RokRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:47:16 UTC

It is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex.

2025-12-21 · Genians · Genians
Operation Artemis: Analysis of HWP-Based DLL Side Loading Attacks

RokRAT 2025-07-21 · AhnLab · ASEC
RokRAT Malware Using Malicious Hangul (.HWP) Documents

RokRAT 2025-05-12 · Genians · Genians
Analysis of APT37 Attack Case Disguised as a Think Tank for National Security Strategy in South Korea (Operation. ToyBox Story)

RokRAT 2025-05-10 · cocomelonc · cocomelonc
Malware development trick 47: simple Windows clipboard hijacking. Simple C example.

CosmicDuke RokRAT 2025-05-01 · cocomelonc · cocomelonc
Malware development trick 46: simple Windows keylogger. Simple C example.

MyDoom Nokki RokRAT 2025-03-01 · ZW01f · Mohamed Ezat
An in-depth analysis of APT37’s latest campaign

RokRAT 2025-02-20 · Cyber Security News · Balaji N
APT-C-28 Group Launched New Cyber Attack With Fileless RokRat Malware

RokRAT 2024-05-07 · AhnLab · ASEC
LNK File Disguised as Certificate Distributing RokRAT Malware

RokRAT 2024-03-04 · · Weixin · Hunting Shadow Lab
Shadow Hunting: Analysis of APT37’s attack activities against South Korea using North Korean political topics

RokRAT 2024-03-01 · 0x0v1 · Ovi
APT37's ROKRAT HWP Object Linking and Embedding

RokRAT 2023-06-06 · Security Intelligence · Agnes Ramos-Beauchamp, Claire Zaboeva, Joshua Chung, Melissa Frydrych
ITG10 Likely Targeting South Korean Entities of Interest to the Democratic People’s Republic of Korea (DPRK)

RokRAT 2023-05-01 · Check Point Research · Check Point Research
Chain Reaction: RokRAT's Missing Link

Amadey RokRAT 2023-04-26 · AhnLab · bghjmun
RokRAT Malware Distributed Through LNK Files (*.lnk): RedEyes (ScarCruft)

RokRAT 2023-03-23 · Medium s2wlab · BLKSMTH, S2W TALON
Scarcruft Bolsters Arsenal for targeting individual Android devices

RambleOn RokRAT 2023-01-01 · ThreatMon · Seyit Sigirci (@h3xecute), ThreatMon Malware Research Team

Reverse Engineering RokRAT: A Closer Look at APT37's Onedrive-Based Attack Vector

RokRAT 2022-09-28 · Twitter (@ESETresearch) · ESET Research

Twitter Thread linking CloudMensis to RokRAT / ScarCruft

CloudMensis RokRAT 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42

Moldy Pisces

RokRAT APT37 2022-04-28 · PWC · PWC UK

Cyber Threats 2021: A Year in Retrospect (Annex)

Cobalt Strike Conti PlugX RokRAT Inception Framework Red Menshen 2021-08-24 · Volexity · Damien Cash, Josh Grunzweig, Steven Adair, Thomas Lancaster

North Korean BLUELIGHT Special: InkySquid Deploys RokRAT

RokRAT 2021-07-14 · Medium s2wlab · Jaeki Kim

Matryoshka : Variant of ROKRAT, APT37 (Scarcruft)

RokRAT 2021-02-18 · PTSecurity · PTSecurity

https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/

Poet RAT Gravity RAT Ketrican Okrum OopsIE Remcos RogueRobinNET RokRAT SmokeLoader 2021-01-06 · Malwarebytes · Hossein Jazi

Retrohunting APT37: North Korean APT used VBA self decode technique to inject RokRat

RokRAT 2020-06-16 · IBM · IBM Security X-Force® Incident Responseand Intelligence Services (IRIS)

Cloud ThreatLandscape Report 2020

QNAPCrypt RokRAT 2020-05-21 · PICUS Security · Süleyman Özarslan

T1055 Process Injection

BlackEnergy Cardinal RAT Downdelph Emotet Kazuar RokRAT SOUNDBITE 2020-03-30 · Kaspersky SAS · Seongsu Park

Behind the Mask of ScarCruft

RokRAT 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-02-19 · Lexfo · Lexfo

The Lazarus Constellation A study on North Korean malware

FastCash AppleJeus BADCALL Bankshot Brambul Dtrack Duuzer DYEPACK ELECTRICFISH HARDRAIN Hermes HOPLIGHT Joanap KEYMARBLE Kimsuky MimiKatz MyDoom NACHOCHEESE NavRAT PowerRatankba RokRAT Sierra(Alfa,Bravo, ...) Volgmer WannaCryptor 2019-08-12 · Kindred Security · Kindred Security

An Overview of Public Platform C2's

HTML5 Encoding LOWBALL Makadocs MiniDuke RogueRobinNET RokRAT 2019-08-01 · Kaspersky Labs · GReAT

APT trends report Q2 2019

ZooPark magecart POWERSTATS Chaperone COMpfun EternalPetya FinFisher RAT HawkEye Keylogger HOPLIGHT Microcin NjRAT Olympic Destroyer PLEAD RokRAT Triton Zebrocy 2019-05-13 · Kaspersky Labs · GReAT

ScarCruft continues to evolve, introduces Bluetooth harvester

Konni RokRAT UACMe APT37 2018-11-16 · · Kim Yejun

Return to ROKRAT!! (feat. FAAAA...Sad...)

RokRAT 2018-10-03 · Intezer · Jay Rosenberg

APT37: Final1stspy Reaping the FreeMilk

Final1stSpy RokRAT 2018-02-27 · VMWare Carbon Black · Jared Myers

Threat Analysis: ROKRAT Malware

RokRAT 2018-02-20 · FireEye · FireEye

APT37 (REAPER) The Overlooked North Korean Actor

PoorWeb RokRAT APT37 2018-01-16 · Cisco Talos · Paul Rascagnères, Warren Mercer

Korea In The Crosshairs

Freenki Loader RokRAT APT37 2018-01-16 · Cisco Talos · Jungsoo An, Paul Rascagnères, Warren Mercer

Korea In The Crosshairs

Freenki Loader PoohMilk Loader RokRAT APT37 2017-11-28 · Cisco · Jungsoo An, Paul Rascagnères, Warren Mercer

ROKRAT Reloaded

RokRAT 2017-04-03 · Cisco Talos · Matthew Molyett, Paul Rascagnères, Warren Mercer

Introducing ROKRAT

RokRAT 2017-01-01 · Cisco Talos · Paul Rascagnères, Warren Mercer

Introducing ROKRAT

RokRAT

▶ [TLP:WHITE] win_rokrat_auto (20251219 | Detects win.rokrat.)
