NullMixer Drops Multiple Malware Families

blog.polyswarm.io/nullmixer-drops-multiple-malware-families

Related Families: SmokeLoader, RedLine Stealer, PseudoManuscrypt, ColdStealer, FormatLoader, CsdiMonetize, Disbuk, Fabookie, DanaBot, Racealer, Generic.ClipBanker, SgnitLoader, ShortLoader, Downloader.INNO, LgoogLoader, Downloader.Bitser, C-Joker, PrivateLoader, Satacom, GCleaner, Vidar

Verticals Targeted: Multiple

Executive Summary

Kaspersky recently reported on NullMixer, a dropper used to drop a myriad of malware families, including SmokeLoader, RedLine Stealer, PseudoManuscrypt, ColdStealer, FormatLoader, CsdiMonetize, Disbuk, Fabookie, DanaBot, Racealer, Generic.ClipBanker, SgnitLoader, ShortLoader, Downloader.INNO, LgoogLoader, Downloader.Bitser, C-Joker, PrivateLoader, Satacom, GCleaner, and Vidar.

Key Takeaways

- NullMixer drops a myriad of malware families.
- NullMixer is typically disguised as software related to cracks, keygens, and activators.
- Currently, at least 21 families are dropped by NullMixer, including bankers, backdoors, stealers, and others.

What is NullMixer?

NullMixer is a dropper currently being used to drop multiple malware families. According to Kaspersky, NullMixer is spread via malicious websites related to cracks, keygens, and activators used for software piracy. Most NullMixer activity was observed targeting users in the US, Brazil, India, Russia, Italy, Germany, France, Egypt, and Turkey.

The threat actors behind NullMixer employ sophisticated SEO to stay near the top of search results. When unwitting victims attempt to download software from the sites, they experience multiple redirects, eventually landing on a page containing an archived password-protected file. While the victims think they are downloading the desired software, the archive actually contains NullMixer.

NullMixer drops the following malware families:

SmokeLoader

SmokeLoader is a modular malware primarily used to download and execute other payloads.

RedLine Stealer

RedLine Stealer is a stealer malware that harvests various types of information, including saved credentials, autocomplete data, cryptocurrency, and credit card information. It also takes a system inventory of the victim's machine, gathering information on the username, location data, hardware configuration, and installed security software. RedLine Stealer can also upload and download files, execute commands, and send information about the infected computer to the C2.

PseudoManuscrypt

PseudoManuscrypt is a MaaS (malware as a service) used to steal cookies from multiple applications, including Firefox, Chrome, Edge, Opera, and Yandex. The malware also allows keylogging and cryptocurrency theft using ClipBanker. PseudoManuscrypt uses the KCP protocol to download additional plugins.

ColdStealer

ColdStealer is used to steal multiple types of information, including crypto wallets, FTP credentials, and credentials from browsers.

FormatLoader

FormatLoader uses hardcoded URLs as format strings. It is used to download an additional file and infect a victim's machine.

CsdiMonetize

CsdiMonetize is an advertising platform typically used to install PUAs (potentially unwanted applications). It also drops trojans, such as Glupteba.

Disbuk

Disbuk, also known as Socelar, steals Facebook cookies from Chrome and Firefox, access tokens, account IDs, and Amazon cookies. It installs a malicious browser extension masquerading as Google Translate.

Fabookie

Fabookie targets Facebook ads and steals browser session cookies. It also uses Facebook Graph API Queries to harvest information about a user's account, linked payment method, balance, and friends.

DanaBot
DanaBot is a modular banking trojan. Functionalities include stealing information and injecting fake forms to collect payment data. It can also give a threat actor full remote access to a machine using the VNC plugin.

Racealer

Racealer, also known as RaccoonStealer, is a relatively unsophisticated malware as a service written in C/C++. More recent versions use Telegram to retrieve C2 information and malware configurations.

Generic.ClipBanker

Generic.ClipBanker is a clipboard hijacker. It monitors the victim machine for cryptocurrency addresses and replaces them with the threat actor's cryptocurrency wallet address to intercept payments.

SgnitLoader

SgnitLoader is a trojan downloader written in C#.

ShortLoader
ShortLoader is another trojan downloader.

Downloader.INNO

Downloader.INNO is an Inno Setup installer that utilizes Inno Download Plugin to download a file from the C2. The downloaded file is related to the Satacom downloader family.

LgoogLoader

LgoogLoader is an installer that drops three files: a batch file, an AutoIt interpreter, and an AutoIt script. After downloading, it executes the batch file.

Downloader.Bitser

Downloader.Bitser is an NSIS installer that installs Lightning Media Player and runs bitsadmin to download additional files.

C-Joker

C-Joker is an Exodus wallet stealer.

PrivateLoader

PrivateLoader is a pay-per-install loader similar to LgoogLoader and SmokeLoader.

Satacom

Satacom, also known as LegionLoader, is a loader that uses anti-analysis methods borrowed from al-khazer.

GCleaner

GCleaner is a pay-per-install loader. It was previously distributed as Garbage Cleaner, which mimicked CCleaner. GCleaner is used to download PUAs such as Azorult, Vidar, Predator the Thief, and others.

Vidar

Vidar is an infostealer that employs password grabbing. It steals browser autofill information, cookies, saved payment information, browser history, coin wallets, and Telegram databases. It can also take screenshots.

IOCs

PolySwarm has multiple samples of NullMixer.

f2ec0aaf1cd2359465bd42b1951d1c59267137ddba96c85f28c981d622ecf093b69a81971bd4800d1737ef67ef47e5b6793723c1fd4b75dfbdddf8b28bd93dd5c91dec1cd5b97079481c76d5d597dde67b60c301ea900eab7db99776d52b465a

You can use the following CLI command to search for all NullMixer samples in our portal:

$ polyswarm link list -f NullMixer

Don't have a PolySwarm account? Go here to sign up for a free Community plan or to subscribe.

Contact us at hivemind@polyswarm.io | Check out our blog | Subscribe to our reports

Topics: Threat Bulletin, RedLine Stealer, NullMixer, Satacom, Dropper, SmokeLoader, PseudoManuscrypt, ColdStealer, FormatLoader, CsdiMonetize, Disbuk, Fabookie, DanaBot, Racealer, Generic.ClipBanker, SgnitLoader, ShortLoader, Downloader.INNO, LgoogLoader, Downloader.Bitser, C-Joker, PrivateLoader, GCleaner, Vidar

Written by PolySwarm Tech Team