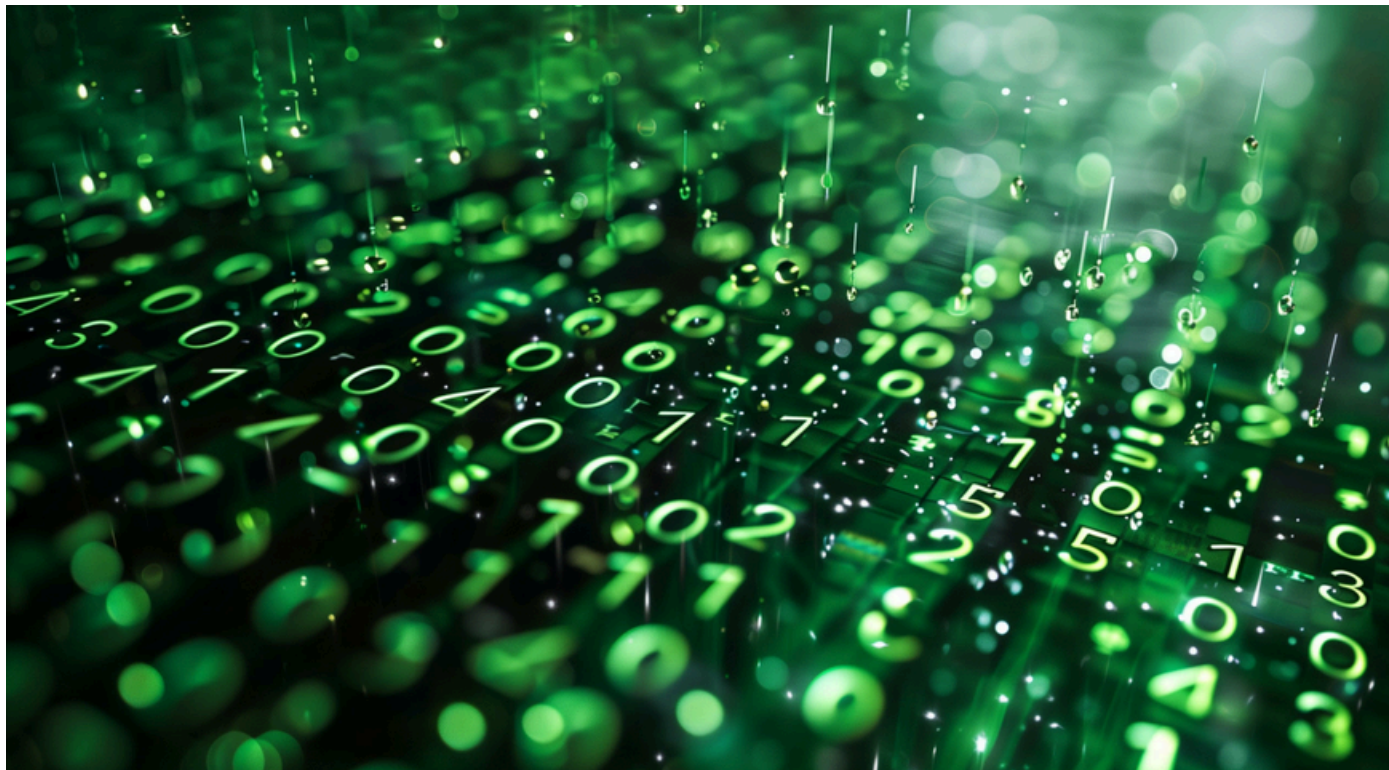


Makop ransomware: GuLoader and privilege escalation in attacks against Indian businesses

 acronis.com/en/tru/posts/makop-ransomware-guloader-and-privilege-escalation-in-attacks-against-indian-businesses



Other languages available: [Español](#) [Italiano](#)

Authors: Ilia Dafchev, Darrel Virtusio

Summary

Makop, a ransomware strain derived from [Phobos](#), continues to exploit exposed RDP systems while adding new components such as local privilege escalation exploits and loader malware to its traditional toolkit.

The attack typically begins with RDP exploitation, followed by the staging of network scanners, lateral movement tools and privilege escalation exploits, before moving to encryption or stopping if the attackers cannot bypass the security solution in place.

