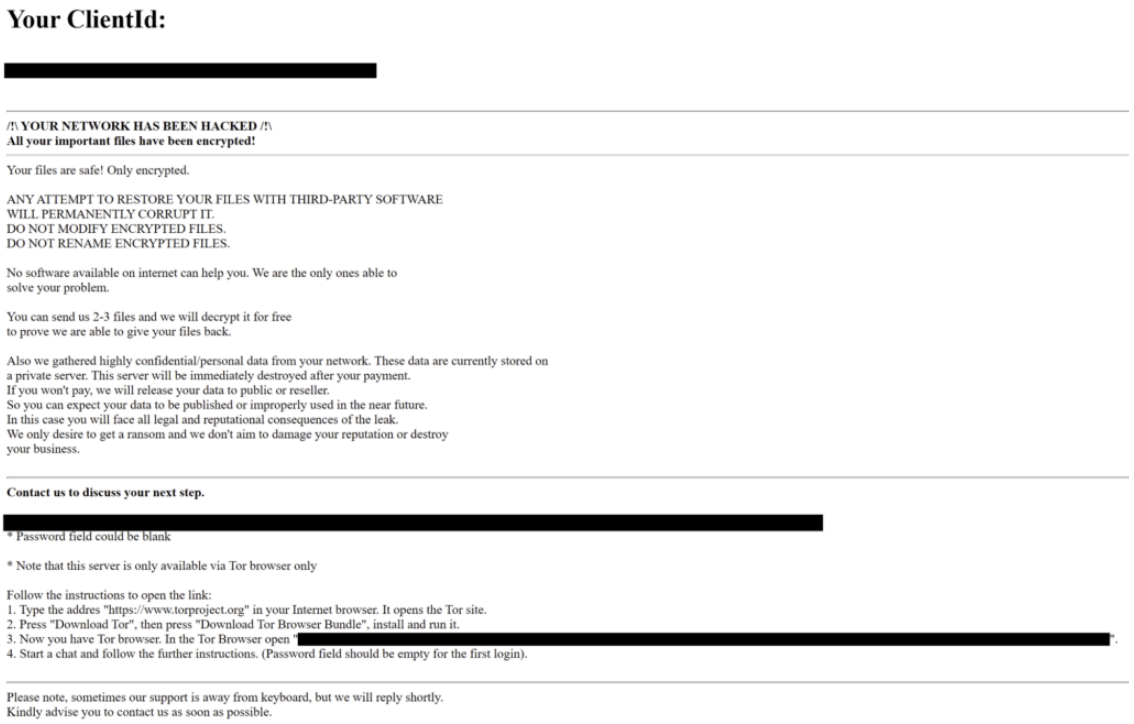
Mount Locker Ransomware Steps up Counter-IR Capabilities, Hindering Efforts for Detection, Response and Investigation

By GuidePoint Security

Published: 2021-04-22 · Archived: 2026-04-06 01:32:39 UTC

3 min read

Over the past six weeks, GuidePoint Security threat researchers have noted a change in the tactics used by Mount Locker ransomware seen in recent engagements.



Your ClientId:

[redacted]

/!\ YOUR NETWORK HAS BEEN HACKED /!
All your important files have been encrypted!

Your files are safe! Only encrypted.

ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE
WILL PERMANENTLY CORRUPT IT.
DO NOT MODIFY ENCRYPTED FILES.
DO NOT RENAME ENCRYPTED FILES.

No software available on internet can help you. We are the only ones able to
solve your problem.

You can send us 2-3 files and we will decrypt it for free
to prove we are able to give your files back.

Also we gathered highly confidential/personal data from your network. These data are currently stored on
a private server. This server will be immediately destroyed after your payment.
If you won't pay, we will release your data to public or reseller.
So you can expect your data to be published or improperly used in the near future.
In this case you will face all legal and reputational consequences of the leak.
We only desire to get a ransom and we don't aim to damage your reputation or destroy
your business.

Contact us to discuss your next step.

[redacted]
* Password field could be blank

* Note that this server is only available via Tor browser only

Follow the instructions to open the link:
1. Type the addres "https://www.torproject.org" in your Internet browser. It opens the Tor site.
2. Press "Download Tor", then press "Download Tor Browser Bundle", install and run it.
3. Now you have Tor browser. In the Tor Browser open "[redacted]".
4. Start a chat and follow the further instructions. (Password field should be empty for the first login).

Please note, sometimes our support is away from keyboard, but we will reply shortly.
Kindly advise you to contact us as soon as possible.

Mount Locker group first announced their ransomware-as-a-service offering in the second half of 2020, and attacks attributed to the variant have been on the rise since. In early November 2020, an update was released broadening the types of files targeted and improving the ransomware's ability to evade security measures. It also appears that Mount Locker may be transitioning to Astro Locker, as the verbiage and victims listed on both variants' shaming sites share significant overlap. While it's not too uncommon for malware to change names, this change is paired with an aggressive shift in Mount Locker's tactics.

Traditionally, Mount Locker ransomware is known for using public tools to move laterally, steal files, and deploy encryption. Attackers deploying Mount Locker use its capabilities for double extortion of victims. Initial access vectors vary, but once a foothold is gained common tactics include the use of AdFind and Bloodhound for Active Directory and user reconnaissance, FTP for file exfiltration, and Cobalt Strike for lateral movement and the delivery and execution of encryption, potentially through psExec. Critical data is staged and exfiltrated to be used as further collateral in extorting ransoms, with threats to release the data if the ransom is not paid. After the

environment is mapped, backup systems are identified and neutralized, and data is harvested, systems are encrypted with target-specific ransomware delivered via the established C2 channels. These payloads include executables, extensions, and unique victim IDs for payment.

However, in recent engagements, it appears Mount Locker is stepping up their game by including scripting and capabilities directly targeting prevention measures. The new batch scripts – designed to disable detection & prevention tools – indicate that Mount Locker is increasing its capabilities and is becoming a more dangerous threat. These scripts were not just blanket steps to disable a large swath of tools, they were customized and targeted to the victim's environment. In recent engagements threat actors have also begun using multiple Cobalt Strike servers with unique domains, which is an added step not often seen due to the increased overhead in management for attackers. This, combined with the recent shift to AstroLocker, could signal a shift in the group's overall tactics and an effort to fully rebrand as a more insidious threat.

This shift in TTPs has coincided with a recent surge in requests for assistance coming from companies in the biotech industry. Some calls were proactive, seeking help in verifying that environments were secure, however, a number were seeking help with active ransomware incidents. Viewed together, this could be an indication of a larger campaign aggressively targeting healthcare-adjacent industries.

Biotech companies, in particular, are a prime target for ransomware because of their position in an industry flush not only with cash but also with highly sensitive IP. Additionally, connections to other research organizations increase the potential to damage the victim's reputation in the industry and put business dealings at risk. Healthcare and biotech companies are prime targets for attack groups because their services and technologies are in increasing demand. They stand to lose the most if operations are halted for too long or critical IP is lost, so attackers view them as more likely to pay the requested ransom quickly.

If you believe you may be at risk of an attack using Mount Locker or Astro Locker, telltale signs include the staging and exfiltration of files via FTP and Cobalt Strike stagers and beacons in your environment. While these would always be cause for alarm, the November 2020 release of an updated, more aggressive Mount Locker and the dramatic increase in attacks attributable to the group make these IOCs particularly alarming.

If you observe any activity in your environment that could indicate you are being targeted, you can reach out to GuidePoint Security's Digital Forensics & Incident Response team here.
