DeceptiveDevelopment: From primitive crypto theft to sophisticated AI-based deception

ESET Research

Malware operators collaborate with covert North Korean IT workers, posing a threat to both headhunters and job seekers

Peter Kálnai

Matěj Havránek

25 Sep 2025 • , 18 min. read

This blogpost introduces our latest white paper, presented at Virus Bulletin 2025, where we detail the operations of the North Korea-aligned threat actor we call DeceptiveDevelopment and its connections to North Korean IT worker campaigns. The white paper provides full technical details, including malware analysis, infrastructure, and OSINT findings. Here, we summarize the key insights and highlight the broader implications of this hybrid threat.

Key points of this blogpost:

- The invention and focus of the operations are on the social-engineering methods.
- DeceptiveDevelopment's toolset is mostly multiplatform and consists of initial obfuscated malicious scripts in Python and JavaScript, basic backdoors in Python and Go, and a dark web project in .NET.
- We provide insights into operational details of North Korean IT workers, like work assignments, schedules, communication with clients, etc., gathered from public sources.
- Native, more complex Windows backdoors are an occasional addition in the execution chain and are likely shared by other North Korea-aligned actors.
- DeceptiveDevelopment and North Korean IT workers have different objectives and means, but we consider them as tightly connected.

Introduction

In this blogpost, we examine the DeceptiveDevelopment group and the WageMole activity cluster as two tightly connected North Korea-aligned entities. WageMole is a label that we have adopted for activities associated with North Korean IT workers. While the campaigns of both are driven by financial gain, each plays a distinct and complementary role in relation to the other:

- DeceptiveDevelopment operators pose as recruiters, using fraudulent job offers to compromise the systems of job seekers.
- North Korean IT workers then use the information gained by the DeceptiveDevelopment operators to pose as job seekers. To secure a real job position, they may employ several tactics, including proxy interviewing, using stolen identities, and fabricating synthetic identities with AI-driven tools.

First, we provide a catalogue of multiplatform tools used by DeceptiveDevelopment, from simple but obfuscated scripts like BeaverTail and InvisibleFerret to a complex toolkit, TsunamiKit, centered around a .NET backdoor. We also disclose specific links between more complex backdoors used by DeceptiveDevelopment, AkdoorTea and Tropidoor, and other, more APT-oriented North Korea-aligned operations. Next, we describe interesting aspects of North Korean IT workers' modus operandi, obtained from public sources, mostly from unintentionally exposed data, testimonials of victims, and investigations of independent researchers..

DeceptiveDevelopment

DeceptiveDevelopment is a North Korea-aligned group active since at least 2023, focused on financial gain. Its activities overlap with Contagious Interview, DEV#POPPER, and Void Dokkaebi. The group targets software developers on all major systems – Windows, Linux, and macOS – and especially those in cryptocurrency and Web3 projects. Initial access is achieved exclusively via various social engineering techniques like ClickFix, and fake recruiter profiles similar to Lazarus's Operation DreamJob, to deliver trojanized codebases during staged job interviews. Its most typical payloads are the BeaverTail, OtterCookie, and WeaselStore infostealers, and the InvisibleFerret modular RAT.

Targeting strategy

DeceptiveDevelopment operators use various methods to compromise their victims, relying on clever social engineering tricks. Via both fake and hijacked profiles, they pose as recruiters on platforms like LinkedIn, Upwork, Freelancer, and Crypto Jobs List. They offer fake lucrative job opportunities to attract their targets' interest. Victims are requested to participate in a coding challenge or a pre-interview task. The task involves downloading a project from private GitHub, GitLab, or Bitbucket repositories. These repositories contain trojanized code, often hidden cleverly in long comments displayed well beyond the right-hand edge of a code browser or editor window. Participation in the task triggers the execution of BeaverTail, the first-stage malware.

Besides these fake recruiter accounts, the addition of a new social engineering technique known as ClickFix was observed. ClickFix in relation to DeceptiveDevelopment was first reported by Sekoia.io in March 2025, when it was used by the group as the initial access method on macOS and Windows systems; in September 2025, GitLab spotted it being used on Linux systems too. The attackers direct the victim to a fake job interview website, containing an application form that they are asked to complete. The application form contains a few lengthy questions related to the applicant's identity and qualifications, leading the victim to put significant time and effort into filling in the form and making them feel like they are almost done, and therefore more likely to fall for the trap. In the final step of the application, the victim is asked to record a video of them answering the final question. The site triggers a pop-up asking the victim to allow camera access, but the camera is never actually accessed. Instead, an error message appears saying that access to the camera or microphone is currently blocked and offers a "How to fix" link. That link leads to a pop-up employing the ClickFix social engineering technique. The victim is instructed, based on their operating system, to open a terminal and copy and paste a command that should solve the issue. However, instead of enabling the victim's camera, the command downloads and executes malware.