The attackers use a mix of off-the-shelf tools including network scanners, AV killers and numerous local privilege escalation exploits, along with deceptive file naming to avoid detection.

GuLoader, a downloader type of trojan, is used to deliver secondary payloads, indicating an evolution in Makop's methodology by integrating more techniques to bypass security measures and additional malware delivery mechanisms.

The majority of attacks (55%) target organizations in India, while incidents are also reported in Brazil, Germany and other regions.

Introduction

Makop is a ransomware strain first observed around 2020 and is generally treated as a variant of the Phobos family. Recently, Acronis TRU researchers identified new activity and tooling associated with Makop, prompting a deeper investigation into several recent ransomware cases to better understand how its operators conduct their attacks.

The pattern which emerged was that attackers prefer to work in a low complexity and low effort manner. Most victims were compromised through RDP and frequently after that attackers use off-the-shelf tools for discovery and lateral movement such as network scanners, local privilege escalation exploits (LPE) for privilege escalation, AV killers such as vulnerable drivers, process terminators, targeted uninstall software, credential access tools such as Mimikatz, and other steps from the kill chain.

What was interesting to see was their collection of local privilege escalation exploits and that on a few occasions we saw GuLoader being used. GuLoader is a loader type of malware that was first discovered in late 2019 and is known for delivering different types of second-stage malware. It is known to drop malware such as AgentTesla, FormBook, XLoader, Lokibot and more.

Makop's toolbox

The flow of Makop's attacks generally follows a familiar pattern. The ransomware operators gain initial access by exploiting publicly exposed and insecure remote desktop protocol (RDP) services. They commonly rely on brute-force or dictionary attacks to crack weak or reused credentials. Once inside, the attackers stage their tools for network scanning, privilege escalation, disabling security software, credential dumping, then ultimately deploying the encryptor.

Following the initial staging phase, attackers proceed with discovery, defense evasion, privilege escalation and lateral movement, although the steps do not always occur in a specific order. In some incidents, attackers quit after their tooling gets detected by the security solution. But sometimes they show an additional effort to bypass the security solution by using VMProtect packed samples of the same tools or disable the security solution, either by manually trying to uninstall it or by using hacking tools. If at this point they also fail, they then quit and leave the victim.

The observed execution chain used by Makop operators in their recent attacks is illustrated in the diagram below.

Makop's toolbox

Makop's tool is most frequently dropped either in network-mounted RDP shares (like "\\tsclient\\") or inside user's **Music** directory. Although in some cases attackers also used **Downloads**, **Desktop**, **Documents** directory or in the root of the **C:** drive. Frequently subfolders had names like "**Bug**" or "**Exp.**" The encryptor binary itself also typically uses one of the following filenames: **bug_osn.exe**, **bug_hand.exe**, **1bugbug.exe**, **bugbug.exe**, **taskmgr.exe**, **mc_osn.exe**, **mc_hand.exe** and variants of those prefixed with a dot (e.g. **".taskmgr.exe"**).

Initial access

Makop operators are known to exploit weak RDP credentials to gain access to victims' environment. RDP is a favored way by cybercriminals to compromise organizations because many of these organizations are still using weak credentials and are lacking multifactor authentication (MFA), making them susceptible to brute force attacks, one of the common tactics by ransomware groups.

During our investigation, we specifically spotted the use of NLBrute. It is an old hacking tool that was being sold on cybercrime forums way back in 2016. Not too long after its debut, a cracked version of NLBrute appeared which made it become widely used by cybercriminals.



NLBrute 1.2 automates large scale RDP password guessing to break into exposed systems using brute force techniques

NLBrute requires information such as a list of target IP addresses that have exposed RDP (often on the default port 3389, though this may be custom) alongside lists of known usernames and passwords to be used for brute force attacks like dictionary attacks or password spraying. Although RDP exploitation isn't the most sophisticated intrusion, it is still one of the most effective techniques that enable ransomware attacks. Once Makop operators successfully gain access through RDP, they can begin to laterally move through the organization's infrastructure and maximize its impact.

