

# Evil Corp demands \$40 million in new Macaw ransomware attacks

---

[bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/](https://bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/)

Lawrence Abrams

By

[Lawrence Abrams](#)

- October 21, 2021
- 03:07 PM
- 0



Evil Corp has launched a new ransomware called Macaw Locker to evade US sanctions that prevent victims from making ransom payments.

The Evil Corp hacking group, also known Indrik Spider and the Dridex gang, has been involved in cybercrime activities since 2007, but mostly as affiliates to other organizations.

Over time, the group began focusing on their own attacks by creating and distributing a banking trojan known as Dridex in phishing attacks.

## Moving to ransomware

---

As ransomware attacks became increasingly more profitable, Evil Corp launched an operation called BitPaymer, delivered via the Dridex malware to compromised corporate networks.

The hacking group's criminal activity ultimately led them to be sanctioned by the US government in 2019.

Due to these sanctions, ransomware negotiation firms will no longer facilitate ransom payments for operations attributed to Evil Corp.

To bypass US sanctions, Evil Corp began creating limited use ransomware operations under various names such as WastedLocker, Hades, Phenoix Locker, and PayloadBin.

Evil Corp began renaming their ransomware operations to different names such as WastedLocker, Hades, Phoenix CryptoLocker, and PayLoadBin.

Other ransomware families that are believed but not proven to be affiliated with Evil Corp is DoppelPaymer, which was recently rebranded as Grief.

## Introducing Macaw Locker

---

This month, Olympus and Sinclair Broadcast Group had their operations severely disrupted by weekend ransomware attacks.

For Sinclair, it caused TV broadcasts to be cancelled, different shows to air, and newscasters to report their stories with whiteboards and paper.

Still dealing with technical difficulties at @CBS6Albany .... Our 11pm newscast (which is starting late after football) will be unconventional. We're working with handwritten notes, and it's going to be a bit more conversational. Tune in, and thanks for bearing with us! pic.twitter.com/D620UCD72F

— Leanne DeRosa (@CBS6Leanne) October 18, 2021

This week, it was discovered that both attacks were conducted by a new ransomware known as Macaw Locker.

In a conversation with Emsisoft CTO Fabian Wosar, BleepingComputer was told that, based on code analysis, MacawLocker is the latest rebrand of Evil Corp's ransomware family.

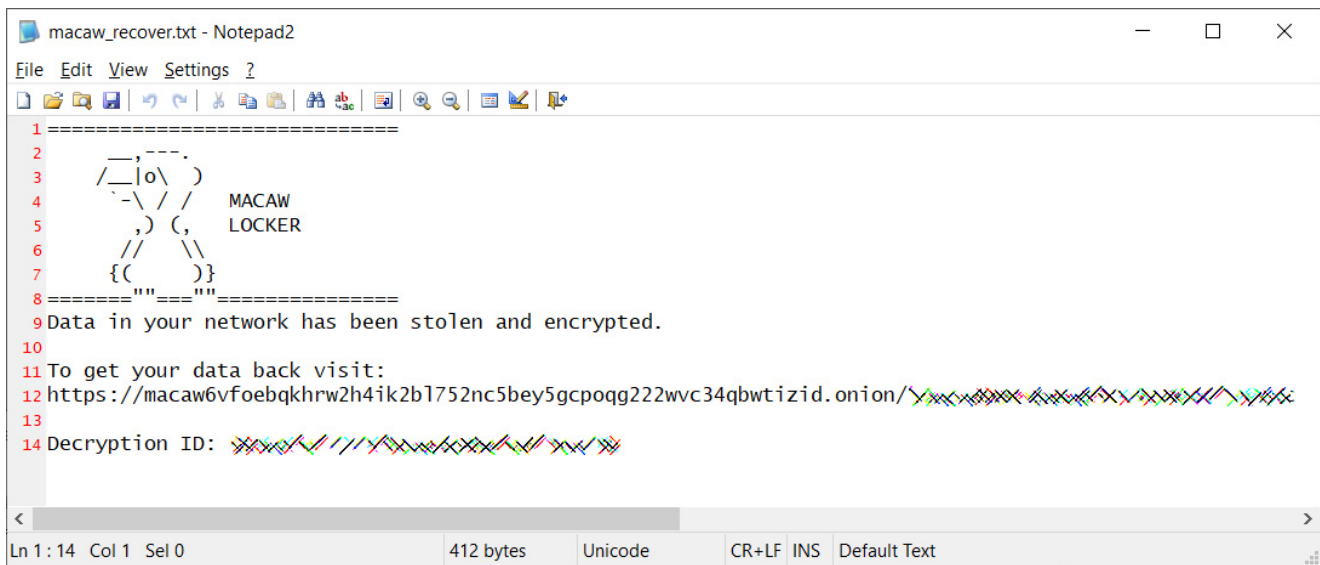
BleepingComputer has also learned from sources in the cybersecurity industry that the only two known Macaw Locker victims are Sinclair and Olympus.

Sources also shared the private Macaw Locker victim pages for two attacks, where the threat actors demand a 450 bitcoin ransom, or \$28 million, for one attack and \$40 million for the other victim.

It is unknown what company is associated with each ransom demand.

The Macaw Locker ransomware will encrypt victims' files and append the **.macaw** extension to the file name when conducting attacks.

