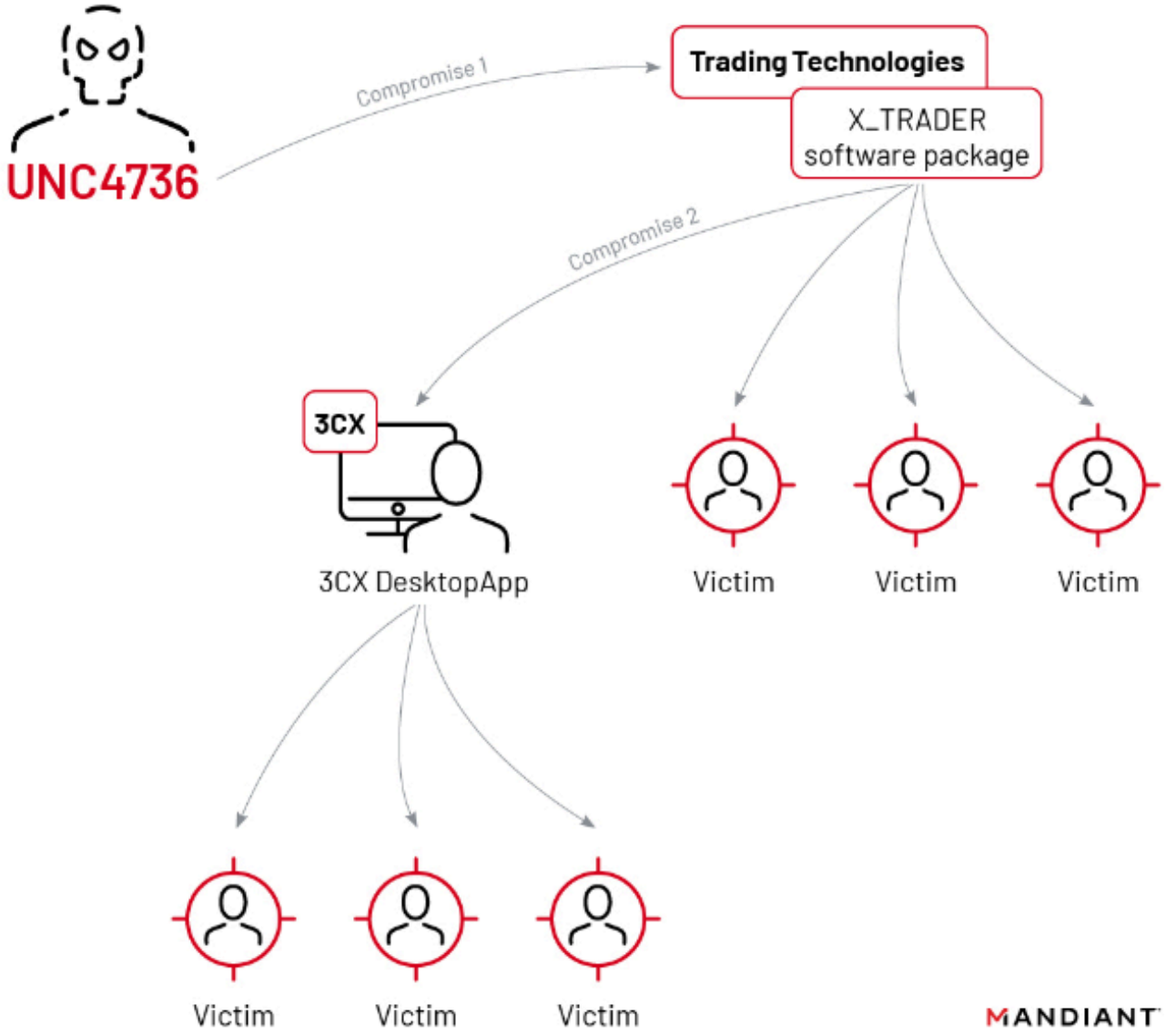
“This is the first time Mandiant has seen a software supply chain attack lead to another software supply chain attack,” reads the April 20 Mandiant report.

Mandiant found the earliest evidence of compromise uncovered within 3CX’s network was through the VPN using the employee’s corporate credentials, two days after the employee’s personal computer was compromised.

“Eventually, the threat actor was able to compromise both the Windows and macOS build environments,” 3CX said in an April 20 update on their blog.