Network scanning and lateral movement

For discovery and lateral movement, multiple tools appeared in our telemetry. NetScan was used most often, with Advanced IP Scanner serving as an alternative in other cases.

-  Acronis
-  Acronis

Advanced IP Scanner scans local networks to identify active hosts and open services, helping attackers map targets for lateral movement.

Threat actors have combined these tools with Advanced Port Scanner and Masscan for port scanning tools. These tools are commonly used by the threat actors to enumerate network and infrastructure and locate high-value hosts and services to support lateral movement activities. It's not only that these tools are highly effective, but they can also blend in with legitimate admin activity.



Defense evasion

Several AV killers were spotted being used by the operators, including tools like Defender Control and Disable Defender to disable Windows Defender. Both tools are lightweight and effective tools for temporarily disabling Microsoft Defender features.



Defender Control



Defender Control 2.0 disables Microsoft Defender protections with a single action, giving attackers an easy way to neutralize built-in security

BYOVD techniques are also leveraged by using vulnerable drivers such as hlpdrv.sys and ThrottleStop.sys. ThrottleStop.sys is a legitimate, signed driver developed by TechPowerUp for the ThrottleStop application, a utility designed to monitor and correct CPU throttling issues. The ThrottleStop vulnerability (CVE-2025-7771) comes from the way the driver handles memory access. Attackers can exploit this to gain control, ultimately leading to disabling security tools.



ThrottleStop driver signed certificate

Another vulnerable driver is the hlpdrv.sys. This driver, when registered as a service, is known to gain kernel-level access and potentially terminate EDR solutions. Both drivers have been used on previous ransomware campaigns — specifically by MedusaLocker, [Akira](#) and Qilin.

We also discovered that the threat actors deployed a tailored uninstall software to remove Quick Heal AV. Quick Heal AV is an antivirus and endpoint-security product from Quick Heal Technologies (India) that provides malware protection for its both consumer and enterprise customers.



Quick Heal AV uninstaller

The use of a tailored Quick Heal AV uninstaller aligns with our telemetry data showing that victims were predominantly located in India. This targeted removal indicates that the attackers adapted parts of their toolkit depending on the target victim's region.

Lastly, they also abused applications such as Process Hacker and IOBitUnlocker. Both applications are legitimate but are abused by threat actors to easily terminate processes and delete programs.



Process Hacker provides attackers with a powerful interface to terminate processes, tamper with services and manipulate running applications

Privilege escalation

Multiple local privilege escalation (LPE) vulnerabilities spanning from older disclosures to the latest have been exploited.

[CVE-2016-0099](#)

[CVE-2017-0213](#)

[CVE-2018-8639](#)

[CVE-2019-1388](#)

[CVE-2020-0787](#)

[CVE-2020-0796](#)

[CVE-2020-1066](#)

[CVE-2021-41379](#)

[CVE-2022-24521](#)

The vulnerabilities abused in these cases exploit Windows components, such as BITS, Win32k, KS/SMB drivers, Windows installers, vendor IOCTL, etc. Makop operators used these specific vulnerabilities as they all focused on targeting the same platform, many have publicly available PoCs that make weaponization straightforward, and they reliably grant system privileges which exactly what ransomware needs to maximize its impact. The range of exploited CVEs also shows the group keeps multiple LPE primitives in its toolkit to fall back on if one fails. In our telemetry, the vulnerabilities CVE-2017-0213, CVE-2018-8639, CVE-2021-41379 and CVE-2016-0099 were among the most frequently used by the attackers, indicating that these vulnerabilities are reliable and effective in the attacks.

Credential access

Attackers use credential dumpers and brute force tools to gather sensitive data. They rely on tools such as Mimikatz, LaZagne and NetPass to extract saved passwords, cached credentials and authentication tokens. They also use brute force utilities like CrackAccount and AccountRestore to break into additional accounts. The stolen credentials enable lateral movement and give the attackers access to more systems within the victim's infrastructure, which increases the impact of the ransomware. Many ransomware groups follow the same pattern, which highlights how effective these tools are for achieving the attackers' objectives.

Among the credential dumping tools, Mimikatz is the most widely used. This post-exploitation tool extracts credentials directly from Windows' memory, including plaintext passwords, NTLM hashes, Kerberos tickets and other sensitive information managed by the Local Security Authority (LSA).



