BeaverTail (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:22:29 UTC

BeaverTail is a JavaScript malware primarily distributed through NPM packages. It is designed for information theft and to load further stages of malware, specifically a multi-stage Python-based backdoor known as InvisibleFerret. BeaverTail targets cryptocurrency wallets and credit card information stored in the victim's web browsers. Its code is heavily obfuscated to evade detection. Threat actors can either upload malicious NPM packages containing BeaverTail to GitHub or inject BeaverTail code into legitimate NPM projects. Researchers have identified additional Windows and macOS variants, indicating that the BeaverTail malware family is likely still under development.

2026-03-11 · Microsoft · Microsoft Defender Experts, Microsoft Defender Security Research Team
Contagious Interview: Malware delivered through fake developer job interviews
BeaverTail OtterCookie StoatWaffle InvisibleFerret PylangGhost GolangGhost 2026-02-25 · Abstract Security ·
Contagious Interview: Evolution of VS Code and Cursor Tasks Infection Chains - Part 1
BeaverTail PylangGhost GolangGhost 2026-02-19 · GitLab · Oliver Smith
GitLab Threat Intelligence Team reveals North Korean tradecraft
BeaverTail OtterCookie 2026-01-20 · Abstract Security · Abstract Security Threat Research Organization
Contagious Interview: Tracking the VS Code Tasks Infection Vector
BeaverTail InvisibleFerret 2026-01-13 · Security Alliance · Security Alliance
VS Code Tasks Abuse by Contagious Interview (DPRK)
BeaverTail InvisibleFerret 2026-01-11 · Red Asgard · Red Asgard
Hunting Lazarus: Inside the Contagious Interview C2 Infrastructure
BeaverTail InvisibleFerret 2025-12-17 · Recorded Future · Insikt Group
PurpleBravo’s Targeting of the IT Software Supply Chain
BeaverTail InvisibleFerret PylangGhost GolangGhost 2025-11-28 · OpenSourceMalware · OpenSourceMalware
"Contagious Interview" campaign abuses Microsoft VSCode tasks to drop malware and gain persistence
BeaverTail InvisibleFerret 2025-11-13 · NVISO Labs · Bart Parys, Efstratios Lontzetidis, Stef Collart
Contagious Interview Actors Now Utilize JSON Storage Services for Malware Delivery
BeaverTail OtterCookie InvisibleFerret Beavertail TsunamiKit 2025-10-20 · Medium Deriv-Tech · Shantanu Ghumade
How a fake AI recruiter delivers five staged malware disguised as a dream job
BeaverTail OtterCookie InvisibleFerret 2025-10-16 · Cisco Talos · Michael Kelley, Vanja Svajcer
BeaverTail and OtterCookie evolve with a new Javascript module
BeaverTail OtterCookie InvisibleFerret 2025-10-10 · Socket · Kirill Boychenko
North Korea’s Contagious Interview Campaign Escalates: 338 Malicious npm Packages, 50,000 Downloads
BeaverTail InvisibleFerret 2025-09-25 · ESET Research · Matěj Havránek, Peter Kálnai
DeceptiveDevelopment: From primitive crypto theft to sophisticated AI-based deception
BeaverTail OtterCookie InvisibleFerret PylangGhost AkdoorTea GolangGhost Tropidoor TsunamiKit 2025-09-25 ·
Virus Bulletin · Matěj Havránek, Peter Kálnai

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

BeaverTail OtterCookie InvisibleFerret PylangGhost AkdoorTea GolangGhost Tropidoor TsunamiKit 2025-09-17 · GitLab · GitLab

Tech Note - BeaverTail variant distributed via malicious repositories and ClickFix lure

BeaverTail OtterCookie BeaverTail InvisibleFerret Beavertail GolangGhost 2025-08-27 · Anthropic · Anthropic

Anthropic - Threat Intelligence Report: August 2025

BeaverTail OtterCookie GolangGhost InvisibleFerret GolangGhost 2025-08-11 · nimanthadeshappriya.com · Nimantha Deshappriya

From Colombo to Pyongyang

BeaverTail BeaverTail Beavertail 2025-07-14 · Socket · Kirill Boychenko

Contagious Interview Campaign Escalates With 67 Malicious npm Packages and New Malware Loader

BeaverTail InvisibleFerret 2025-06-24 · Socket · Socket

Another Wave: North Korean Contagious Interview Campaign Drops 35 New Malicious npm Packages

BeaverTail InvisibleFerret 2025-06-03 · ANY.RUN · ANY.RUN

OtterCookie: Analysis of Lazarus Group Malware Targeting Finance and Tech Professionals

BeaverTail OtterCookie InvisibleFerret 2025-05-12 · ESET Research · ESET Research

ESET APT Activity Report Q4 2024–Q1 2025

BeaverTail InvisibleFerret GolangGhost 2025-05-07 · NTT Security · Masaya Motoda, Rintaro Koike

Additional Features of OtterCookie Malware Used by WaterPlum

BeaverTail OtterCookie InvisibleFerret 2025-04-24 · Silent Push · Silent Push

Contagious Interview (DPRK) Launches a New Campaign Creating Three Front Companies to Deliver a Trio of Malware: BeaverTail, InvisibleFerret, and OtterCookie

