

MOONLOCK.COM →

macOS Malware Threats in 2023

Intro

Moonlock Lab has gathered the biggest **macOS malware threats in 2023**

The macOS threat landscape in 2023 has been marked by the rise of infostealers and a general increase in the number of Dark Web actors targeting the system. For this report, we've gathered the most significant macOS malware threats detected each month of the year.

04 Top malware categories ↗

05 January ↗

06 February ↗

07 March ↗

09 April ↗

13 May ↗

15 June ↗

16 July ↗

21 August ↗

25 September ↗

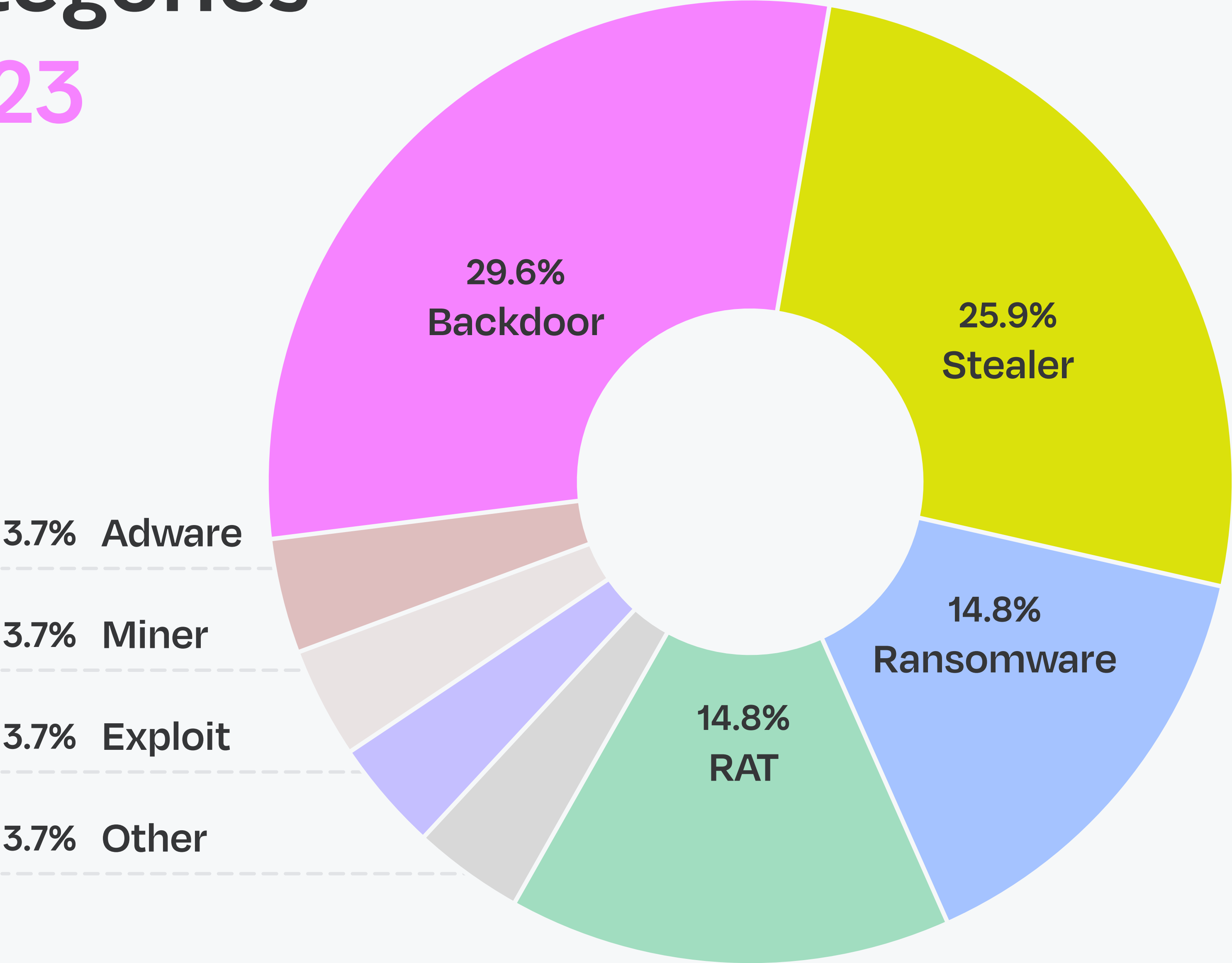
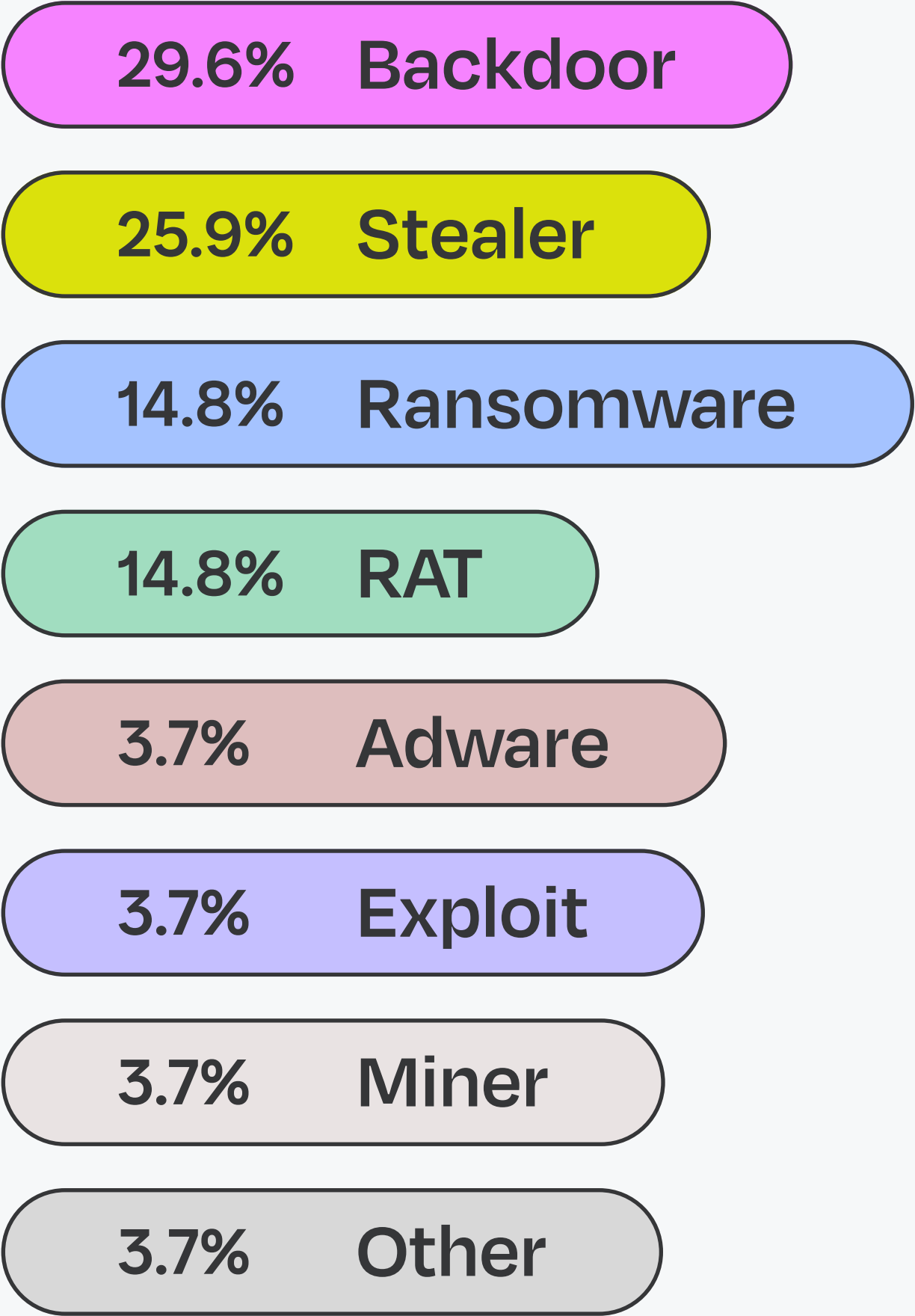
27 October ↗