Toolset

BeaverTail and InvisibleFerret

The first indication of DeceptiveDevelopment activity came in November 2023, when Unit 42 reported the Contagious Interview campaign; we later associated this campaign with the group. Unit 42 coined the names BeaverTail and InvisibleFerret for the two malware families used in this campaign. We documented this campaign in more detail in our WeLiveSecurity blogpost from February 2025, dissecting how the threat actor makes use of these two malware families.

BeaverTail is a simple infostealer and downloader that collects data from cryptocurrency wallets, keychains, and saved browser logins. We have observed variants of this malware written in JavaScript, hidden in fake job challenges, and also in C++, using the Qt framework and disguised as conferencing software. Its primary function is downloading the second-stage malware InvisibleFerret. At the end of 2024, a new malware family with functionality similar to BeaverTail emerged – it was named OtterCookie by NTT Security. OtterCookie is written in JavaScript and uses very similar obfuscation techniques. We believe that OtterCookie is an evolution of BeaverTail and is used by some teams within DeceptiveDevelopment instead of the older BeaverTail, while other teams continue using and modifying the original codebase.

InvisibleFerret is modular malware written in Python with more information-stealing capabilities than BeaverTail, also capable of providing remote control to attackers. It usually comes with the following four modules:

- a browser-data stealer module (extracts and exfiltrates data saved by browsers and cryptocurrency wallets),
- a payload module (remote access trojan),
- a clipboard module (containing keylogging and clipboard logging capabilities) – in some cases distributed as part of the payload module, and
- an AnyDesk module (which deploys the AnyDesk remote access tool to allow direct attacker access to the compromised machine).

WeaselStore

As DeceptiveDevelopment evolved and started to include more teams in its operations, those teams started modifying the codebase to meet their own needs and introduced new malware tooling. One such example is a campaign that ESET researchers investigated in August 2024. In addition to the conventional BeaverTail and InvisibleFerret malware, the team responsible for the campaign deployed what we believe is its own new malware – which we named WeaselStore.

WeaselStore (also called GolangGhost and FlexibleFerret) is a multiplatform infostealer written in Go, though in May 2025, Cisco Talos reported about WeaselStore being rewritten in Python; they called that malware PylangGhost. As the implementation is identical, for simplicity, we refer to both implementations as WeaselStore in this blogpost.

WeaselStore's functionality is quite similar to both BeaverTail and InvisibleFerret, with the main focus being exfiltration of sensitive data from browsers and cryptocurrency wallets. Once the data has been exfiltrated, WeaselStore, unlike traditional infostealers, continues to communicate with its C&C server, serving as a RAT capable of executing various commands.

