TLP:CLEAR

FBI FLASH

ACTIONABLE CYBER INTELLIGENCE

12 NOVEMBER 2026

FLASH Number
AC-111226-MS

North Korean Hackers Use Secretly Recorded Webcam Library of 900+ Tech Workers in $400M "FaceStealer" Crypto Theft Scheme

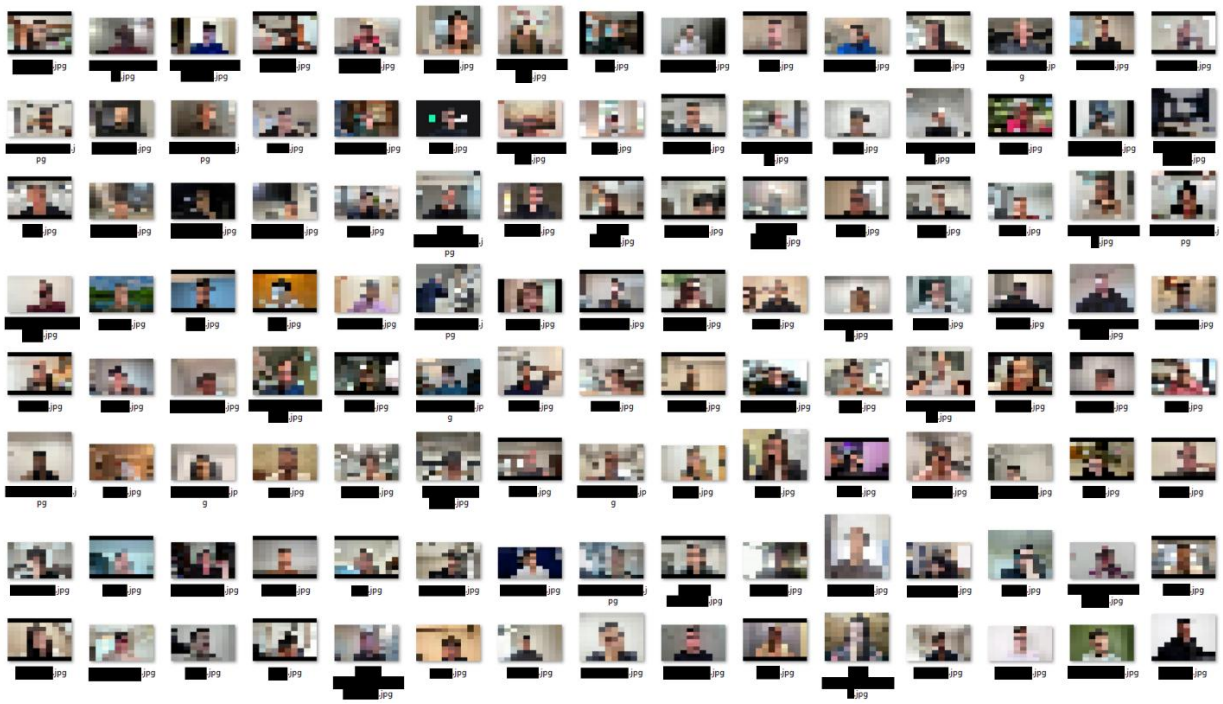


Figure 1 - FBI redacted and blurred examples of the 900 victim videos secretly recorded by North Korean hackers.

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to alert the cryptocurrency/web3 industry and open-source software maintainers of a highly effective North Korean social engineering scheme that the FBI calls "FaceStealer." The FBI attributes this activity to North Korean state-sponsored hackers, known publicly by the names Sapphire Sleet, UNC1069, Dangerous Password, CryptoCore, APT38, BlueNoroff and Stardust Chollima. Using the FaceStealer scheme, the actors have stolen more than $400 million in cryptocurrency over the past 18 months and attempted to compromise the open-source software supply chain. FaceStealer relies on imposter versions of popular video meetings like Zoom, Microsoft Teams and Google Meets controlled by the hackers. Targets are lured to the fake video meetings through invitations from genuine communication and social media accounts that were hijacked from prior victims. The actors have hijacked accounts on platforms including Telegram, LinkedIn, Slack, and Discord. Once a target joins a fake meeting, hackers play prerecorded webcam videos of previous victims to simulate a legitimate video call with participants the target knows. The hackers also record the victim's webcam video. The hackers then introduce a mock technical error into the meeting and, while impersonating the victim's trusted contact, provide instructions to fix the problem. The "fix" installs

