Threat actor believed to be spreading new MedusaLocker variant since 2022

By Tiago Pereira

Published: 2024-10-03 · Archived: 2026-04-05 21:53:21 UTC

- Cisco Talos has discovered a financially motivated threat actor, active since 2022, recently observed delivering a MedusaLocker ransomware variant.
- Intelligence collected by Talos on tools regularly employed by the threat actor allows us to see an estimate of the amount and countries of origin of this group's victims. This actor has been active since at least late 2022 and targets organizations worldwide, although the number of victims was higher than average in EU countries until mid-2023 and, since then, in Latin American countries.
- This threat actor was observed distributing a MedusaLocker ransomware variant known as "BabyLockerKZ." This variant is compiled with a PDB path containing the word "paid_memes" which is also present in other tools observed during the attacks, presumably by the same author.
- Talos has new information on the attacker's tools, including BabyLockerKz and attacker TTPs and IOCs to assist in detecting and preventing further attacks.

Talos has recently observed an attack leading to the deployment of a MedusaLocker ransomware variant known as "BabyLockerKZ." The distinguishable techniques — including consistently storing the same set of tools in the same location on compromised systems, the use of tools that have the PDB path with the string "paid_memes," and the use of a lateral movement tool named "checker" — used in the attack led us to take a deeper look to try to understand more about this threat actor.

This attacker uses several publicly known attack tools and living-off-the-land binaries (LoLBins), a set of tools built by the same developer (possibly the attacker) to assist in credential theft and lateral movement in compromised organizations. These tools are mostly wrappers around publicly available tools that include additional functionality to streamline the attack process and provide graphical or command-line interfaces.

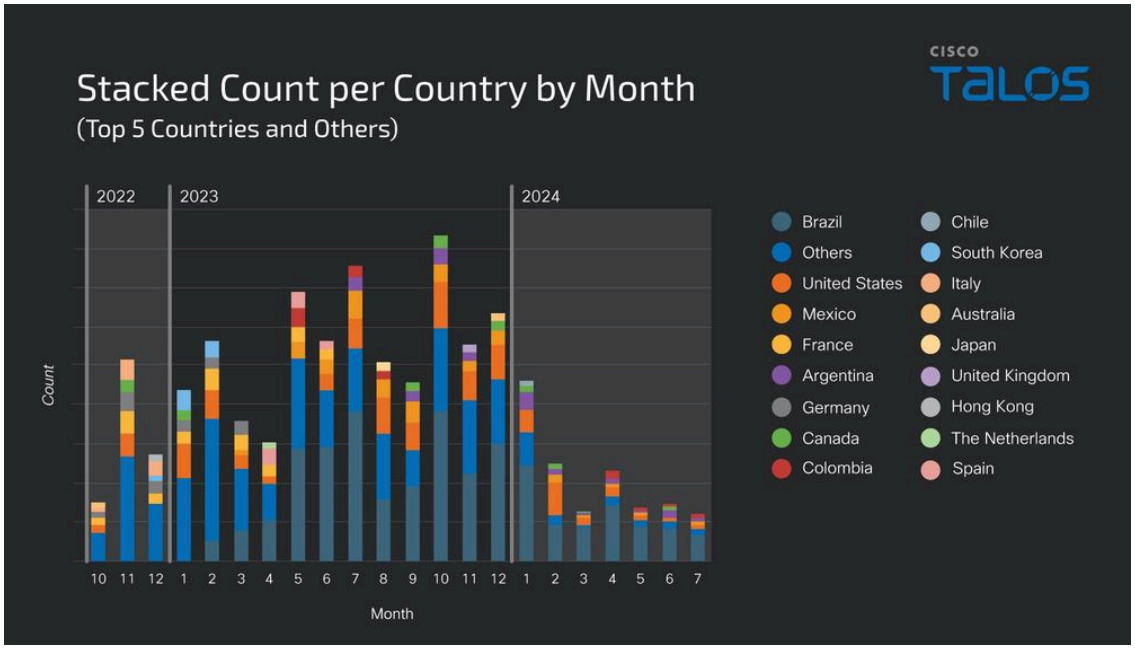
The same developer built the MedusaLocker variant used in the initial attack. This variant that uses the same chat and leak site URLs contains several differences to the original MedusaLocker ransomware, such as a different autorun key or an extra public and private key set stored in the registry. Based on the name of the autorun key, the attackers call this variant "BabyLockerKZ."