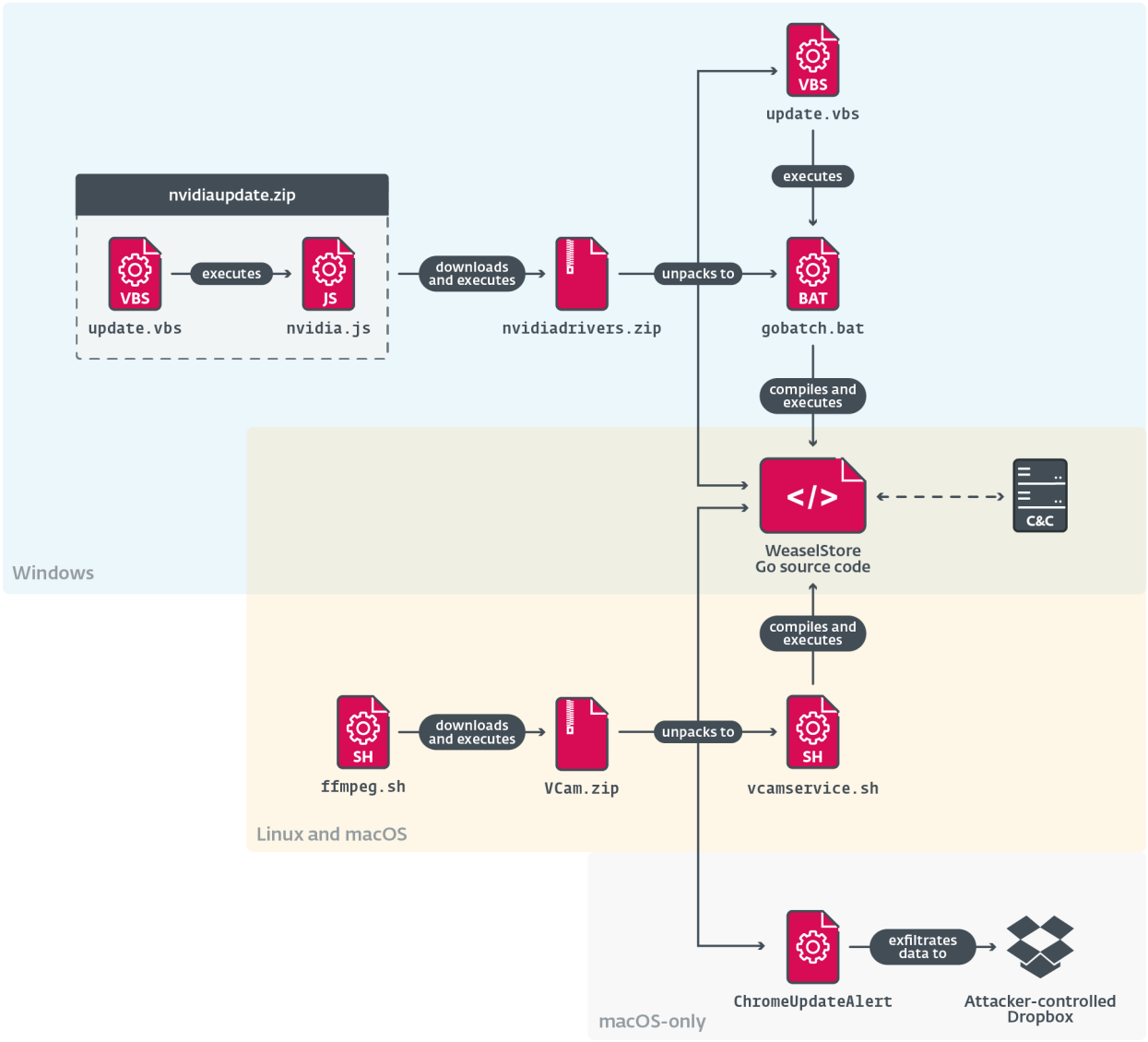

Figure 1. Execution chain of WeaselStore

The most interesting aspect of WeaselStore in Go is that it is delivered to the victim's system in the form of Go source code, along with the Go environment binaries necessary to build and execute it, allowing the malware to target three main operating systems – Windows, Linux, and macOS (see Figure 1). The installation mechanism differs based on the victim's operating system, but in all cases the chain ends with downloading the WeaselStore Go source code and then compiling and executing it using a Go build environment, which is also provided alongside.

TsunamiKit

In November 2024, a new version of the InvisibleFerret malware delivered a modified browser-data stealer module. This module, in addition to its normal functionality, contains a previously unseen, large, encoded block with the first stage of the execution chain deploying a completely new malware toolkit, also intended for information and cryptocurrency theft. We named this toolkit TsunamiKit, based on the developer's repeated use of "Tsunami" in the names of its components (see Table 1). The threat being publicly reported

by Alessio Di Santo in November 2024 and by Bitdefender in February 2025; our white paper adds context by placing it in the overall DeceptiveDevelopment modus operandi. The paper also dives into the details of TsunamiKit's complex execution chain.

Table 1. Components of the TsunamiKit execution chain

Component name	Description
TsunamiLoader	The initial stage, obfuscating and dropping TsunamiInjector. It contains a quote *Sometimes you never know the value of a moment until it becomes a memory*, often attributed to Dr. Seuss.
TsunamiInjector	Downloader of TsunamiInstaller. Also drops TsunamiHardener.
TsunamiHardener*	Referred to as TsunamiPayload in the code. Sets up persistence for TsunamiClient, and Microsoft Defender exclusions for TsunamiClient and the XMRig miner (one of TsunamiClient's components).
TsunamiInstaller	.NET dropper of TsunamiClientInstaller and a Tor proxy.
TsunamiClientInstaller*	Fingerprints the system; downloads and executes TsunamiClient.
TsunamiClient	Complex .NET spyware; drops XMRig and NBMiner.