Mandiant concluded that the 3CX attack was orchestrated by the North Korean state-sponsored hacking group known as Lazarus, a determination that was independently reached earlier by researchers at Kaspersky Lab and Elastic Security.

Mandiant found the compromised 3CX software would download malware that sought out new instructions by consulting encrypted icon files hosted on **GitHub**. The decrypted icon files revealed the location of the malware’s control server, which was then queried for a third stage of the malware compromise — a password stealing program dubbed ICONICSTEALER.



The double supply chain compromise that led to malware being pushed out to some 3CX customers. Image: Mandiant.

Meanwhile, the security firm **ESET** today published research showing remarkable similarities between the malware used in the 3CX supply chain attack and Linux-based malware that was recently deployed via fake job offers from phony executive profiles on LinkedIn. The researchers said this was the first time Lazarus had been spotted deploying malware aimed at Linux users.

As reported in a series last summer here, LinkedIn has been inundated this past year by fake executive profiles for people supposedly employed at a range of technology, defense, energy and financial companies. In many cases, the phony profiles spoofed chief information security officers at major corporations, and some attracted quite a few connections before their accounts were terminated.

Mandiant, Proofpoint and other experts say Lazarus has long used these bogus LinkedIn profiles to lure targets into opening a malware-laced document that is often disguised as a job offer. This ongoing North Korean espionage campaign using LinkedIn was first documented in August 2020 by **ClearSky Security**, which said the Lazarus group operates dozens of researchers and intelligence personnel to maintain the campaign globally.

Microsoft Corp., which owns LinkedIn, said in September 2022 that it had detected a wide range of social engineering campaigns using a proliferation of phony LinkedIn accounts. Microsoft said the accounts were used to impersonate recruiters at technology, defense and media companies, and to entice people into opening a malicious file. Microsoft found the attackers often disguised their malware as legitimate open-source software like **Sumatra PDF** and the SSH client **Putty**.

Microsoft attributed those attacks to North Korea's Lazarus hacking group, although they've traditionally referred to this group as "**ZINC**". That is, until earlier this month, when Redmond completely revamped the way it names threat groups; Microsoft now references ZINC as "**Diamond Sleet**."

The ESET researchers said they found a new fake job lure tied to an ongoing Lazarus campaign on LinkedIn designed to compromise **Linux** operating systems. The malware was found inside of a document that offered an employment contract at the multinational bank HSBC.

"A few weeks ago, a native Linux payload was found on VirusTotal with an HSBC-themed PDF lure," wrote ESET researchers **Peter Kalnai** and **Marc-Etienne M.Leveille**. "This completes Lazarus's ability to target all major desktop operating systems. In this case, we were able to reconstruct the full chain, from the ZIP file that delivers a fake HSBC job offer as a decoy, up until the final payload."

ESET said the malicious PDF file used in the scheme appeared to have a file extension of ".pdf," but that this was a ruse. ESET discovered that the dot in the filename wasn't a normal period but instead a Unicode character (U+2024) representing a "leader dot," which is often used in tables of contents to connect section headings with the page numbers on which those sections begin.

"The use of the leader dot in the filename was probably an attempt to trick the file manager into treating the file as an executable instead of a PDF," the researchers continued. "This could cause the file to run when double-clicked instead of opening it with a PDF viewer."

ESET said anyone who opened the file would see a decoy PDF with a job offer from HSBC, but in the background the executable file would download additional malware payloads. The ESET team also found the malware was able to manipulate the program icon displayed by the malicious PDF, possibly because fiddling with the file extension could cause the user's system to display a blank icon for the malware lure.

Kim Zetter, a veteran Wired.com reporter and now independent security journalist, interviewed Mandiant researchers who said they expect "many more victims" will be discovered among the customers of Trading Technologies and 3CX now that news of the compromised software programs is public.

"Mandiant informed Trading Technologies on April 11 that its X_Trader software had been compromised, but the software maker says it has not had time to investigate and verify Mandiant's assertions," Zetter wrote in her Zero Day newsletter on Substack. For now, it remains unclear whether the compromised X_Trader software was downloaded by people at other software firms.

If there's a silver lining here, the X_Trader software had been decommissioned in April 2020 — two years before the hackers allegedly embedded malware in it.

“The company hadn’t released new versions of the software since that time and had stopped providing support for the product, making it a less-than-ideal vector for the North Korean hackers to infect customers,” Zetter wrote.