Mimikatz extracts plaintext passwords, hashes and authentication tokens directly from Windows memory to support credential theft during intrusions

Meanwhile, LaZagne complements Mimikatz by focusing on locally stored credentials across applications. This open-source tool supports browsers, Wi-Fi profiles, email clients, databases and Windows credential stores.



LaZagne collects locally stored credentials to expand an attacker's access

Network password recovery (NetPass) targets network-related credentials, recovering passwords for mapped drives, VPN connections, remote desktop sessions and other Windows networking features. This allows attackers to gain quick access to passwords saved by the operating system.



NetPass recovers saved network passwords, enabling quick access to additional systems

Lastly, other brute force tools like AccountRestore work differently compared to the credential dumpers mentioned above. These tools test multiple password combinations to gain access to accounts.



AccountRestore 0.1b automates brute force attempts against user accounts

GuLoader

In addition to the tools mentioned above, there were instances where GuLoader was dropped in the same directory as other tools and used to deliver additional payloads. The use of loaders to deploy ransomware encryptors is a common tactic among ransomware groups. Ransomware

groups such as [Qilin](#), [Ransomhub](#), [BlackBasta](#) and [Rhysida](#) have leveraged loaders in previous campaigns, **but this appears to be the first documented case of Makop being distributed via a loader.**

Once GuLoader has been successfully installed in the system, it will now be able to deploy its payloads.

File path

Command line

Description

%USERPROFILE%\Music\1\BUG\TreasureRoberts.exe

“%USERPROFILE%\Music\1\BUG\TreasureRoberts.exe”

Execution of GuLoader, drops a VBS script to install the malware.

%WINDIR%\System32\WScript.exe

“%USERPROFILE%\Music\1\BUG\67138435cf99c.vbs”

Installation of GuLoader

%USERPROFILE%\Music\1\BUG\mc_fxt.exe

Makop ransomware

%USERPROFILE%\Music\1\BUG\mc_n1tro.exe

Makop ransomware

%USERPROFILE%\Music\1\BUG\mc_p1z.exe

Makop ransomware

Victim countries

The largest share of attacked organizations (55% of all Makop attacks) was located in India, with smaller numbers in Brazil and Germany and isolated incidents across other countries. This distribution doesn't necessarily mean that Makop targets a specific country more than others but could be the result of more businesses with lower security posture. Makop's operators appear to act opportunistically, focusing on networks where weaknesses reduce the effort needed for initial entry, subsequent compromise and encryption.

Conclusion

Makop ransomware campaigns underline the threat posed by attackers who exploit well-known vulnerabilities and weak security practices. By leveraging exposed RDP systems together with an array of off-the-shelf tools, from network scanners to local privilege escalation exploits, the adversaries demonstrate a low effort yet highly effective approach. The integration of techniques, such as using GuLoader for secondary payload delivery and tailoring tactics based on target regions, further emphasizes the need for organizations to adopt robust security measures, including strong authentication and regular patch management.

Overall, seemingly mundane entry points like unsecured RDP can lead to significant breaches. Organizations across the globe, particularly those with known security gaps, should continuously reassess and fortify their defenses against ransomware and other cyberthreats.

Detection by Acronis

This threat has been detected and blocked by Acronis EDR / XDR:



Indicators of Compromise

Makop ransomware

[8ccb30606e3229ff88b3b67a5f4b2b087cab290ce7eedfcb24d1d3954b01d5f9](#)

[f43b86ff363f19f26cc7d80aa64fa0894a264a736ae0abd013d98e344637e4d8](#)

[0e3c6b3366640989979ae059b768586ff1d8ba4c4b96b49b40609cdaa871363c](#)

Local privilege escalation (LPE) exploits

CVE-2016-0099

- o [10ea5ac09ec72101c6f8656f3f08f6f9495f8b43849f27928efd6485cee04913](#)
- o [6752d24da3565761c94ab10d3010e1be702221783f9b509209f97a8e32003767](#)