* These components were originally both named TsunamiPayload; we have renamed them to avoid any confusion.

PostNapTea and Tropidoor

Over the course of our research, we spotted an interesting piece of evidence, further linking DeceptiveDevelopment to North Korea. In April 2025, Ahnlab researchers reported about trojanized Bitbucket projects containing BeaverTail and a 64-bit downloader named car.dll or img_layer_generate.dll. While BeaverTail, as expected, downloaded InvisibleFerret, this new downloader retrieved an in-memory payload that was named Tropidoor by Ahnlab. We realized that Tropidoor shares large portions of code with PostNapTea, a Lazarus RAT distributed via exploitation against South Korean targets in 2022. Table 2 contains a comparison of both payloads.

Table 2. Comparison of Tropidoor (DeceptiveDevelopment) and PostNapTea (Lazarus) payloads (asterisks indicate the country of a VirusTotal submission)

	Tropidoor	PostNapTea
First seen	2024-11-28	2022-02-25
Targeted countries	Kenya*, Colombia*, Canada*	South Korea
Initial Access	Social engineering	Exploitation
Hash-based resolution of Windows APIs	Fowler–Noll–Vo	Fowler–Noll–Vo
String encryption	Plain + XOR-based	XOR-based
Encryption for network communication	Base64 + AES-128	Base64 + AES-128

	Tropidoor	PostNapTea
Project	C DLL	MFC C++ DLL
Type of commands	Internal implementation of Windows commands	Internal implementation of Windows commands
Building environment	Visual Studio 2019, v16.11	Visual Studio 2017, v15.9
Configuration format	Binary	JSON
User-Agent (differences in reversed color)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.64	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36

Tropidoor is the most sophisticated payload yet linked to the DeceptiveDevelopment group, probably because it is based on malware developed by the more technically advanced threat actors under the Lazarus umbrella. Some of the supported commands are shown in Figure 2.

```
__int64 __fastcall Cmd::internal_console_commands(const WCHAR *sCommandLine, std::wstring *Result)
{
  Error = 0;
  Params = CommandLineToArgvW(sCommandLine, &pNumArgs);
  Command = 0;
    switch ( Command )
    {
      case 1u:
        Error = Cmd::schtasks(pNumArgs, Params, Result);
        if ( Error != 1 )
          return Error;
LABEL_11:
        v12 = 17;
        v13 = L"Wrong parameter\r\n";
        break;
      case 2u:
        return Cmd::ping(pNumArgs, Params, Result);
      case 3u:
        return Cmd::reg(pNumArgs, Params, Result);
      case 4u:
        err = Cmd::net(pNumArgs, Params, Result);
      case 9u:
        return Cmd::nslookup(pNumArgs, Params, Result);
      case 0xAu:
        v22 = Cmd::wmic_process(pNumArgs, Params, Result);
```

Figure 2. Some Windows commands implemented internally in the Tropidoor code

New findings

Since our white paper's submission, we have uncovered new findings that further strengthen the link between the activity of DeceptiveDevelopment and other North Korea-aligned cyberattacks.

We discovered that the TsunamiKit project dates back at least to December 2021, when it was submitted to VirusTotal under the name Nitro Labs.zip. One of the components contains the PDB path E:\Programming\The Tsunami Project\Malware\C#\C# Tsunami Dist Version 3.0.0\CTsunami\obj\Release\netcoreapp3.1\win-x64\\System Runtime Monitor.pdb. We conclude that

TsunamiKit is likely a modification of a dark web project rather than a new creation by the attackers, based on TsunamiKit largely predating the approximate start of DeceptiveDevelopment activity in 2023, similar TsunamiKit payloads without any signs of BeaverTail having been observed in ESET telemetry, and cryptocurrency mining being a core feature of TsunamiKit.

