

New Royal Ransomware emerges in multi-million dollar attacks

bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/

Lawrence Abrams

By

[Lawrence Abrams](#)

- September 29, 2022
- 10:32 AM
- [0](#)



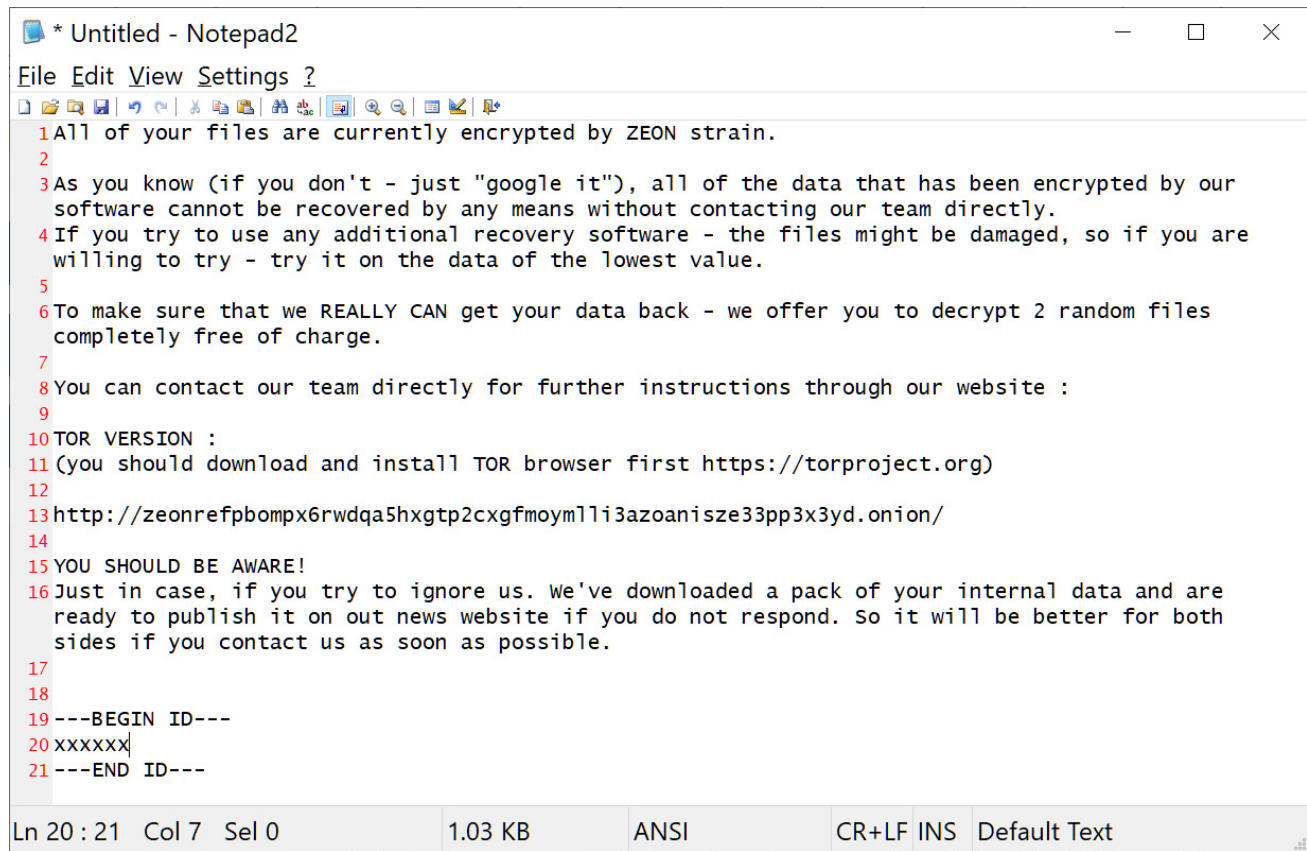
A ransomware operation named Royal is quickly ramping up, targeting corporations with ransom demands ranging from \$250,000 to over \$2 million.

Royal is an operation that launched in January 2022 and consists of a group of vetted and experienced ransomware actors from previous operations.