We assess with medium confidence that the actor is financially motivated, likely working as an IAB or an affiliate of a ransomware cartel, and has been carrying out attacks since at least 2022. Our telemetry indicates that the actor opportunistically targeted many victims worldwide. In late 2022 and early 2023, most victims were in European countries, but since the first quarter of 2023, the group's focus shifted toward Latin American countries and, as a result, the number of victims per month almost doubled.

Tracking BabyLockerKZ across the globe

Intelligence collected by Talos on tools regularly employed by the threat actor allows us to estimate the number of, and the countries of origin of the victims. Although this is unlikely to capture all of the adversary's activities, it still provides a look at a specific window of activity.

The actor has been active since at least October 2022. At that time, the targets were mostly located in European countries such as France, Germany, Spain or Italy. During the second quarter of 2023, the attack volume per month almost doubled, and the group shifted its focus toward Latin American countries such as Brazil, Mexico, Argentina and Colombia, as shown in the chart below. The attacks kept a steady volume of around 200 unique IPs compromised per month until the first quarter of 2024 when the attacks decreased.



The actor has consistently compromised a large number of organizations, often more than 100 per month, since at least 2022. This reveals the professional and highly aggressive nature of the attacks and is coherent with the activity we would expect from an IAB or ransomware affiliate.

Attacker TTPs and tools

During the attack leading to the deployment of the BabyLockerKZt, the adversary used several publicly known attack tools and others that could be unique to this actor. The group frequently used the Music, Pictures or Documents user folders of compromised systems to store attack tools. For example, the following paths were used to store tools during this attack:

- c:\users\<user>\music\advanced_port_scanner_2.5.3869.exe
- c:\users\<user>\music\hrsword\hrsword install.bat
- c:\users\<user>\music\killav\build.004\disabler.exe
- c:/users/<user>/music/checker/checker(222).exe
- c:/users/<user>/music/checker/invoke-thehash.ps1
- c:/users/<user>/music/checker/checker (222).exe
- c:/users/<user>/music/checker/invoke-smbexec.ps1

- c:/users/<user>/music/checker/invoke-wmiexec.ps1
- c:/users/<user>/appdata/roaming/ntsystem/ntlhost.exe.exe
- c:/users/<user>/appdata/local/temp/advanced port scanner 2/advanced_port_scanner.exe
- c:/users/<user>/appdata/local/temp/is-juad3.tmp/advanced_port_scanner_2.5.3869.tmp

These are similar to a previous attack leading to MedusaLocker ransomware, documented by ASEC in February 2023, which our telemetry suggests was a more active period for this threat actor.

Some of the publicly known tools used by the attacker are:

- HRSword_v5.0.1.1.rar: A tool used to disable AV and EDR software.
- Advanced_Port_Scanner_2.5.3869.exe: A network-scanning tool with several additional features to map internal networks and devices.
- Netscan.exe: SoftPerfect Network Scanner: A tool similar to Advanced Port Scanner.
- Processhacker.exe: Process Monitoring and administration software. Allows a TA to enumerate and control processes running on the infected endpoint.
- PCHunter64.exe: A tool similar to processhacker.
- Mimikatz: A tool to dump Windows user credentials from memory.

While most of the tools the attacker uses are publicly available, they also use some tools that are not widely distributed that streamline the attack process by automating the interaction between popular attack tools (e.g., Mimikatz, Invoke-the-hash, PSEXEC, RDP) and by adding convenient functionality and interfaces. One of these tools, called “Checker” used in an attack that deployed BabyLockerKZ, consisted of pivotal characteristics of BabyLockerKZ, the “Checker” tool has a PDB path containing the string “**paid_memes**”. Pivoting off this string, we identified files on VirusTotal, of which most are BabyLockerKZ samples. We also discovered several other tools, which we’ll outline below.