CVE-2017-0213

- o [aac0c5ad612fb9a0ac3b4bbfd71b8931fc762f8e11fdf3ffb33ef22076f9c4bc](#)
- o [0a4a0f0df5eea57f16a76bff6489dd95a7089afba8e9e5c8bcadc46870af33fb](#)
- o [a903f4d8f126a830b8f12e05c035b86e4dfd65cb1fd64d0d0b503035b49d0cb7](#)
- o [6cf6dd6119abcb2751c2692fb93a623b5b4bd290cb3dc217fa9fe09dd721fcdd](#)
- o [7470ae5b55ca282695d2f7c4896344622c94292a915aa63e55000beeb2c1350e](#)

CVE-2018-8639

- o [ca08299002fa6181d249115907ee29356e698d72ff06afdca05431c1ed38db35](#)
- o [fb1dd40577af7ac4d8c32506e78e39841ff6d05ee643c18270ef26eac798df3f](#)

CVE-2019-1388

- o Legitimate HHUPD:

[0745633619afd654735ea99f32721e3865d8132917f30e292e3f9273977dc021](#)

CVE-2020-0787

- o [5b9407df404506219bd672a33440783c5c214eefa7feb9923c6f9fded8183610](#)

CVE-2020-0796

- o [c7e471218b00cdec4f7845a80f1c5b069ee97bf270f878ea45b2dd53aad14798](#)

CVE-2020-1066

- o [0d468fa92767ca1abe881155224d94879b575860e403636d3dbb550e9b9a6a7a](#)
- o [5994db4362ded8bf15f81f134e14b9ed581cd2e073709b5fae6b2363bae455e9](#)
- o [7470ae5b55ca282695d2f7c4896344622c94292a915aa63e55000beeb2c1350e](#)

CVE-2021-41379

- o [f181b8ae88f6c657c3ec3d1d5e8420fbf340c543b3d9292947ae035e3591b664](#)

CVE-2022-24521

- o [43c3b5dbc18ebbc55c127d197255446d5f3e074fdac37f3e901b718acbe7c833](#)

AV Killers and Hacking Tools

dfControl

- o [20c730c7033b5bdc0a6510825e90449ba8f87942d2d7f61fa1ba5f100e98c141](#)
- o [1ef6c1a4dfdc39b63bfe650ca81ab89510de6c0d3d7c608ac5be80033e559326](#)

disable-defender.exe

- o [feb09cc39b1520d228e9e9274500b8c229016d6fc8018a2bf19aa9d3601492c5](#)

Hlpdrv.sys

- o [bd1f381e5a3db22e88776b7873d4d2835e9a1ec620571d2b1da0c58f81c84a56](#)

0th3r_av5.exe

- o [5b7b280b53ff3cf95ead4fd4a435cd28294c5fce6a924ec52e500a109deb868b](#)
- o [16f83f056177c4ec24c7e99d01ca9d9d6713bd0497eedb777a3ffefa99c97f0](#)

4avr64 – QuickHeal Uninstaller

- o [5caacdc577c27110f639d4d7c0241607c1bc53ee6f5dbd337793d05cc57e703f](#)
- o [41a328c3bb66e94d73e861699a5ebc4a5c0c7fcee2129e5ecd98c7bde1f95e8e](#)

Proc.exe – ProcessHacker

- o [bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4](#)

IOBitUnlocker

- o [eea9dc1c9dc8620549fee54d81399488292349d2c8767b58b7d0396564fb43e7](#)
- o [37d2a1626dc205d60f0bec8746ab256569267e4ef2f8f84dff4d9d792aa3af30](#)
- o [1845fe8545b6708e64250b8807f26d095f1875cc1f6159b24c2d0589feb74f0c](#)

Credential dumping and brute force tools

NLBrute (RDP brute-force tool)

- o [ffa28db79daca3b93a283ce2a6ff24791956a768cb5fc791c075b638416b51f4](#)
- o [a332f863da1709b27b62f3a3f2a06dca48c7dabe6b8db76ec7bb81ce3786e527](#)

Lazagne

- o [3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05](#)

Mimikatz

- o [61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1](#)
- o [8c57b97b04d7eabbae651c3400a5e6b897aea1ae8964507389340c44b99c523a](#)

Miparser

- o [a8bf7da7e2f62296985e1aadbac8373f5ac813ac158047f5b5579a3f900fd85b](#)