30 November ↗

31 December ↗

32 Sources ↗

Top malware categories on macOS in 2023



Jan
2023

Dridex RAT

Threat level:  Low

A new variant of the Dridex banking malware, previously targeting Windows systems, has been discovered attempting to infect Apple's macOS. The malware uses a novel technique, overwriting document files with malicious macros, avoiding the need to disguise them as invoices or business-related files.

Miner

XMRig

Threat level:  High

The campaign disguises itself as legitimate software like Apple Logic Pro X and Final Cut Pro to trick victims into installing malicious apps. By utilizing open source XMRig crypto mining software and the I2P network tool, the attackers conduct crypto mining operations on compromised Mac devices.

Feb
2023

Stealer

SmoothOperator 3CX

Threat level:  High

Mar
2023

A supply chain attack involving the 3CX Desktop application, attributed to a North Korean TA, UTA0040. The malware, dubbed SmoothOperator, was distributed through 3CX's automatic updates, affecting both Windows and macOS platforms.

Stealer

MacStealer

Threat level: 🟡 Middle

New macOS stealer malware controlled via Telegram. It extracts sensitive data from browsers and KeyChain databases, affecting macOS Catalina and newer versions on Intel M1 and M2 CPUs. The malware spreads through a fake password prompt in a .dmg file and sends collected data to a Command and Control server via Python requests.

Mar
2023

Backdoor

RustBucket

Threat level:  High

Associated with the BlueNorOff group and operated by the DPRK, RustBucket communicates with C2 servers to download and execute various payloads. The malware is actively evolving, incorporating built-in persistence and employing signature reduction techniques to avoid detection. Its new variant REF9135 specifically targets a venture-backed cryptocurrency company in the United States.

Apr
2023

Stealer

AMOS (Atomic Stealer)

Threat level:  High

New malware called Atomic macOS Stealer (AMOS), being advertised on a Telegram channel. AMOS specifically targets macOS systems, stealing sensitive information including keychain passwords, crypto wallets, browser data, and files from victims' machines. The malware is distributed via .dmg files, displaying a fake password prompt to obtain system passwords.

Apr
2023

Backdoor

POOLRAT

Threat level:  Low

UNC4736, a financially motivated North Korean group, employed the POOLRAT backdoor to gain access, enabling the collection of system information, execution of commands, and manipulation of files.

Apr
2023

Ransomware

Lockbit attacks

Threat level: 🟡 Middle

The LockBit ransomware gang, previously known for targeting Windows, Linux, and VMware ESXi servers, has now created encryptors specifically designed for macOS, including Apple M1-powered devices.

Apr
2023

Backdoor

Snake

Threat level: 🟡 Middle

May
2023

A Turla APT attack specifically targeting MacOS systems. The backdoor, dubbed Snake, was identified as the tool used in these targeted attacks. The malicious code was found within a file associated with Adobe Flash Player installation.

Other

Geacon

Threat level:  Low

May
2023

Geacon, a Go implementation of the infamous Cobalt Strike red-teaming tool, has raised concerns as it increasingly targets macOS devices. Geacon variants have been detected on VirusTotal, some showing signs of genuine malicious intent.