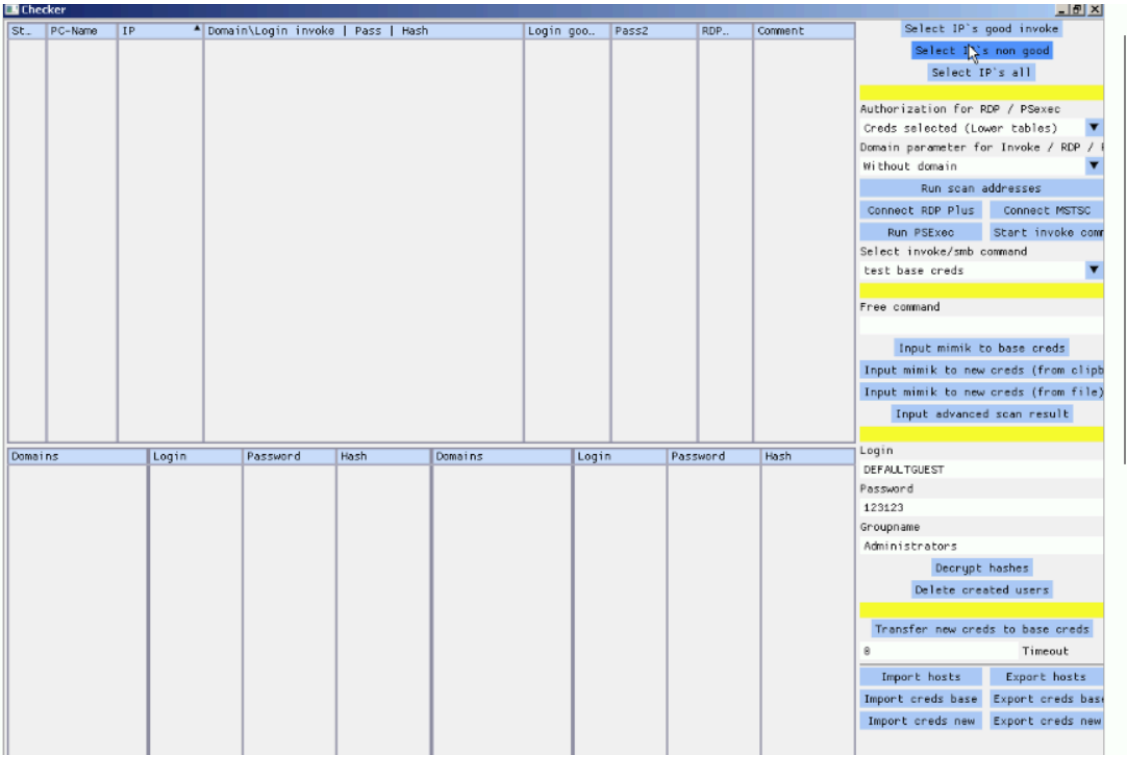
Checker tool

Checker (E:**paid_memes**\wmi_smb_rdp_checker\Release\checker.pdb) is an app that bundles several other freely available apps and provides a GUI for management of credentials as the attackers proceed with lateral movement. In particular it contains a set of tools:

- Remote Desktop Plus
- PSEXEC
- MIMIKATZ

And a set of scripts based on the Invoke-TheHash tool.

The tool also contains a GUI, as shown below, and a database to store the credentials.



As the image illustrates, the tool can be used to scan IPs for valid credentials using several protocols/techniques (PSEXEC, RDP, SMB and WMI) and is prepared to import data from lists of hosts and some of the tools in the attacker toolset, such as Mimikatz, as well as an advanced port scanner. The tool can also decrypt hashes and offers the convenience of a GUI to store a database of the hosts and respective credentials that have been obtained or verified.

PTH project

The PTH (D:\Projects**paid_memes**\PTH\Release\PTH.pdb) name suggests the pass-the-hash technique to use NTLM hashes to authenticate remotely without having to crack the password. Looking at its resources it embeds:

- Invoke-SMBClient.ps1
- Invoke-SMBEnum.ps1
- Invoke-SMBExec.ps1
- Invoke-TheHash.ps1
- Invoke-WMIExec.ps1

These were also used in the checker tool and are part of Invoke-TheHash. According to the author:

"Invoke-TheHash contains PowerShell functions for performing pass the hash WMI and SMB tasks. WMI and SMB connections are accessed through the .NET TCPClient. Authentication is performed by passing an NTLM hash into the NTLMv2 authentication protocol. Local administrator privilege is not required client-side."

MIMIK tool

MIMIK (D:\Projects**paid_memes**\mimik\Release\stub_mimik.pdb) is a wrapper around Mimikatz and rclone that can be used to steal credentials and automatically upload them to an attacker-controlled server. The following image shows the terminal output for the tool.

The following command lines are examples of commands executed via the tool:

- 64.exe privilege::debug sekurlsa::logonPasswords token::elevate lsadump::sam full exit
- C:\Users\user\Desktop\64.exe 64.exe "privilege::debug" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam full" exit
- 64.exe "privilege::debug" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam full" exit
- C:\Users\user\Desktop\rclone.exe rclone rcd --rc-no-auth --bwlimit=30M
- C:\Users\user\Desktop\rclone.exe rclone rc operations/stat

BabyLockerKZ

BabyLockerKZ is a variant of MedusaLocker that has been around at least since late 2023 and has been analyzed by other researchers, although not specifically called out as a MedusaLocker variant with this name.