Unlike most active ransomware operations, Royal does not operate as a Ransomware-as-a-Service but is instead a private group without affiliates.

Vitali Kremez, CEO of [AdvIntel](#), told BleepingComputer that they utilized other ransomware operation's encryptors when first starting, such as BlackCat.

Soon after, the cybercrime enterprise began using its own encryptors, the first being Zeon [[Sample](#)], which generated ransom notes very similar to Conti's.



```
* Untitled - Notepad2
File Edit View Settings ?
1 All of your files are currently encrypted by ZEON strain.
2
3 As you know (if you don't - just "google it"), all of the data that has been encrypted by our
  software cannot be recovered by any means without contacting our team directly.
4 If you try to use any additional recovery software - the files might be damaged, so if you are
  willing to try - try it on the data of the lowest value.
5
6 To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files
  completely free of charge.
7
8 You can contact our team directly for further instructions through our website :
9
10 TOR VERSION :
11 (you should download and install TOR browser first https://torproject.org)
12
13 http://zeonrefpbomp6rwdqa5hxgtp2cxgfmoyml1i3azoanisze33pp3x3yd.onion/
14
15 YOU SHOULD BE AWARE!
16 Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are
  ready to publish it on our news website if you do not respond. So it will be better for both
  sides if you contact us as soon as possible.
17
18
19 ---BEGIN ID---
20 xxxxxx
21 ---END ID---
```

Zeon ransom note

Source: *BleepingComputer*

However, since the middle of September 2022, the ransomware gang has rebranded again to 'Royal' and is using that name in ransom notes generated by a new encryptor.

How Royal breaches their victims

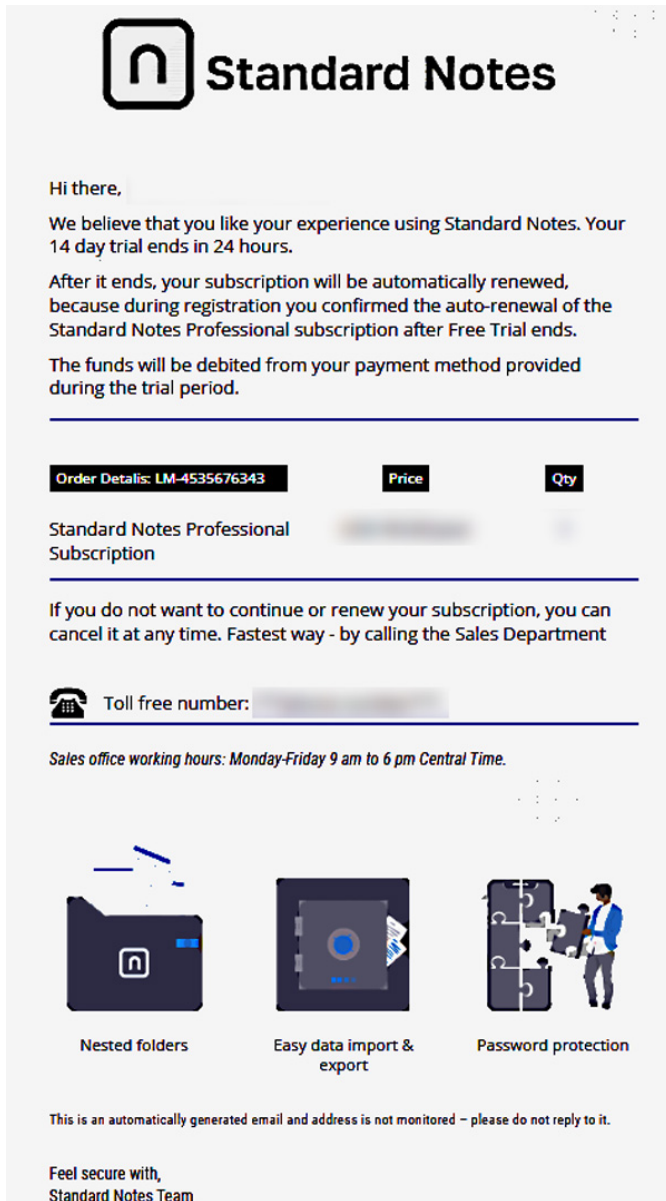
The Royal operation has been operating in the shadows, not using a data leak site and keeping news of their attacks quiet.

