

it didn't turn into a truck, but a widely spread Android botnet

Archived: 2026-04-05 21:26:43 UTC

[Android Flutter malware](#)

VB2024 paper: Android Flutter malware, Axelle Apvrille

[CeranaKeeper: a relentless shape-shifting group targeting Thailand](#)

VB2024 paper: CeranaKeeper: a relentless shape-shifting group targeting Thailand, Romain Dumont

[A wild RAT appears: reversing DinodasRAT on Linux](#)

VB2024 paper: A wild RAT appears: reversing DinodasRAT on Linux, Anderson Leite & Fabio Marengi

[Reviewing the 2022 KA-SAT incident & implications for distributed communication environments](#)

VB2024 paper: Reviewing the 2022 KA-SAT incident & implications for distributed communication environments, Joe Slowik

[Dark deals: unveiling the underground market of exploits](#)

VB2024 paper: Dark deals: unveiling the underground market of exploits, Anna Pavlovskaja

[SO that looks suspicious: leveraging process memory and kernel/usermode probes to detect Shared Object injection at scale on Linux](#)

VB2024 presentation: SO that looks suspicious: leveraging process memory and kernel/usermode probes to detect Shared Object injection at scale on Linux, Daniel Jary

[P-wave of malicious code signing](#)

VB2024 paper: P-wave of malicious code signing, Yuta Sawabe, Shogo Hayashi & Rintaro Koike

[Project 0xA11C: deoxidizing the Rust malware ecosystem](#)

VB2024 paper: Project 0xA11C: deoxidizing the Rust malware ecosystem, Nicole Fishbein & Juan Andrés Guerrero-Saade

[Sugarcoating KANDYKORN: a sweet dive into a sophisticated MacOS backdoor](#)

VB2024 paper: Sugarcoating KANDYKORN: a sweet dive into a sophisticated MacOS backdoor, Salim Bitam

[Leveraging AI to enhance the capabilities of SHAREM Shellcode Analysis Framework](#)

VB2024 paper: Leveraging AI to enhance the capabilities of SHAREM Shellcode Analysis Framework, Bramwell Brizendine

[Automatically detect and support against anti-debug with IDA/Ghidra to streamline debugging process](#)

VB2024 paper: Automatically detect and support against anti-debug with IDA/Ghidra to streamline debugging process, Takahiro Takeda

[Go-ing arsenal: a closer look at Kimsuky's Go strategic advancement](#)

VB2024 paper: Go-ing arsenal: a closer look at Kimsuky's Go strategic advancement, Jiho Kim, Sebin Lee & Sojun Ryu

[Cybercrime turned cyber espionage: the many faces of the RomCom group](#)

VB2024 paper: Cybercrime turned cyber espionage: the many faces of the RomCom group, Vlad Stolyarov & Dan Black

[Don't be a PUP-pet: exposing pay-per-install networks](#)

VB2024 paper: Don't be a PUP-pet: exposing pay-per-install networks, Dmitrij Lenz & James Wyke

[Ghosts from the past: become Gh0stbusters in 2024](#)

VB2024 paper: Ghosts from the past: become Gh0stbusters in 2024, Hiroshi Takeuchi

[Shadow play: WildCard's malware campaigns amidst Israel-Hamas conflict](#)

VB2024 paper: Shadow play: WildCard's malware campaigns amidst Israel-Hamas conflict, Nicole Fishbein & Ryan Robinson

[Supercharge your malware analysis workflow](#)

VB2024 paper: Supercharge your malware analysis workflow, Kevin Hardy-Cooper & Ryan Samaroo

[From code to crime: exploring threats in GitHub Codespaces](#)

VB2024 paper: From code to crime: exploring threats in GitHub Codespaces, Jaromir Horejsi & Nitesh Surana

[The Mask has been unmasked again](#)

VB2024 paper: The Mask has been unmasked again, Georgy Kucherin & Marc Rivero López

[CrackedCantil: a malware symphony delivered by cracked software; performed by loaders, infostealers, ransomware, et al.](#)

VB2024 paper: CrackedCantil: a malware symphony delivered by cracked software; performed by loaders, infostealers, ransomware, et al., Lena Yu

[Who plays on AZORult? An unknown attacker collects various data and spreads additional payloads with AZORult for around 5 years](#)

VB2024 paper: Who plays on AZORult? An unknown attacker collects various data and spreads additional payloads with AZORult for around 5 years, Masaki Kasuya

[Confronting the surge of macOS stealers in 2024](#)

VB2024 paper: Confronting the surge of macOS stealers in 2024, Kseniia Yamburh & Mykhailo Hrebenuik

[Code blue: energy](#)

VB2024 paper: Code blue: energy, Righard Zwienenberg & Josep Albors

[Marketplace scams: neanderthals hunting mammoths with Telekopye](#)

VB2024 paper: Marketplace scams: neanderthals hunting mammoths with Telekopye, Jakub Souček & Radek Jizba