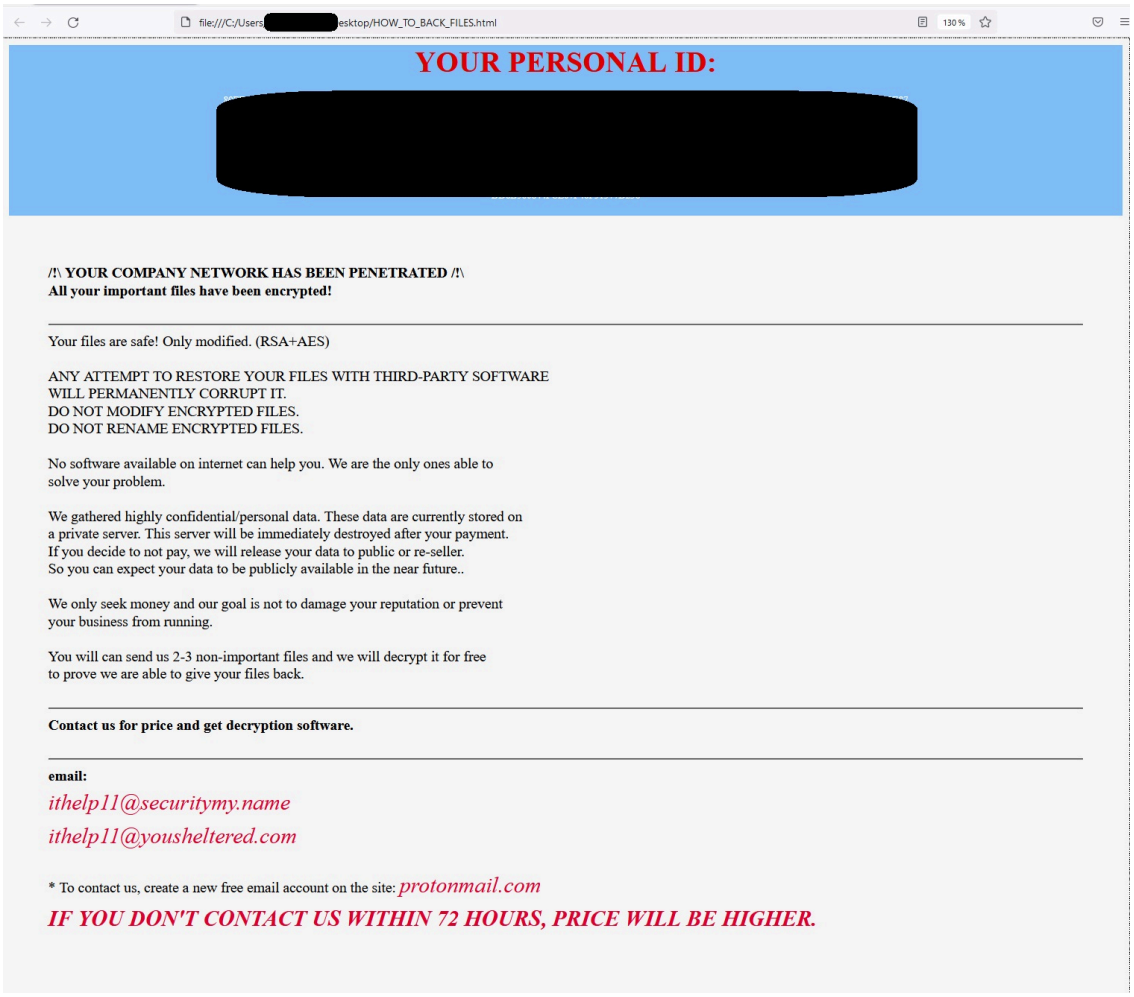
A Cynet blog post on the malware used the name “Hazard” for a MedusaLocker variant (named after the extension used for encrypted files) and mentions the existence of the BabyLockerKZ registry key.

Another post from Whitehat mentions the existence of PAIDMEMES PUBLIC and PRIVATE registry keys on a MedusaLocker sample.

This variant has not been given much attention outside of that, though, possibly because it’s highly similar to MedusaLocker or because it uses the same chat and leak sites as MedusaLocker. But there are several notable differences between BabyLockerKZ and MedusaLocker, such as:

- No {8761ABBD-7F85-42EE-B272-A76179687C63} mutex.
- No MDSLK reg key.
- The PAIDMEMES Public and private keys.
- The BabyLockerKZ run key.