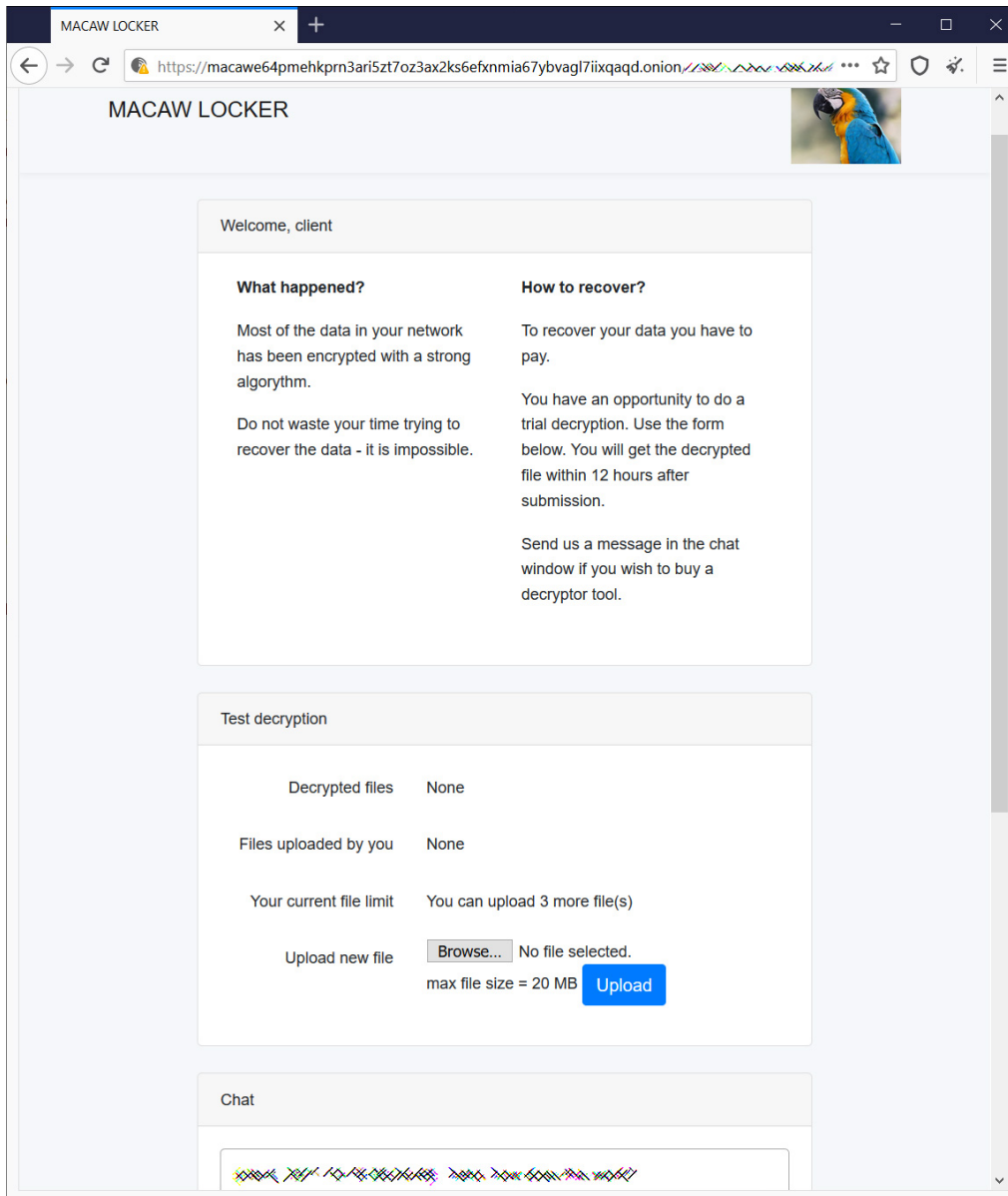
While encrypting files, the ransomware will also create ransom notes in each folder named **macaw\_recover.txt**. For each attack, the ransom note contains a unique victim negotiation page on the Macaw Locker's Tor site and an associated decryption ID, or campaign ID, as shown below.



```
macaw_recover.txt - Notepad2
File Edit View Settings ?
=====
1
2
3  /_ |o\ )
4  - \ / ( MACAW
5  , ) ( , LOCKER
6  // \ \
7  {( ) }
8  =====
9 Data in your network has been stolen and encrypted.
10
11 To get your data back visit:
12 https://macaw6vfoebqkhrw2h4ik2b1752nc5bey5gcpoqg222wvc34qbwtizid.onion/
13
14 Decryption ID: 
```

### Macaw Locker ransom note

The gang's dark web negotiation site contains a brief introduction to what happened to the victim, a tool to decrypt three files for free, and a chatbox to negotiate with the attackers.



Macaw Locker Tor

### payment negotiation site

Now that Macaw Locker has been exposed as an Evil Corp variant, we will likely see the threat actors rebrand their ransomware again.

This constant cat-and-mouse game will likely never end until Evil Corp stops performing ransomware attacks or sanctions are lifted.

However, neither of those scenarios is likely to take place in the immediate future.

### Related Articles:

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[SpiceJet airline passengers stranded after ransomware attack](#)

[US Senate: Govt's ransomware fight hindered by limited reporting](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.