AkdoorTea

In August 2025, a BAT file named ClickFix-1.bat and a ZIP archive named nvidiaRelease.zip were uploaded to VirusTotal. The BAT file just downloads the archive and executes run.vbs from it. The archive contains various legitimate JAR packages for the NVIDIA CUDA Toolkit, together with the following malicious files:

- shell.bat, a trojanized installer for Node.js, which is executed afterward.
- main.js, an obfuscated BeaverTail script, automatically loaded by Node.js.
- drvUpdate.exe, a TCP RAT, to which we assign the codename AkdoorTea, as it is similar to Akdoor reported by AlienVault in 2018 (see Table 3). Akdoor is a detection root name by Ahnlab and usually identifies a North Korea-aligned payload.
- run.vbs, a VBScript that executes the trojanized installer and AkdoorTea.

Table 3. Comparison of variants of AkdoorTea and Akdoor

	AkdoorTea 2025	**Akdoor 2018**
Distribution name	drvUpdate.exe	splwow32.exe, MMDx64Fx.exe
Encryption	Base64 + XOR with 0x49	Base64 + RC4
Number of supported commands	5	4
C&C	103.231.75[.]101	176.223.112[.]74 164.132.209[.]191
Version	01.01	01.01

One of the differences between AkdoorTea from 2025 and Akdoor from 2018 is the numbering of commands; see Figure 3. Also, the command name “version” is called “shi” now.

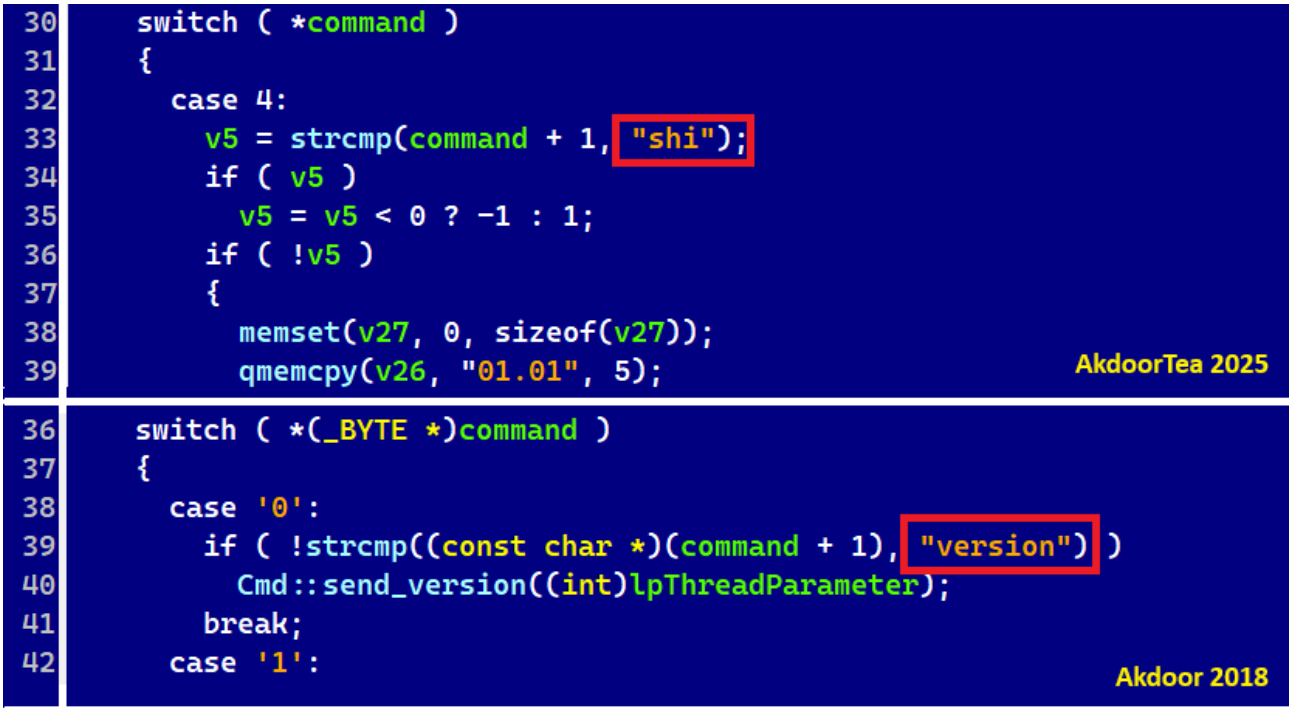

Figure 3. Version parsing in Akdoor from 2018 and AkdoorTea from 2025

North Korean IT workers (aka WageMole)

While our research into DeceptiveDevelopment is primarily based on data from our telemetry and reverse-engineering the group's toolset, it is interesting to point out DeceptiveDevelopment's relations to fraud operations by North Korean IT workers, overlapping with the activity of the UNC5267 and Jasper Sleet threat groups.