[Multimodal AI: the sixth sense for cyber defence](#)

VB2024 paper: Multimodal AI: the sixth sense for cyber defence, Younghoo Lee

[Down the GRAYRABBIT hole - exposing UNC3569 and its mastermind](#)

VB2024 paper: Down the GRAYRABBIT hole - exposing UNC3569 and its mastermind, Steve Su, Aragorn Tseng, Chi-Yu You (YCY) & Cristiana Brafman Kittner

[Hospitals, airports and telcos - modern approach to attributing hacktivism attacks](#)

VB2024 paper: Hospitals, airports and telcos - modern approach to attributing hacktivism attacks, Itay Cohen

[Breaking boundaries: investigating vulnerable drivers and mitigating risks](#)

VB2024 paper: Breaking boundaries: investigating vulnerable drivers and mitigating risks, Jiří Vinopal

[Life and DEaTH: building detection, forensics, and intelligence at scale](#)

VB2024 paper: Life and DEaTH: building detection, forensics, and intelligence at scale, Selena Larson & Konstantin Klinger

[Workshop: Writing malware configuration parsers](#)

VB2024 Workshop: Writing malware configuration parsers, Mark Lim & Zong-Yu Wu

[Unveiling shadows: key tactics for tracking cyber threat actors, attribution, and infrastructure analysis](#)

VB2024 paper: Unveiling shadows: key tactics for tracking cyber threat actors, attribution, and infrastructure analysis

[Open by default: the hidden cost of convenience in network security](#)

VB2024 paper: Open by default: the hidden cost of convenience in network security, Aurelio Picon

[Octopus Prime: it didn't turn into a truck, but a widely spread Android botnet](#)

VB2024 paper: Octopus Prime: it didn't turn into a truck, but a widely spread Android botnet, Thibault Seret

[Modern-day witchcraft: a new breed of hybrid attacks by ransomware operators](#)

VB2024 paper: Modern-day witchcraft: a new breed of hybrid attacks by ransomware operators, Vaibhav Deshmukh, Ashutosh Raina & Sudhanshu Dubey

[Unveiling the dark side of set-top boxes: the Bigpanzi cybercrime syndicate](#)

VB2024 paper: Unveiling the dark side of set-top boxes: the Bigpanzi cybercrime syndicate, Alex Turing

[The deck is stacked: analysis of OracleBamboo's SPYDEALER Android backdoor e domestic surveillance](#)

VB2024 paper: The deck is stacked: analysis of OracleBamboo's SPYDEALER Android backdoor, Paul Rascagneres & Charles Gardner

[Arming WinRAR: deep dive into APTs exploiting WinRAR's 0-day vulnerability - a SideCopy case study](#)

VB2024 paper: Arming WinRAR: deep dive into APTs exploiting WinRAR's 0-day vulnerability - a SideCopy case study, Sathwik Ram Prakki

[Over the cassowary's nest - dissecting Turla's latest revision of the Kazuar backdoor](#)

VB2024 paper: Over the cassowary's nest - dissecting Turla's latest revision of the Kazuar backdoor, Daniel Frank & Tom Fakterman

[TA577 walked just past you: indirect syscalls in Pikabot](#)

VB2924 paper: TA577 walked just past you: indirect syscalls in Pikabot, Emre Güler

[An open-source cloud DFIR kit - Dredge!](#)

VB2024 paper: An open-source cloud DFIR kit - Dredge!, Santiago Abastante

[Byteing back: detection, dissection and protection against macOS stealers](#)

VB2024 paper: Byteing back: detection, dissection and protection against macOS stealers, Patrick Wardle

[Extending STIX 2.1 to capture malware incidents](#)

VB2024 paper: Extending STIX 2.1 to capture malware incidents, Desiree Beck

[Spot the difference: Earth Kasha's new LODEINFO campaign and the correlation analysis with APT10 umbrella](#)

VB2024 paper: Spot the difference: Earth Kasha's new LODEINFO campaign and the correlation analysis with APT10 umbrella, Hiroaki Hara

[How to hunt geopolitically driven Bitter APT operations](#)

VB2024 paper: How to hunt geopolitically driven Bitter APT operations, Shengbin Bao

[TIPS: Certified malware: a case for industry TI sharing of DigSig metadata](#)

VB2024 TIPS presentation: Certified malware: a case for industry TI sharing of DigSig metadata, Samir Mody

[TIPS: Bye Bye WarZone RAT \(for now\); Capturing Cybercriminals through #CoordinatedDisruption, Part 2](#)

VB2024 TIPS presentation: Bye Bye WarZone RAT (for now); Capturing Cybercriminals through #CoordinatedDisruption, Part 2, Sara Eberle & Mike Bordini

[TIPS: Fireside chat: Achtung Baby! Cybersecurity insights with U2 \(you too\)](#)

VB2024 TIPS presentation: Fireside chat: Achtung Baby! Cybersecurity insights with U2 (you too), Jeannette Jarvis, Selena Larson, Jeanette Miller-Osborn & Kathi Whitbey