malware on the target's computer, turning the target into the next victim. With the victim's computer compromised, the North Korean hackers can steal accessible cryptocurrency or exploit the victim's access to external infrastructure, such as an employer's network or an open-source software maintainer's account. In several reported cases, the hackers stole cryptocurrency and hijacked communication accounts, months to over a year after the initial compromise as the hackers waited for the balances of cryptocurrency wallets to increase. The hackers also access the new victim's contact lists, social media and communications apps, and webcam video to target the victim's personal and professional contacts.

The FBI has identified and seized over 900 victim webcam videos the hackers have used to convincingly impersonate victims in follow-on attacks. The FBI recommends people working in the cryptocurrency/ web3 industry and open-source software maintainers become familiar with the details of the scheme and follow the recommendations provided in this FLASH.

Technical Details



Stage 1: The Compromise of Victim A

The scheme begins with an already compromised victim. In a successful compromise, the North Korean hackers have: 1) scanned the victim's device for accessible cryptocurrency wallets, seed phrases, and other valuable access; 2) taken over and locked the victim out of their Telegram account or other Encrypted Communication Application (ECA); 3) gained access to the victim's contact lists and chat histories; and 4) secretly recorded the victim as they waited for the start of a video chat.

Stage 2: Exploitation of Victim A's Telegram Account or other ECA

Using Victim A's compromised ECA, the North Korean hackers impersonate Victim A and send messages to the victim's contacts proposing a Zoom or Teams meeting. The pretext of the invite is typically to "catch up," "discuss collaboration," or "talk about investment opportunities." Because the hackers have access to Victim A's chat histories, they can also craft custom messages for high-value contacts that are tailored to past communications. The FBI is aware that the North Korean hackers have also created new and hijacked established Telegram, LinkedIn, Slack, and Discord accounts to make initial contact with targets.

Stage 3: Use of Legitimate Services and Creation of Imposter Video Chat Sessions

When targeted contacts respond positively to the video chat invite, the North Korean hackers send Calendly or other calendaring service invites to facilitate scheduling a time and date for the video chat meeting. Shortly before the scheduled meeting time and date arrives, the North Korean hacker uses Victim A's ECA to send the target a link that looks like a legitimate Zoom or Teams meeting link. The link is not legitimate but rather one of many typo-squatted[1] domain addresses the North Korean hackers registered previously to impersonate Zoom and Teams links. Examples of North Korean controlled typo-squatted domains are:

- uu01webzoom.us
- teams.livemeet.us

When the target clicks the imposter link, they are directed to a North Korean-controlled server hosting a copycat version of Zoom or Teams designed by the hackers to be indistinguishable from the genuine interfaces.

Stage 4: Exploiting Victim A's Secretly Recorded Video Image

By the time the new target joins the North Korean-controlled fake Zoom or Teams session, they have received at least two communications from Victim A's legitimate ECA account. The target has also received a link that appears to be for a legitimate Zoom or Teams meeting and is seemingly in the lobby of a Zoom or Teams session waiting to be admitted. Once the target is admitted, the North Korean hacker plays Victim A's stored web camera video and frequently plays additional videos to make it seem as if there are multiple participants, convincingly portraying that Victim A and other participants have joined the meeting.