IT worker campaigns have been ongoing since at least April 2017, according to an FBI wanted poster, and have been increasingly prominent in recent years. A joint advisory released in May 2022 describes IT worker campaigns as a coordinated effort by North Korea-aligned individuals to gain employment at overseas companies, whose salaries are then used to help fund the country. They have also been known to steal internal company data and use it to extort companies, as stated in an announcement by the FBI in January 2025.

In addition to using AI to perform their job tasks, they rely heavily on AI for manipulating photos in their profile pictures and CVs, and even perform face swaps in real-time video interviews to look like the persona they are currently using, as described in more detail in a blogpost by Unit 42 in April 2025.

A methodological insight was provided by a DTEX report in May 2025. The IT workers reportedly operate in a scattered manner, with numerous teams of workers, usually based in foreign countries like China, Russia, and countries in Southeast Asia. Each team works in a slightly different manner, but their end goals and modus operandi are the same – posing as foreign remote workers with fake documents and CVs, and looking for remote employment or freelance work to gather funds from the salaries.

Analyzing OSINT data

Multiple researchers have observed ties and instances of information exchange between these IT workers and DeceptiveDevelopment. In August 2024, the cybersecurity researcher Heiner García published an investigation of how both groups share email accounts or are mutually followed between the GitHub profiles of fake recruiters and IT workers. In November 2024, Zscaler confirmed that identities stolen from compromised victims are used by scammers to secure remote jobs. This leads us to assert with medium confidence that although these activities are conducted by two different groups, they are most likely connected and collaborating.

Additionally, we managed to gather publicly available data detailing the inner workings of some of the IT worker teams. We gathered this information from multiple sources (with significant help from @browsercookies on X), among them GitHub profiles belonging to the IT workers, containing publicly accessible internal data and content shared publicly by researchers. These include details of their work assignments, schedules, communication with clients and each other, emails, various pictures used for online profiles (both real and fake), fake CVs, and text templates used when job hunting; due to information sharing agreements, we are not disclosing the specific sources of the data used in our analysis. We dive into these details in our white paper, and provide a compact summary below.

Analysis of fake CVs and internal materials shows that IT workers initially targeted jobs in the US, but have recently shifted focus to Europe, including France, Poland, Ukraine, and Albania.

Each team is led by a “boss” who sets quotas and coordinates work. Members spend 10–16 hours daily acquiring jobs, completing tasks, and self-educating – mainly in web programming, blockchain, English, and AI integration.

They meticulously track their work and use fake identities, CVs, and portfolios to apply for jobs. Communication with employers follows scripted responses to appear qualified.

Additionally, they use premade scripts to recruit real people as proxies, offering them a share of the salary to attend interviews or host work devices in less suspicious countries. In one case, Ukrainian developers were targeted due to perceived hiring advantages.

Conclusion

DeceptiveDevelopment’s TTPs illustrate a more distributed, volume-driven model of its operations. Despite often lacking technical sophistication, the group compensates through scale and creative social engineering. Its campaigns demonstrate a pragmatic approach, exploiting open-source tooling, reusing available dark web projects, adapting malware probably rented from other North Korea-aligned groups, and leveraging human vulnerabilities through fake job offers and interview platforms.

The activities of North Korean IT workers constitute a hybrid threat. This fraud-for-hire scheme combines classical criminal operations, such as identity theft and synthetic identity fraud, with digital tools, which classify it as both a traditional crime and a cybercrime (or eCrime). Proxy interviewing poses a severe risk to employers, since an illegitimate employee hired from a sanctioned country may not only be irresponsible or underperforming, but could also evolve into a dangerous insider threat.

Our findings also highlight the blurred lines between targeted APT activity and cybercrime, particularly in the overlap between malware campaigns by DeceptiveDevelopment and the operations of North Korean IT workers. These dual-use tactics – combining cybertheft and cyberespionage with non-cyberspace employment-fraud schemes – underscore the need for defenders to consider broader threat ecosystems rather than isolated campaigns..

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

Files

A comprehensive list of indicators of compromise (IoCs) and samples can be found in our GitHub repository.