System.exe (ruadmin.exe)

- o [3fa65f17518d10af9ed316fbd0395bf39b3b75a63a5374ff071cbba4b642e4a3](#)

CrackAccount

- o [6e95adda5f24fdf805ad10ae70069484def3d47419db5503f2c44b130eedf591](#)
- o [e97bdf7fafb1cb2a2bf0a4e14f51e18a34f3ff2f6f7b99731e93070d50801bef](#)

Account Restore

- o [76f88afe7a18e3583bfcc4aed3b3a0ca8a9c18c62ee5f4d746f8da735c47a5e3](#)
- o [3902165d0645afdb4b7d95f5cc55d65ecee17d3b77a31d51170e0beae3fd296a](#)
- o [b044c6dbd55747c3592ac527215c3dbf71f92aa4bd8eee5e29ddad571b9335b4](#)
- o [4c6cf8dda0c55fafab37569d2e11621c42e17f37a290b13087215190f7518d73](#)

LoginParser

- o [10c0dd2878bd0ab9732cd593febf61d94bb2b798bf0aa1c8fa45ddf8c7092cbc](#)

Netpass

- o [17fb52476016677db5a93505c4a1c356984bc1f6a4456870f920ac90a7846180](#)
- o [51fd557a7325dd58cfcabebbbc33ef452d93f812c189360d4f2bf87c6df0a59c](#)

Network scanning tools

NetScan

- o [c7d994eb2042633172bd8866c9f163be531444ce3126d5f340edd25cbdb473d4](#)
- o [f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446](#)

- o [dd748db20e3909596ab18ce3f0b1264e2cfe9f67dfb4bce7d4f9c085ec1fce0a](#)
- o [92c65b58c4925534c2ce78e54b0e11ecaf45ed8cf0344ebff46cdfc4f2fe0d84](#)
- o [3da3b704547f6f4a1497107e78856d434a408306b92ba7c6e270c7c9790aa576](#)

Advanced Port Scanner

- o [a1a6005cc3eb66063ae33f769fc2d335487b2ed7f92c161e49ad013ffed11ec8](#)
- o [8b9c7d2554fe315199fae656448dc193accbec162d4aff3f204ce2346507a8a](#)

Advanced IP Scanner

- o [be2b45b7df8e7dea6fb6e72d776f41c50686c2c9cfbaf4d456bcc268f10ab083](#)
- o [722fff8f38197d1449df500ae31a95bb34a6ddaba56834b13eaaff2b0f9f1c8b](#)
- o [26d5748ffe6bd95e3fee6ce184d388a1a681006dc23a0f08d53c083c593c193b](#)
- o [4b036cc9930bb42454172f888b8fde1087797fc0c9d31ab546748bd2496bd3e5](#)
- o [f20721945a0a4150470e63bc81c9316cbb5802a60615ae4393283273a62cf8a2](#)

Masscan

- o [de903a297afc249bb7d68fef6c885a4c945d740a487fe3e9144a8499a7094131](#)
- o [37ff328175acd45ef27d3d339c3127a7612ad713fccd9c9aae01656dfbf13056](#)

Other tools / samples

GuLoader - MUI

- o [8f7569e82bd339f3e24431884687b095f678971f20053787d93359672bb9f687](#)
- o [5cdabf41672241798bcc94a7fdb25974ba5ab2289ebadc982149b3014677ae3](#)
- o [b5c2474397fb38a4dd9edab78b6e5178832074ba5bab9bac3f0cad7bc0660cf2](#)
- o [5ff803269d6491dd3f0267f6f07b8869e3f08d62cf2110b552bba2cc3d75d26a](#)

GuLoader - VBS

- o [c8afb68260b9036d8e65811927c379112274a2526cc161c7f1502457a501a0d3](#)
- o [01f34180bb635022681723eef73c19adf330d7a32a2e6639c27b1ee5777312be](#)

- o [c8e8cca4ee3c4f4ce4f2076ed93cca058fa1ff88d5ffe49d8d293b27ad25ef68](#)
- o [8315327f22eff069457c02ddda1ea32a31964e1b8ab688709bcb96c6ccbb6212](#)