Stage 5: Social Engineering the Target to Self-Infect

By presenting Victim A's video image, the North Korean hacker primes the target for easy social engineering. After a small delay, the North Korean hacker, acting as Victim A, sends a direct message to the target via the fake Zoom/Teams session. In the message, the hacker claims there is an audio problem or other technical issue, and the target cannot be heard by everyone in the session. The hackers often include multiple fake participants in the Zoom/Teams sessions to add pressure on the target to "correct" a problem only they are seeming to have. The hacker, again acting as Victim A, then guides the target to click an "update" prompt or link, run a script, or copy and paste code into the target's command line or terminal. Unbeknownst to the target, following those instructions downloads malware that will eventually install a browser cookie harvester, keyloggers, screen capturers, and a backdoor onto the infected

[1] Typo-squatting , also called URL hijacking or domain mimicry, occurs when a bad actor registers deliberately misspelled, altered, or hyphenated website domain names to catch internet users who make typing mistakes.

device. The hacker also started recording the target's web camera video when they first clicked the imposter Zoom or Teams link. The target has now become the next victim.

Stage 6: Repeat the Cycle and Return to Stage 1: With the new victim's video and control of their device, the hackers can steal their cryptocurrency or exploit the victim's access. The hackers can also target the new victim's contacts, continuing the cycle of compromise. With each victim and compromised contact list, the pool of targets and victims grows exponentially.

Additional Warnings

Emerging Use of SI to Generate Deepfake Videos

The North Korean hackers behind the FaceStealer campaign have begun to use super intelligence (SI) to make their scheme even more efficient and effective. One of the more concerning ways they use SI is to generate deepfake videos. Their deepfake production tends to focus on well-known and influential individuals in the cryptocurrency and web3 industries. The hackers take publicly available photos or videos of these individuals and convert the images into realistic deepfakes. The deepfakes can then be used by the hackers to make it appear as if the notable individual is a participant in the hackers' imposter Zoom/Teams chats. The deepfake of a notable person can be used instead of victim video or be used along with real victim video to present a multi-person video chat. The quality of the deepfakes only needs to be good enough to pass as webcam video. The deepfakes provide the hackers with additional targeting flexibility, but the FaceStealer scheme currently continues to overwhelmingly rely on the theft of genuine victim videos. The best practices included at the end of this FLASH should assist potential targets regardless of whether North Korean hackers try to use victim video or SI deepfakes to go after you.

Targeting Open-Source Software Developers and Maintainers to Infect the Supply Chain

North Korean hackers have primarily used the FaceStealer scheme to target individuals and companies from which the hackers can steal cryptocurrency. The hackers have also targeted supply-chain software developers and maintainers with the same technique. In targeting software developers and maintainers, the hackers are trying to gain access to their devices and the software repository accounts they control. If the hackers can infect the distribution of the software, they can compromise the supply chain and turn a single victim (the developer or maintainer) into potentially millions of victims. Earlier this year, North Korean hackers used the FaceStealer scheme to nearly achieve that goal.

The hackers used multiple interactions to lure a significant open-source JavaScript library into a fake Teams video chat. The hackers made it appear that there were multiple participants in the Teams session, including at least one individual the maintainer recognized. The maintainer was then messaged that something was wrong on his system and he followed the recommended "corrective" measures, unwittingly infecting his computer with the hackers' malware. The hackers then proceeded to use the maintainer's access to the JavaScript library to create malicious dependencies that would be downloaded along with legitimate library downloads. The library receives tens of millions of downloads per week. If not for the quick detection and response to the compromise, the failed attack could easily have resulted in very large-scale victimization. The FBI is aware of several other attempts by North Korean hackers to target software developers, maintainers, and software libraries with significant download volume. Multiple attempts have been directed at maintainers with repositories on the JavaScript registry, Node Packet Manager (NPM), and recently against maintainers of Rust crates.

Recommendations

- When joining a video chat, use the official video chat application (i.e. Zoom or Teams) and use an invite code instead of clicking on links to join web versions of the applications. This best practice should be followed particularly when responding to invitations from infrequent or new contacts. This will help to protect against being lured into an imposter video chat session.

- When joining a video chat that you have been invited to attend, do not turn on your webcam until you are able to see, hear, and communicate with the person who invited you. This best practice should be followed particularly when responding to invitations from infrequent or new contacts. By delaying the start of your web camera, you give yourself the opportunity to visually inspect and communicate with the person who invited you before offering up your webcam feed.