SHA-1	Filename	Detection	Description
E34A43ACEF5AF1E5197D940B94FC37BC4EFF0B2A	nvidiadrivers.zip	WinGo/DeceptiveDevelopment.F	A trojanized project containing WeaselStore.
3405469811BAE511E62CB0A4062AADB523CAD263	VCam1.update	WinGo/DeceptiveDevelopment.F	A trojanized project containing WeaselStore.
C0BAA450C5F3B6AACDE2807642222F6D22D5B4BB	VCam2.update	WinGo/DeceptiveDevelopment.F	A trojanized project containing WeaselStore.
DAFB44DA364926BDAFC72D72DBD9DD728067EFBD	nvidia.js	JS/Spy.DeceptiveDevelopment.Q	WeaselStore downloader for Windows.
015583535D2C8AB710D1232AA8A72136485DB4EC	ffmpeg.sh	OSX/DeceptiveDevelopment.B	WeaselStore downloader for OSX/Linux.
CDA0F15C9430B6E0FF1ACDA4D44DA065D547AF1C	DriverMinUpdate	OSX/DeceptiveDevelopment.B	Fake prompt requesting user's login on macOS.
214F0B10E9474F0F5D320158FB71995AF852B216	nvidiaupdate.exe	WinGo/DeceptiveDevelopment.B	Compiled WeaselStore binary for Windows.
4499C80DDA6DBB492F8667D11D3FFBFEEC7A3926	bow	Python/DeceptiveDevelopment.C	InvisibleFerret.
B20BFBAB8BA732D428AFBA7A688E6367232B9430	N/A	Python/DeceptiveDevelopment.C	Browser-data stealer module of InvisibleFerret.
C6888FB1DE8423D9AEF9DDEA6B1C96C939A06CF5	Windows Update Script.pyw	Python/TsunamiKit.A	TsunamiInjector.
4AAF0473599D7E3A503841ED10281FDC186633D2	Runtime Broker .exe	MSIL/DeceptiveDevelopment.A	TsunamiInstaller.
251CF5F4A8E73F8C5F91071BB043B4AA7F29D519	Tsunami Payload .exe	MSIL/DeceptiveDevelopment.A	TsunamiClientInstaller.
D469D1BAA3417080DED74CCB9CFB5324BDB88209	Tsunami Payload .dll	MSIL/DeceptiveDevelopment.A	TsunamiClient.
0C0F8152F3462B662318566CDD2F62D8E350A15E	Runtime Broker .exe	Win64/Riskware.Tor.A	Tor Proxy.

SHA-1	Filename	Detection	Description
F42CC34C1CFAA826B962 91E9AF81F1A67620E631	autopart.zip	Win64/DeceptiveDevelopment.C JS/Spy.DeceptiveDevelopment.A	A trojanized project containing BeaverTail and a downloader of Tropidoor.
02A2CD54948BC0E2F696 DE412266DD59D150D8C5	hoodygang.zip	Win64/DDeceptiveDevelopment.C JS/Spy.DeceptiveDevelopment.A	A trojanized project containing BeaverTail and a downloader of Tropidoor.
6E787E129215AC153F3A 4C05A3B5198586D32C9A	tailwind.config.js	JS/Spy.DeceptiveDevelopment.A	A trojanized JavaScript containing BeaverTail.
FE786EAC26B61743560A 39BFB905E6FB3BB3DA17	tailwind.config.js	JS/Spy.DeceptiveDevelopment.A	A trojanized JavaScript containing BeaverTail.
86784A31A2709932FF10 FDC40818B655C68C7215	img_layer_generate.dll	Win64/DeceptiveDevelopment.C	A downloader of the Tropidoor RAT.
90378EBD8DB757100A83 3EB8D00CCE13F6C68E64	N/A	Win64/DeceptiveDevelopment.D	Tropidoor RAT.
C86EEDF02B73ADCE0816 4F5C871E643E6A32056B	drivfixer.sh	OSX/DeceptiveDevelopment.C	A trojanized macOS installer and launcher of Node.js.
4E4D31C559CA16F8B7D4 9B467AA5D057897AB121	ClickFix-1.bat	PowerShell/DeceptiveDevelopment.B	An initial stage on Windows: BAT downloading a malicious nvidiaRelease.zip archive.
A9C94486161C07AE6935 F62CFCC285CD342CDB35	driv.zip	JS/Spy.DeceptiveDevelopment.A OSX/DeceptiveDevelopment.C	A ZIP archive containing BeaverTail.
F01932343D7F13FF1094 9BC0EA27C6516F901325	nvidiaRelease.zip	JS/Spy.DeceptiveDevelopment.A Win32/DeceptiveDevelopment.A VBS/DeceptiveDevelopment.B BAT/DeceptiveDevelopment.A	A ZIP archive containing BeaverTail and AkdoorTea.
BD63D5B0E4F2C72CCFBF 318AF291F7E578FB0D90	mac-v-j1722.fixer	OSX/DeceptiveDevelopment.D	An initial stage on macOS: a bash script that downloads a malicious driv.zip archive.
10C967386460027E7492 B6138502AB61CA828E37	main.js	JS/Spy.DeceptiveDevelopment.A	An obfuscated BeaverTail script, automatically loaded by Node.js.
59BA52C644370B4D627F 0B84C48BDA73D97F1610	run.vbs	VBS/DeceptiveDevelopment.B	A VBScript that executes AkdoorTea and shell.bat.