BeaverTail OtterCookie FrostyFerret GolangGhost InvisibleFerret GolangGhost 2025-04-23 · Trend Micro · Feike Hacquebord, Stephen Hilt

Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations

BeaverTail FrostyFerret GolangGhost InvisibleFerret GolangGhost WageMole 2025-04-11 · Bitso Quetzal Team · Mauro Eldritch

Interview with the Chollima

BeaverTail OtterCookie InvisibleFerret 2025-04-04 · Socket · Socket

Lazarus Expands Malicious npm Campaign: 11 New Packages Add Malware Loaders and Bitbucket Payloads

BeaverTail InvisibleFerret 2025-04-02 · ASEC · ASEC

BeaverTail and Tropidoor Malware Distributed via Recruitment Emails

BeaverTail Tropidoor 2025-03-31 · Aikido · Charlie Eriksen

Malware hiding in plain sight: Spying on North Korean Hackers

BeaverTail 2025-02-20 · ESET Research · ESET Research

DeceptiveDevelopment targets freelance developers

BeaverTail InvisibleFerret 2025-02-13 · Recorded Future · Recorded Future

Inside the Scam: North Korea’s IT Worker Threat

BeaverTail OtterCookie InvisibleFerret 2025-02-07 · · SI-CERT · SI-CERT

SI-CERT TZ016 / BeaverTail & InvisibleFerret

BeaverTail InvisibleFerret 2025-02-05 · Bitdefender · Alina Bizga, Andrei ANTON-AANEI, Ionuț-Alexandru Baltariu

Lazarus Group Targets Organizations with Sophisticated LinkedIn Recruiting Scam

BeaverTail InvisibleFerret tsunami 2025-01-29 · SecurityScorecard · SecurityScorecard STRIKE Team

Operation Phantom Circuit: North Korea’s Global Data Exfiltration Campaign

BeaverTail InvisibleFerret 2025-01-29 · Socket · Kirill Boychenko, Peter van der Zee

North Korean APT Lazarus Targets Developers with Malicious npm Package

BeaverTail InvisibleFerret 2024-12-24 · · NTT Security Holdings · NTT Security Holdings

Contagious Interview Uses New Malware Otter Cookie

BeaverTail OtterCookie InvisibleFerret 2024-11-26 · Arxiv · Alessio Di Santo

Lazarus Group Targets Crypto-Wallets and Financial Data while employing new Tradecrafts

BeaverTail InvisibleFerret tsunami TsunamiKit 2024-11-14 · eSentire · eSentire

Bored BeaverTail & InvisibleFerret Yacht Club – A Lazarus Lure Pt.2

BeaverTail InvisibleFerret 2024-11-14 · Palo Alto · Unit 42

Fake North Korean IT Worker Linked to BeaverTail Video Conference App Phishing Attack

BeaverTail InvisibleFerret WageMole 2024-11-04 · Israel National Cyber Directorate (INCD) · Israel National Cyber Directorate (INCD)

Deep Drive Analysis of the BeaverTail Infostealer

BeaverTail 2024-11-04 · Zscaler · Zscaler

From Pyongyang to Your Payroll: The Rise of North Korean Remote Workers in the West

BeaverTail InvisibleFerret WageMole 2024-10-29 · SecurityScorecard · SecurityScorecard STRIKE Team

The Job Offer That Wasn’t: How We Stopped an Espionage Plot

BeaverTail InvisibleFerret 2024-10-29 · · Macnica · Hiroshi Takeuchi

Job Offer from the North: Contagious Interview for Software Developers

BeaverTail InvisibleFerret 2024-10-24 · Datadog · Datadog

Tenacious Pungsan: A DPRK threat actor linked to Contagious Interview

BeaverTail InvisibleFerret 2024-10-17 · Github (ssrdio) · Gregor Spagnolo

Analysis of BeaverTail & InvisibleFerret activity

BeaverTail InvisibleFerret 2024-09-10 · Stacklok · Stacklok

Dependency hijacking: Dissecting North Korea’s new wave of DeFi-themed open source attacks targeting developers

BeaverTail InvisibleFerret 2024-09-04 · Group-IB · Sharmine Low

APT Lazarus: Eager Crypto Beavers, Video calls and Games

BeaverTail BeaverTail InvisibleFerret Beavertail 2024-07-31 · Securonix · Securonix

Research Update: Threat Actors Behind the DEV#POPPER Campaign Have Retooled and are Continuing to Target Software Developers via Social Engineering

BeaverTail 2024-07-15 · Objective-See · Patrick Wardle

This Meeting Should Have Been an Email: A DPRK stealer, dubbed BeaverTail, targets users via a trojanized meeting app

BeaverTail BeaverTail InvisibleFerret 2024-05-10 · · Qianxin Threat Intelligence Center · Threat Intelligence Center

Recruitment trap for blockchain practitioners: Analysis of suspected Lazarus (APT-Q-1) stealing operations

BeaverTail 2024-03-24 · Securonix · Securonix

Analysis of DEV#POPPER: New Attack Campaign Targeting Software Developers Likely Associated With North Korean Threat Actors

BeaverTail 2023-11-21 · Palo Alto Networks Unit 42 · Unit 42

Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors

BeaverTail InvisibleFerret WageMole

There is no Yara-Signature yet.