The use of the PAIDMEMES public and private keys is unclear. In their post, Whitehat mentioned that they believe the keys aren’t necessary for the encryption process, as the Linux version doesn’t use them. Further research into the use of these keys might be a topic for another blog post.



Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	N/A	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
N/A	N/A	N/A	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this

threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. SIDs for this threat: Snort3 Rules: 1:300998:1:0 Snort2 Rules: 1:63928:1:0, 1:63929:1:0

ClamAV detections are also available for this threat:
Win.Ransomware.MedusaLocker-10035000-1
Win.Tool.PassTheHash-10034996-0
Win.Ransomware.MedusaLocker-10035000-0

Indicators of Compromise

IOCs for this research can be found at our Github repository here

BabylockerKZ:

33a8024395c56fab4564b9baef1645e505e00b0b36bff6fad3aedb666022599a

b8c994e3ed7dcc9080916119ddc315533c129479f508676d7544b82b2e24745f

63eb3d2886d9cb880c9b0d54b94f3e149b3b5b6215a33a0ef63588a09dcd4499

270c3354b3ee2940b499e365eaba143fba9d458f434dc38e663dc0f08e96121e

759b96f44806578cc0836a3a2bf11c8bc553effac72f8d28b94aec78b66be906

dc4840a0992b218cbedd5a7ac5c711cb98f1f9e78a8ffdea37c694061dfd34c6

48046fb0e566f5a2d184f84b76d6cadc458762556daed0ae4a3a1200afbefb54

c0c726a23111c220d022fcd01a85f9788249e42baece03f83b6059170453b801

012657c4548d9c98223caa4cc7aa52fc083d6983d42fde16ca3271412e7fe3fe

8edbb1944d94ff91ee917c31590b6d1d5690a52fc153e44355ee9749aa0f4625

364f1b7466d8e4c9f55294ecf1f874c763bcf980c59b0250c613ac366def6aca

5d5d639fdfbf632bb7d9f1bb28731217d09d36078ab5e594baf2a5a41267a5d2

PTH:

9f066975f1e02b29c7c635280f405c59704ce4f4e06b04e9ac8a7eac22acd3c7

8bc455e5de35290f8a94376357947bd72aaf6f4d452c25a8ef444e037ef76b9f

Checker:

d00f7cf6af68ba832b9d364f28411346cfe66fd3b1f5bcac318766add29ff7f0

1f2df15442593b159e45d16a27e4d43d3a9062da212a588ba4c048f214a0b7be

1e9246e6a35731143368eaa0ade4f3cf576d6b22e6090152f6e94f1fa3070651

6ae3a58a78be9c606009c657de4e390538b21ad951e62b6f4d31138e1a75732c

2eddfe711c32ef1668e14a10d00452c83c29e394e17c41f491550a1583c1bcac

PDB list:

d:/projects/paid_memes/virus/release/stub.pdb

e:/locker/bin/stub_win_x64_encrypter.pdb

i:/locker/bin/stub_win_x64_encrypter.pdb

d:/education/locker/bin/stub_win_x64_encrypter.pdb

d:/education/locker/bin/stub_win_x86_encrypter.pdb

d:/projects/paid_memes/wmi_smb_rdp_checker/release/checker.pdb

d:/projects/paid_memes/mimik/release/stub_mimik.pdb

i:/locker/x64/release/phantom.pdb

d:/projects/paid_memes/pth/release/pth.pdb

Registry keys:

HKEY_USERS\%SID%\SOFTWARE\PAIDMEMES\PRIVATE

HKEY_USERS\%SID%\SOFTWARE\PAIDMEMES\PUBLIC

HKEY_CURRENT_USER\SOFTWARE\PAIDMEMES\PUBLIC

HKEY_CURRENT_USER\SOFTWARE\PAIDMEMES\PRIVATE

HKCU\SOFTWARE\PAIDMEMES\PUBLIC

HKCU\SOFTWARE\PAIDMEMES\PRIVATE

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ

HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ

Extension names observed being used by BabyLockerKZ samples:

crypto125

crypto1317

crypto165

crypto41

crypto76

encrypted1

hazard11

hazard21

hazard23

hazard24

hazard25

hazard27

hazard31

hazard38

hazard49

hazard55

hazard56

hazard7

infected

lock2

lock3

lock5

locked9

lockfiles

meduza210

rapid1

rapid10

readtext13

readtext47

readtext49

recovery29

recovery70

virus2

virus3

virus57

Encryption key BabyLockerKZ:

PUTINHUILO1337

MUTEX BabyLockerKZ:

HOHOL1488