SHA-1	Filename	Detection	Description
792AFE735D6D356FD30D2E7D0A693E3906DECCA7	drvUpdate.exe	Win32/DeceptiveDevelopment.A	AkdoorTea, a TCP RAT.

Network

IP	Domain	Hosting provider	First seen	Details
199.188.200[.]147	driverservices[.]store	Namecheap, Inc.	2025-08-08	Remote storage for DeceptiveDevelopment.
116.125.126[.]38	www.royalsevres[.]com	SK Broadband Co Ltd	2024-06-25	Remote storage for DeceptiveDevelopment.
N/A	n34kr3z26f3jzp4ckmwuv5ipqyatumdxhgjgsmucc65jac56khdy5zqd[.]onion	N/A	2023-10-06	TsunamiClient C&C server.
103.231.75[.]101	N/A	THE-HOSTING-MNT	2025-08-10	AkdoorTea C&C server.
45.159.248[.]110	N/A	THE-HOSTING-MNT	2025-06-29	BeaverTail C&C server.
45.8.146[.]93	N/A	STARK INDUSTRIES SOLUTIONS LTD	2024-10-26	Tropidoor C&C server.
86.104.72[.]247	N/A	STARK INDUSTRIES SOLUTIONS LTD	2024-10-31	Tropidoor C&C server.
103.35.190[.]170	N/A	STARK INDUSTRIES SOLUTIONS LTD	2024-06-24	Tropidoor C&C server.

MITRE ATT&CK techniques

This table was built using version 17 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Reconnaissance	T1589	Gather Victim Identity Information	DeceptiveDevelopment steals victims' credentials to be used by WageMole in consequent social engineering.
Resource Development	T1585.001	Establish Accounts: Social Media Accounts	Fake recruiter accounts created on LinkedIn, Upwork, Freelancer.com, etc.
	T1586	Compromise Accounts	Hijacked GitHub and social media accounts used to distribute malware.
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Fake job offers include attachments or links to malicious projects.

Tactic	ID	Name	Description
	T1566.002	Phishing: Spearphishing Link	ClickFix technique uses deceptive links to fake troubleshooting guides.
Execution	T1204.001	User Execution: Malicious Link	Victims are lured to fake job interview sites (e.g., ClickFix) that initiate malware download.
	T1204.002	User Execution: Malicious File	Trojanized coding challenges contain variants of BeaverTail.
	T1059	Command and Scripting Interpreter	DeceptiveDevelopment uses VBS, Python, JavaScript, and shell commands for execution.
Defense Evasion	T1078	Valid Accounts	WageMole reuses stolen identities and credentials, especially for fake recruiter and GitHub accounts.
	T1027	Obfuscated Files or Information	Obfuscated malicious scripts are hidden in long comments or outside IDE view.
	T1055	Process Injection	TsunamiKit uses injection techniques in its execution chain.
	T1036	Masquerading	Malware disguised as legitimate software (e.g., conferencing tools, NVIDIA installers).
	T1497	Virtualization/Sandbox Evasion	TsunamiKit includes environment checks and obfuscation to evade analysis.
Collection	T1056.001	Input Capture: Keylogging	InvisibleFerret includes clipboard and keylogging modules.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	AkdoorTea, BeaverTail, and Tropidoor communicate with C&C servers over HTTP/S.
	T1105	Ingress Tool Transfer	BeaverTail downloads second-stage payloads like InvisibleFerret, TsunamiKit, or Tropidoor.

Let us keep you up to date

Sign up for our newsletters