Ragnar Locker Ransomware: Unlocked by Deep Instinct

By Deep Instinct Threat Lab

Published: 2020-04-27 · Archived: 2026-04-05 22:40:27 UTC

On April 14th the news broke that, Portuguese multinational energy giant Energias de Portugal (EDP) was hit by ransomware attacking the network of the company's 11,500 employees. The attack was by Ragnar Locker ransomware, which upon encrypting the systems demanded a 1,580 Bitcoin ransom fee, the equivalent to around $11 million. In their ransom note, the attackers claim to have stolen 10TB of sensitive company files which will be leaked if the ransom isn't paid. According to security analysts, the methodology of the attack and the ransom demand both indicate the attack was well thought out with the attacker fully aware of its victim's financial capabilities.

Ragnar Locker is often delivered through MSPs tools such as ConnectWise, from which the attackers drop a highly targeted ransomware executable. This is a technique that has been used by other highly malicious ransomware campaigns, most notably, Sodinokibi. In this type of attack, the operators of the ransomware initially infiltrate organizations through unsecured or badly secured RDP connections and then used both tools to push Powershell scripts to all accessible endpoints. The scripts then downloaded a payload from Pastebin, which executes the ransomware and encrypts the endpoints. In some cases, the payload is an executable file that is executed as part of a file-based attack, in other cases additional scripts were downloaded, as part of a completely file-less attack.

Ragnar Locker is specifically targeting software commonly used by managed service providers, Below, is the list of targeted strings:

- vss
- sql
- memtas
- mepocs
- sophos
- veeam
- backup
- pulseway
- logme
- logmein
- connectwise
- splashtop
- kaseya

Attackers first steal a victim's files and upload it to their servers. They then tell the victim that they will only release the files publicly if a ransom is not paid, in a tactic that has recently been dubbed - the 'Name & Shame Game'.

Ragnar Locker ransomware undermines the MSP's security tools (as mentioned above, before the tools can block it from executing) and once inside, commences the encryption process. It contains a specific extension to use for encrypted files, an embedded RSA-2048 key.

The ransomware appends a new file extension, such as '.ragnar_22015ABC' to the file's name. The 'RAGNAR' file marker will also be added to the end of every encrypted file.

Ragnar Locker will drop a ransom note named '.RGNR_[extension].txt.' The ransom note contains information on the ransom amount, a bitcoin payment address, a TOX chat ID to communicate with the cybercriminals, and a backup email address if TOX does not work. In each case, the ransom amount is calculated individually.

```
****************************************************************************************************************************************

 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED

                                        by RAGNAR_LOCKER !

****************************************************************************************************************************************

                                        !!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT use any third party or public decryption software, it also may damage files.
DO NOT Shutdown or reset your system
-----------------------------------

There is ONLY ONE possible way to get back your files - contact us and pay for our special decryption key !
For your GUARANTEE we will decrypt 2 of your files FOR FREE, as a proof of our capabilities

Don't waste your TIME, the link for contacting us will be deleted if there is no contact made in closest future
and you will never restore your DATA.
HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

ATTENTION !
We had downloaded more than 10TB of data from your fileservers and if you don't contact us for payment, we will
publish it or sell to interested parties.
Here is just a small part of your files that we have, for a proof (use Tor Browser for open the link) :
[redacted]

We gathered the most sensitive and confidential information about your transactions, billing, contracts,
clients and partners. And be assure that if you wouldn't pay,
all files and documents would be publicated for everyones view and also we would notify all your clients and
partners about this leakage with direct links.
So if you want to avoid such a harm for your reputation, better pay the amount that we asking for.

============================================================================================================
! HERE IS THE SIMPLE MANUAL HOW TO GET CONTACT WITH US VIA LIVE CHAT !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

a) Download and install TOR browser from this site : https://torproject.org
b) For contact us via LIVE CHAT open our website :
[redacted]
c) For visit our NEWS PORTAL with your data, open this website [redacted]
d) If Tor is restricted in your area, use VPN

When you open LIVE CHAT website follow rules :

Follow the instructions on the website.
At the top you will find CHAT tab.
Send your message there and wait for response (we are not online 24/7, So you have to wait for your turn).
```

Amongst our customer environments, Deep Instinct found seven samples of this ransomware, and all were prevented statically with Deep Instinct's current model in production. The previous model which was trained in Q3 of 2019 was also able to successfully detect and prevent the ransomware. This is a considerable feat considering that RagnarLocker went undetected by most other engines when it was first spotted in the wild. In the days following detection rates by other engines gradually improved.

Not only could Deep Instinct **prevent** Ragnar Locker statically prior to execution, our solution was also able to label it as a ransomware attack. This classification was achievable due to our product's enhanced

The implication of this is that without ever having been trained to identify this specific form of ransomware before, both of our engines (the pre-execution and on-execution engines) could prevent this attack the first time that it appeared in the wild.

The IOC hashes associated with the malware:

b670441066ff868d06c682e5167b9dbc85b5323f3acfbbc044cabc0e5a594186

68eb2d2d7866775d6bf106a914281491d23769a9eda88fc078328150b8432bb3

9bdd7f965d1c67396afb0a84c78b4d12118ff377db7efdca4a1340933120f376

dd5d4cf9422b6e4514d49a3ec542cffb682be8a24079010cda689afbb44ac0f4

c2bd70495630ed8279de0713a010e5e55f3da29323b59ef71401b12942ba52f6

63096f288f49b25d50f4aea52dc1fc00871b3927fa2a81fa0b0d752b261a3059

a8ee0fafbd7b84417c0fb31709b2d9c25b2b8a16381b36756ca94609e2a6fcf6

5fc6f4cfb0d11e99c439a13b6c247ec3202a9a343df63576ce9f31cffcdbaf76

1472f5f559f90988f886d515f6d6c52e5d30283141ee2f13f92f7e1f7e6b8e9e

ec35c76ad2c8192f09c02eca1f263b406163470ca8438d054db7adcf5bfc0597

Source: https://www.deepinstinct.com/2020/04/27/ragnar-locker-ransomware-unlocked-by-deep-instinct/