Backdoor

JokerSpy

Threat level:  High

REF9134 is a complex cyber intrusion dubbed JokerSpy, targeting a prominent Japanese cryptocurrency exchange. Attackers employed the sh.py backdoor to deploy the macOS Swiftbelt enumeration tool, showcasing advanced evasion techniques and manipulation of system permissions.

Jun
2023

Backdoor

DangerousPassword

Threat level:  High

DangerousPassword, a cyberattack group, targeted cryptocurrency exchange developers using malware that exploited vulnerabilities in Windows, macOS, and Linux systems. In macOS and Linux, the attackers injected malicious code into Python files, compromising user data and system information.

Jul
2023

Backdoor

NokNok (GorjolEcho)

Threat level:  High

Jul
2023

The threat group APT42, also known as Charming Kitten, targeted experts in Middle Eastern affairs and nuclear security using benign emails. What's noteworthy is their development of sophisticated malware named GorjolEcho and its macOS variant, NokNok.

Stealer

ShadowVault

Threat level:  High

New ShadowVault is sophisticated malware designed to steal sensitive data from macOS devices. ShadowVault operates silently in the background, collecting valuable information like login IDs and financial data.

Jul
2023

Stealer

Realst

Threat level:  **High**

New infostealer being distributed through fake blockchain games on malicious websites. Realst steals sensitive information, including crypto wallets and passwords, using various methods such as AppleScript spoofing and Terminal prompts. The malware comes in different variants with distinct characteristics, and some samples are preparing to target Apple's macOS 14 Sonoma.

Jul 2023

Backdoor

FULLHOUSE. DOORED

Threat level: 🟡 Middle

Fullhouse (aka FULLHOUSE.DOORED) is a custom backdoor used by subsets of the North Korean Lazarus Group.

Fullhouse is written in C/C++ and includes the capabilities of a tunneler and backdoor commands support, such as shell command execution, file transfer, file management, and process injection.

Jul
2023

RAT

HVNC

Threat level: 🟡 Middle

HVNC allows attackers to gain unauthorized access to macOS devices silently. Offered at \$60,000, the HVNC tool includes features like persistence, reverse shell, and remote file manager, compatible with macOS versions 10 to 13.2. An additional \$20,000 add-on enhances its malicious capabilities.

Aug
2023

Stealer

XLoader

Threat level: 🟡 **Middle**

XLoader, a persistent malware targeting macOS users, has reemerged in a new form as an office productivity app named OfficeNote. This infostealer, previously limited by Java dependencies, is now written in C and Objective C languages. Distributed through a revoked Apple Developer signature, XLoader attempts to steal user data from Chrome and Firefox browsers.

Aug
2023

Adware

AdLoad

Threat level: ● High

AdLoad malware, initially discovered in 2017, continues to infect Mac systems with a recent discovery of a previously unreported payload. The malware, acting as a downloader for various payloads, has been observed delivering adware, bundleware, PiTM attacks, backdoors, and proxy applications to macOS systems.

Aug
2023

Aug
2023

Ransomware

Akira

Threat level:  Low

The Akira ransomware has been targeting corporate networks through Cisco VPN products. This ransomware operation breaches networks, steals data, and encrypts files.

Stealer

MetaStealer

Threat level:  High

New MetaStealer malware is targeting business users. MetaStealer spreads through deceptive disk image bundles, posing as fake clients. Once executed, it attempts to extract sensitive data and connect to specific domains.

Sep
2023

Ransomware

Knight

Threat level:  High

Knight ransomware, an evolution of Cyclops ransomware, emerged in August 2023 and operates as a RaaS. It targets both enterprise and SMB environments. The threat operator offers normal and 'lite' versions of the ransomware, delivering it primarily through phishing campaigns. Knight ransomware is designed to target macOS systems along with Windows and Linux/ESXi platforms

Sep
2023

Ransomware

Monti

Threat level:  High

Oct
2023

A new ransomware affiliate scheme called Monti has emerged on dark web forums, actively participating in macOS discussions. Monti claims to be using a modified version of Conti's EXSi ransomware and has experienced operators linked to the early days of REvil in 2019.

