Ragnar Locker ransomware - what you need to know | Tripwire

By Graham Cluley

Published: 2022-03-10 · Archived: 2026-04-05 21:14:35 UTC

What is this Ragnar Locker thing I've heard about?

Ragnar Locker is a family of ransomware, which first came to prominence in early 2020 when it became notorious for hitting large organisations, attempting to extort large amounts of cryptocurrency from its victims.

So just your bunch of cybercriminals then?

Yes, although on their underground website, where they leak files stolen from their corporate victims, they attempt to portray themselves rather differently.

In the Ragnar Locker gang's "About us" section they make the rather unconvincing claim that they "don't pursuit aim to make huge damage to anyone's business", whilst admitting that "if it would be necessary, no doubt we will do what we promise and the consequences will be disastrous."

The criminals even attempt to convince their victims that they can help improve security:

> "We are interesting in finding weaknesses and vulnerabilities in networks and we are good at this, we can help to improve the security measures, that's why we give a chance to make a deal and providing list of recommendations and penetrations reports." "Companies under attack of Ragnar_Locker can count it as a bug hunting reward, we are just illustrating what can happens. But don't forget there are a lot of peoples in internet who don't want money - someone might want only to crash and destroy. So better pay to us and we will help you to avoid such issues in future."

Hmm. It sounds like they're making an offer you can't refuse…

Yes, the words may seem kindly but there's no disguising the implicit threat that if you don't pay the ransom after they exploit your network, things could get very nasty indeed.

Because your data will be encrypted, and could be leaked online?

Precisely. The FBI is clearly concerned, and has issued an alert warning that the Ragnar Locker gang has infected at least 52 critical infrastructure organisations across America with its ransomware.

Systems have been hit in the critical manufacturing, energy, financial services, government, and information technology sectors, says the FBI.

It's bad enough for any company to get hit, but critical infrastructure…

Right.

And that's why the FBI's alert is raising awareness of the Ragnar Locker ransomware threat and offering information about how it works, indicators of compromise, and tips on how to better secure your business.

Is it just a problem facing North American businesses?

No, Ragnar Locker can be used against organisations around the world, although interestingly the ransomware terminates if it identifies that a computer identified as "Azerbaijani," "Armenian," "Belorussian,", "Kazakh," "Kyrgyz," "Moldavian," "Tajik," "Russian," "Turkmen," "Uzbek," "Ukrainian," or "Georgian."

Might that indicate what part of the world the ransomware originates from?

You might think that, I couldn't possibly comment. But it is generally believed that some cybercriminal gangs deliberately avoid hitting companies in their own country, in the hope of avoiding unwanted interest from local law enforcement agencies.

Gotcha. So when the Ragnar Locker ransomware triggers - what does it encrypt?

What's perhaps quicker to describe is what it *doesn't* encrypt. In order to allow the computer to operate "normally" during the encryption process, it avoids encrypting files in the following folders on the C: drive:

- Windows
- Windows.old
- Mozilla
- Mozilla Firefox
- Tor browser
- Internet Explorer
- $Recycle.Bin
- Program Data
- Google
- Opera
- Opera Software

In addition, when cycling through files, Ragnar Locker ignores files with the following extensions:

- .db
- .sys
- .dll
- .lnk
- .msi
- .drv
- .exe

Of course, these are all filetypes that can normally be easily replaced - unlike data files which normally carry greater value.

But to encrypt files it needs to have found its way into your organisation somehow. How does it do that?

The Ragnar Locker gang is like many other cybercriminal groups targeting businesses with ransomware - taking advantage of internet-exposed services such as RDP, brute-forcing passwords or using stolen credentials. Once in, an attacker will attempt to gain greater privileges and move laterally throughout the network.

So how can my company protect itself from Ragnar Locker?

The best advice is to follow the recommendations on how to protect your organisation from other ransomware. Those include:

- making secure offsite backups.
- running up-to-date security solutions and ensuring that your computers are protected with the latest security patches against vulnerabilities.
- using hard-to-crack unique passwords to protect sensitive data and accounts, as well as enabling multi-factor authentication.
- encrypting sensitive data wherever possible.
- reducing the attack surface by disabling functionality which your company does not need.
- educating and informing staff about the risks and methods used by cybercriminals to launch attacks and steal data.

If my company has fallen victim to Ragnar Locker, should we pay the ransom?

That's a decision that only your company can make. What is clear is that the more companies that pay a ransom, the more likely it is that criminals will launch similar attacks against others in the future.

At the same time, your business may feel it has no choice but to make the hard decision to pay. After all, the alternative may put the entire business at risk.

Whatever your decision, you should inform law enforcement agencies of the incident and work with them to help them investigate who might be behind the attacks.

And remember this: paying the ransom does not necessarily mean you have erased the security problems that allowed you to be infected in the first place. If you don't find out what went wrong – and why – and fix it, then you could easily fall victim to further ransomware attacks in the future.

Editor's Note: *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*