However, as the gang became more active this month, victims have appeared at [BleepingComputer](#), and a sample was uploaded to [VirusTotal](#).

In conversations with Kremez and a victim, BleepingComputer has created a better picture of how the gang operates.

According to Kremez, the Royal group utilizes targeted callback phishing attacks where they impersonate food delivery and software providers in emails pretending to be subscription renewals.

These phishing emails contain phone numbers that the victim can contact to cancel the alleged subscription, but, in reality, it is a number to a service hired by the threat actors.



Example of a Royal callback phishing

email

Source: AdvIntel

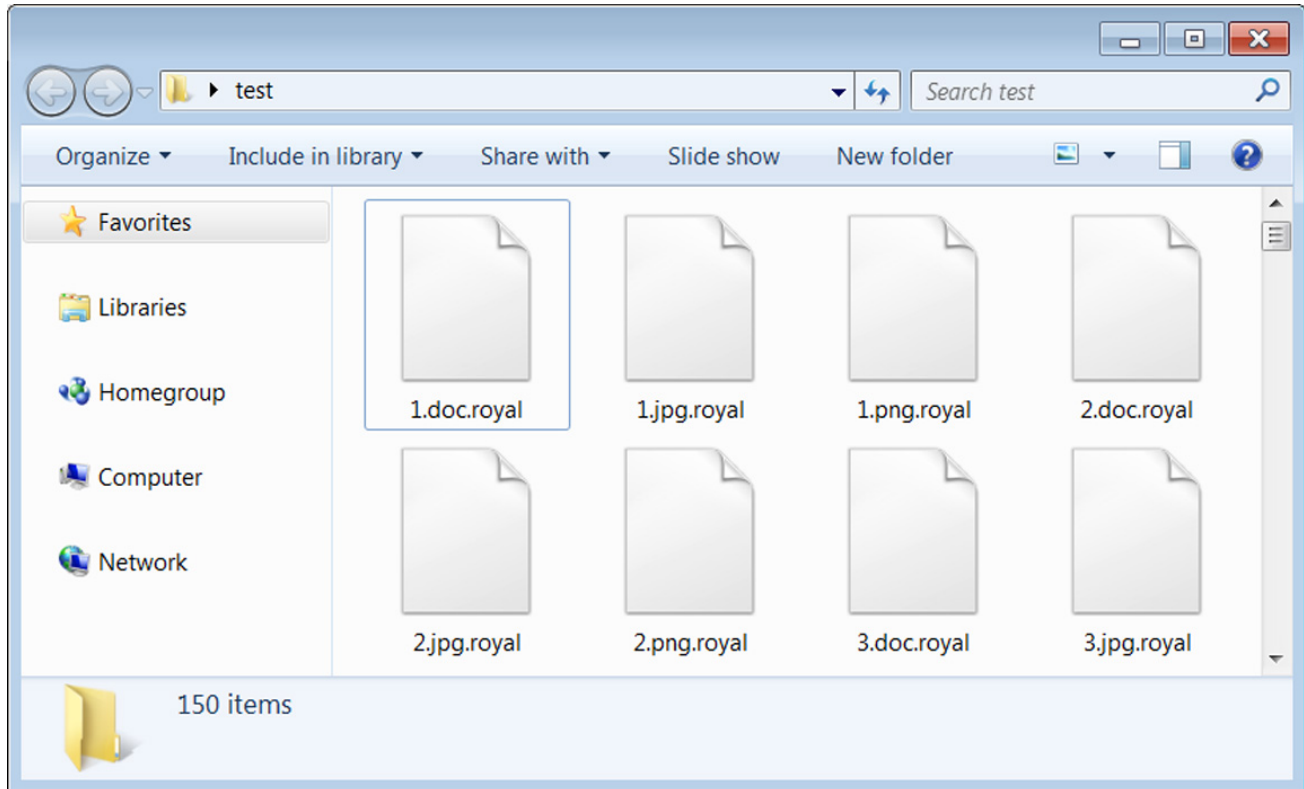
When a victim calls the number, the threat actors use social engineering to convince the victim to install remote access software, which is used to gain initial access to the corporate network.