Exploit

DirtyNIB

Threat level:  Low

Oct
2023

Researchers created a method called DirtyNIB to gain code execution through a modified NIB file. The exploit was initially found in macOS Monterey and still works in Sonoma, although new constraints and protections have been introduced in subsequent macOS versions.

RAT

TriangleDB

Threat level: 🟡 Middle

Researchers investigating Operation Triangulation uncovered a complex iOS spyware implant called TriangleDB, deployed through targeted attacks involving exploits to gain root privileges. The implant, written in Objective-C, operates in memory, making detection challenging. It communicates with C2 servers using encrypted Protobuf messages, allowing attackers to remotely control infected devices.

Oct
2023

RAT

Kandycorn

Threat level:  High

A macOS-targeted campaign called REF7001 involves Python scripts for initial compromise, followed by delivery of SugarLoader and HLoader malware variants, culminating in the KandyKorn payload. This malware can collect data, execute arbitrary commands, and retrieve additional payloads from the attackers' servers.

Nov
2023

Backdoor













WSProxy














Threat level: 🟡 Middle







Discovered by the Kaspersky research team, WSProxy is distributed via cracked software packages. It installs a backdoor as GoogleHelperUpdater agent and has Proxy and CnC functionality. No malicious payloads were detected at the time.

Dec
2023

Sources

-  [Dridex Malware Now Attacking macOS Systems with Novel Infection Method](#)
-  [Analysis of a MacOS Malware Spotted with Old Dridex Sample](#)
-  [Cybercriminals Use macOS Apps to Deploy XMRig Crypto Mining Software](#)
-  [A Comprehensive Analysis of the 3CX Attack](#)
-  [Ironing out \(the macOS\) details of a Smooth Operator](#)
-  [SmoothOperator | Ongoing Campaign Trojanizes 3CXDesktopApp in Supply Chain Attack](#)
-  [MacStealer: Unveiling a Newly Identified MacOS-based Stealer Malware](#)
-  [BlueNoroff APT group targets macOS with 'RustBucket' Malware](#)
-  [The DPRK strikes using a new variant of RUSTBUCKET](#)
-  [Threat Actor Selling New Atomic macOS \(AMOS\) Stealer on Telegram](#)
-  [Under the hood of the Atomic macOS stealer \(AMOS\)](#)
-  [3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible](#)

-  [MalwareHunterTeam on X](#)
-  [Victor Kubashok on X](#)
-  [Geacon Brings Cobalt Strike Capabilities to macOS Threat Actors](#)
-  [Initial research exposing JOKERSPY](#)
-  [DangerousPassword attacks targeting developers' Windows, macOS, and Linux environments](#)
-  [Welcome to New York: Exploring TA453's Foray into LNKs and Mac Malware](#)
-  [Guardz Uncovers A New Threat Targeting macOS – 'ShadowVault'](#)
-  [Apple Crimeware | Massive Rust Infostealer Campaign Aiming for macOS Sonoma Ahead of Public Release](#)
-  [North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack](#)
-  [The Massive macOS Threats Trending in the Dark Web](#)
-  [XLoader's Latest Trick | New macOS Variant Disguised as Signed OfficeNote App](#)
-  [Mac systems turned into proxy exit nodes by AdLoad](#)
-  [Akira ransomware targets Cisco VPNs to breach organizations](#)

-  [macOS MetaStealer | New Family of Obfuscated Go Infostealers Spread in Targeted Attacks](#)
-  [Knight Ransomware: In-Depth Analysis, Detection, and Mitigation](#)
-  [1,000% increase in dark web threat actors targeting macOS](#)
-  [MacOS "DirtyNIB" Vulnerability](#)
-  [Operation Triangulation](#)
-  [Elastic catches DPRK passing out KANDYKORN](#)