- If prompted for an update while using a video chat service, do not run scripts or copy code into the command line or terminal to update the client. Instead, separately update the communication application or join the meeting through web versions of the service with the invite code.

- Inspect Calendly or other calendaring invites for meeting links. North Korean hackers frequently do not include video chat links in their scheduling emails, instead sending malicious video chat links closer to the appointed meeting date and time. They do this to minimize exposure of their malicious infrastructure.

- When possible, confirm a scheduled video chat meeting with the person who invited you through an alternate communication method from how you were contacted. For example, if you receive a Telegram message, confirm the meeting by text or phone if you have that information.

- Secure Telegram, WhatsApp, Slack, and other apps used for communication by adding multifactor authentication, turning on login alerts, and using expiring messages. This will help to protect your communication applications from being hijacked and limit accessible chat histories if they are hijacked. The hackers will hijack the accounts by logging onto the account from a different device, changing the recovery account such as the recovery phone number, then closing your sessions.

- Enhance the security of your cryptocurrency by keeping only low-dollar amounts on browser extension wallets. Keep larger cryptocurrency balances on a separate physical ledger (not connected to the device) or deposited with an exchange. Do not keep any secret recovery phrases or private keys anywhere on your devices. North Korean hackers have been known to copy recovery phrases, patiently monitor balances on the blockchain, and reconstitute the wallet (stealing your cryptocurrency) following a large transfer.

What You Should Do If You Suspect You Have Been Compromised

- Immediately secure your cryptocurrency assets by creating a new cryptocurrency wallet (with new seed phrases) on a device that was not used to communicate with the suspected hackers and

transfer the cryptocurrency assets to the new wallet. As noted above, North Korean hackers have stolen cryptocurrency months and years after compromises by copying seed phrases, monitoring addresses/wallet balances, and reconstituting the address/wallet when the balance increases.

- Secure your Telegram, WhatsApp, other ECAs, and sensitive accounts, including developer accounts, by changing passwords, logging off all active sessions, and adding multifactor authentication.

- Inform your friends and contacts that malicious cyber actors have hijacked your accounts and may be trying to impersonate you with prerecorded Zoom/Teams webcam video. If you communicated with the hackers on a work device, or have work files on your personal device, let employers know that you were hacked and that work documents may have been compromised. Failure to notify your contacts and employers puts them at risk of compromise and insulates the scheme.

- Change all passwords.

- If you lose access to your ECA/developer accounts, reach out to the platform to request the account gets shut down or restored to you.

- File a report at IC3.gov with the keyword “FaceStealer.”

Acknowledgements

Cyber security and incident response companies, Arctic Wolf, Jumpsec, and Microsoft Threat Intelligence Center (MSTIC) recently published reports that provide valuable additional technical information gathered from the companies’ investigations and responses to victim compromises. Their reports include robust lists of indicators of compromise (IOCs).

- https://arcticwolf.com/resources/blog/still-in-the-meeting-bluenoroff-six-months-on/

- https://www.jumpsec.com/guides/inside-a-dprk-bluenoroff-clickfix-kit/

- https://www.microsoft.com/en-us/security/blog/2026/04/16/dissecting-sapphire-sleets-macos-intrusion-from-lure-to-compromise

The FBI acknowledges Arctic Wolf for their contributions to this advisory regarding North Korea SI usage and deepfake production.

Reporting Notice

If you identify suspicious activity within your enterprise or have information related to the contents of this document, please contact your local FBI Cyber Squad immediately at **www.fbi.gov/contact-us/field-**

offices. The FBI also encourages you to report suspicious or criminal activity to the FBI Internet Crime Complaint Center at www.ic3.gov with the keyword "**FaceStealer**." When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated in light of your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistent with applicable state and federal law.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI.

This FLASH is marked TLP:CLEAR. The information in this product may be shared without restriction. Information is subject to standard copyright rules.