A Royal victim who spoke to BleepingComputer shared that the threat actors breached their network using a vulnerability in their custom web application, showing the threat actors are also being creative in how they gain access to a network.

Once they gain access to a network, they perform the same activities commonly used by other human-operated ransomware operations. They deploy Cobalt Strike for persistence, harvest credentials, spread laterally through the Windows domain, steal data, and ultimately

encrypt devices.

When encrypting files, the Royal encryptor will append the **.royal** extension to the file names of encrypted files. For example, test.jpg would be encrypted and renamed to test.jpg.royal, as shown below.



Files encrypted by the Royal Ransomware

Source: *BleepingComputer*

A Royal victim also told BleepingComputer that they target virtual machines by directly encrypting their virtual disk files (VMDK). The threat actors then print out the ransom notes on network printers or create them on encrypted Windows devices.

These ransom notes are named **README.TXT** and contain a link to the victim's private Tor negotiation page at royal2xthig3ou5hd7zsliaqgy6yygk2cdelaxtni2fyad6dpmpxedid.onion. XXX in the ransom note below has been redacted but is unique to the victim.

```
1 Hello!
2
3 If you are reading this, it means that your system were hit by Royal ransomware.
4 Please contact us via :
5 http://royal2xthig3ou5hd7zs1iqagy6yygk2cde1axtni2fyad6dpmplexidid.onion/xxx
6
7 In the meantime, let us explain this case. It may seem complicated, but it is not!
8 Most likely what happened was that you decided to save some money on your security infrastructure.
9 Alas, as a result your critical data was not only encrypted but also copied from your systems on a
  secure server.
10 From there it can be published online. Then anyone on the internet from darknet criminals, ACLU
  journalists, Chinese government (different names for the same thing),
11 and even your employees will be able to see your internal documentation: personal data, HR reviews,
  internal lawsuits and complains, financial reports, accounting, intellectual property, and more!
12
13 Fortunately we got you covered!
14
15 Royal offers you a unique deal. For a modest royalty (got it; got it ? ) for our pentesting services we
  will not only provide you with an amazing risk mitigation service,
16 covering you from reputational, legal, financial, regulatory, and insurance risks, but will also
  provide you with a security review for your systems.
17 To put it simply, your files will be decrypted, your data restored and kept confidential, and your
  systems will remain secure.
18
19 Try Royal today and enter the new era of data security!
20 We are looking to hearing from you soon!
```