[TIPS: Unveiling cybersecurity impact: the role of published security findings in strengthening internet defence strategies](#)

VB2024 TIPS presentation: Unveiling cybersecurity impact: the role of published security findings in strengthening internet defence strategies, Slawek Grzonkowski

[TIPS: Panel: Briskets or biscuits: how to construct your CTI team](#)

VB2024 TIPS presentation: Panel: Briskets or biscuits: how to construct your CTI team, Noortje Henrichs, Hossein Hadian Jazi, Kathi Whitbey, Righard Zwienenberg

[TIPS: Building resilience through collaboration: a data-driven and data-informed cyber threat intelligence sharing style guide based on STIX 2.1](#)

VB2024 TIPS presentation: Building resilience through collaboration: a data-driven and data-informed cyber threat intelligence sharing style guide based on STIX 2.1, Linda Beverly

[TIPS: Indicator wranglin' - an approach to dynamically typing IOCs with poor data context](#)

VB2024 TIPS presentation: Indicator wranglin' - an approach to dynamically typing IOCs with poor data context, Noah Dunn

[TIPS: Adaptive protection put to the test](#)

VB2024 TIPS presentation: Adaptive protection put to the test, Zsomber Kovacs, Liam O'Murchu

[TIPS: Stix and stones: enabling faster intelligence gathering with GenAI and OASIS](#)

VB2024 TIPS presentation: Stix and stones: enabling faster intelligence gathering with GenAI and OASIS, Kieran Hughes

[TIPS: Operation Endgame](#)

VB2024 TIPS presentation: Operation Endgame, Marijn Schuurbiens

[Opening keynote: Solving puzzles: protecting high-risk communities](#)

VB2024 opening keynote: Solving puzzles: protecting high-risk communities, Runa Sandvik

[Closing keynote: May you live in interesting times](#)

VB2024 closing keynote: May you live in interesting times, Brian Honan

[TIPS: Radical transparency in cyber](#)

VB2024 TIPS presentation: Radical transparency in cyber, Suzanne Spaulding

[Threat intelligence for high-risk communities](#)

VB2024 presentation: Threat intelligence for high-risk communities, Martijn Grooten

[IcePeony with the '996' work culture](#)

VB2024 paper: IcePeony with the '996' work culture, Rintaro Koike & Shota Nakajima

[Unmasking DarkPlum: inside the operations of DPRK's elite cyber espionage group](#)

VB2024 paper: Unmasking DarkPlum: inside the operations of DPRK's elite cyber espionage group, Amata Anantaprayoon & Rintaro Koike

[The Impersonators](#)

VB2024 paper: The Impersonators, Gabor Szappanos & Steeve Gaudreault

[The dark dream of the Lumma malware developer](#)

VB2024 paper: The dark dream of the Lumma malware developer, Raman Ladutska

[RevivalStone: new puzzle posed by Winnti group](#)

VB2024 paper: RevivalStone: new puzzle posed by Winnti group, Yoshihiro Ishikawa & Takuma Matsumoto

[Mind the \(air\) gap: GoldenJackal gooses government guardrails](#)

VB2024 presentation: Mind the (air) gap: GoldenJackal gooses government guardrails, Matias Porolli

[The Phantom Syndicate: a hacking collective with a North Korean allegiance](#)

VB2024 paper: The Phantom Syndicate: a hacking collective with a North Korean allegiance, Youjin Lee

[Tracking FIN7 malware honeypots, new AI deepfake lures](#)

VB2024 paper: Tracking FIN7 malware honeypots, new AI deepfake lures, Zach Edwards

[BEC and phishing targets local election candidate \(me!\)](#)

VB2024 paper: BEC and phishing targets local election candidate (me!), Andrew Brandt

[All quiet on the signalling front? Dispatches from the front-line of telecom network security](#)

VB2024 paper: All quiet on the signalling front? Dispatches from the front-line of telecom network security, Cathal Mc Daid

[Proactively hunting for low-reputed infrastructure used by large cybercrimes and APTs](#)

VB2024 paper: Proactively hunting for low-reputed infrastructure used by large cybercrimes and APTs, Mohamed Nabeel, Keerthiraj Nagaraj & Alex Starov

[Origins of a logger - Agent Tesla](#)

VB2024 paper: Origins of a logger - Agent Tesla, Berk Albayrak & Utku Çorbacı

[A web of surveillance](#)

VB2024 paper: A web of surveillance, Jurre van Bergen

[Getting cozy with milk and WARMCOOKIES](#)

VB2024 presentation: Getting cozy with milk and WARMCOOKIES, Daniel Stepanic

[TIPS: Wrap-up](#)

VB2024 TIPS presentation: Wrap-up, Michael Daniel

Source: <https://www.virusbulletin.com/conference/vb2024/abstracts/octopus-prime-didnt-turn-truck-widely-spread-android-botnet/>