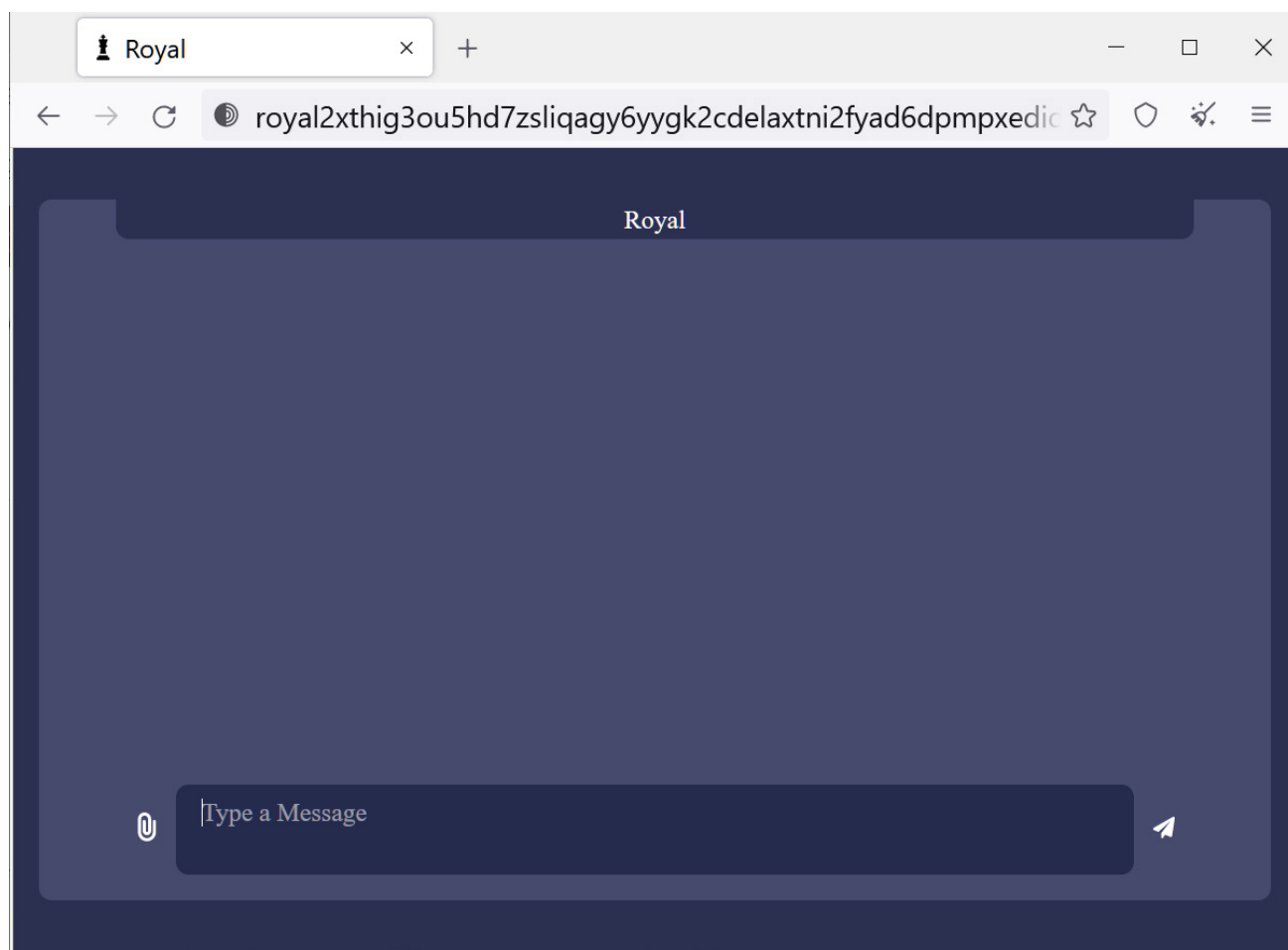
Royal ransom note

Source: *BleepingComputer*

The Tor negotiation site is nothing special, simply containing a chat screen where a victim can communicate with the Royal ransomware operators.

As part of these negotiations, the ransomware gang will provide the ransom demand, with ransom demands between \$250,000 and over \$2 million.

The ransomware gang will also commonly decrypt a few files for the victims to prove their decryptor works and share file lists of the stolen data.



Royal Ransomware Tor negotiation site

Source: BleepingComputer

BleepingComputer is unaware of successful payments and has not seen a decryptor for this ransomware family.

While the group claims to steal data for double-extortion attacks, it does not appear that a data leak site has been launched under the Royal brand as of yet.

However, it is strongly advised that network, windows, and security admins keep an eye out for this group, as they are quickly ramping up operations and will likely become one of the more significant enterprise-targeting ransomware operations.

Update 8/29/22: Article updated with some corrections, including launch date and callback phishing example.

Related Articles:

[Medibank now says hackers accessed all its customers' personal data](#)

[TommyLeaks and SchoolBoys: Two sides of the same ransomware gang](#)

[BlackByte ransomware uses new data theft tool for double-extortion](#)

The Week in Ransomware - September 30th 2022 - Emerging from the Shadows

Hackers breach energy orgs via bugs in discontinued web server

- [CallBack](#)
- [Data Exfiltration](#)
- [Exploit](#)
- [Ransomware](#)
- [Royal Group](#)
- [Zeon](#)

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.

- [Previous Article](#)
- [Next Article](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
