# New Royal Ransomware emerges in multi-million dollar attacks

By Lawrence Abrams

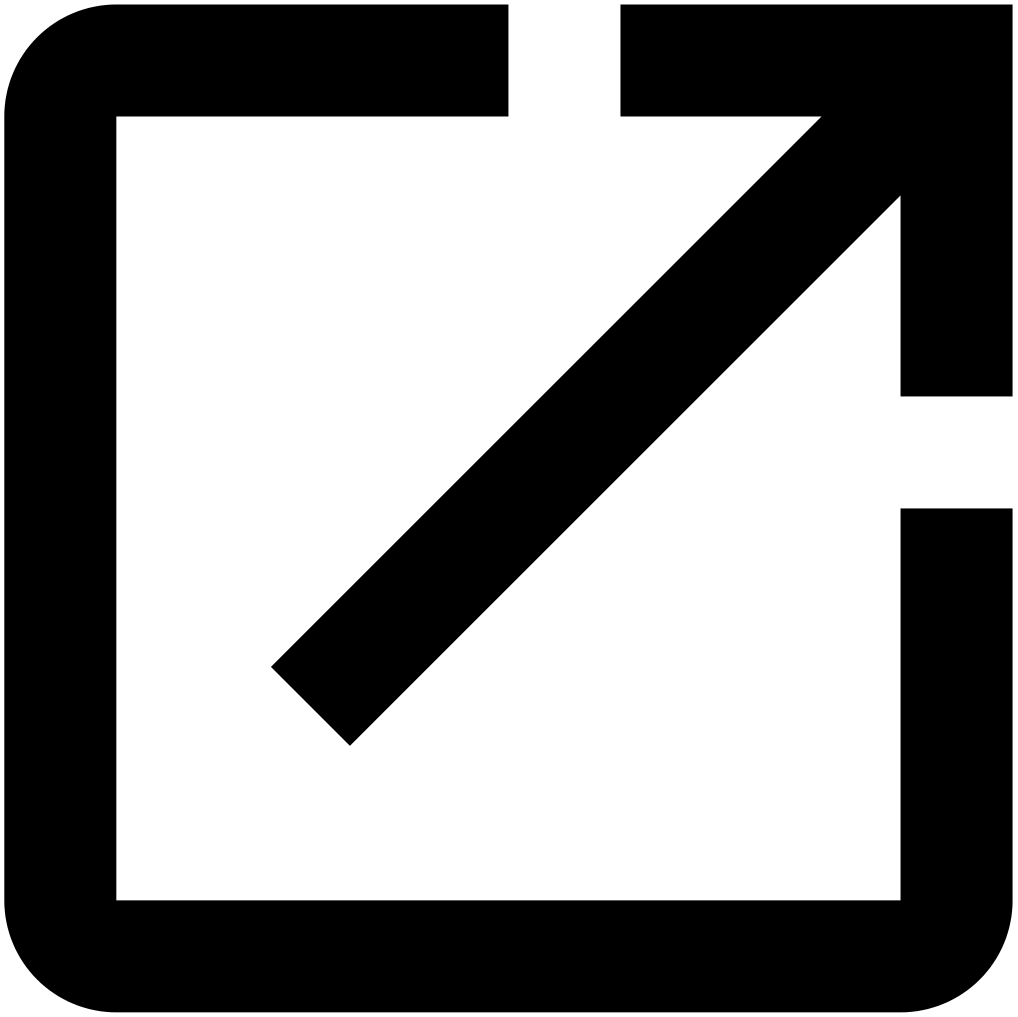
Published: 2022-09-29 · Archived: 2026-04-05 14:26:31 UTC

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.

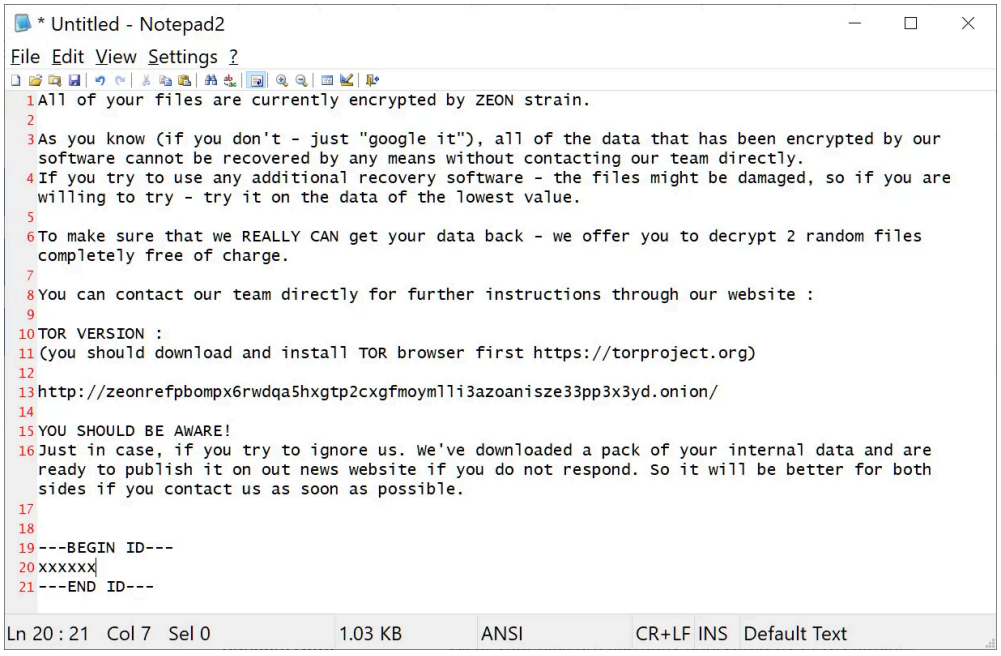
Unlike most active ransomware operations, Royal does not operate as a Ransomware-as-a-Service but is instead a private group without affiliates.


DIE LINKE.
0:00



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.




**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

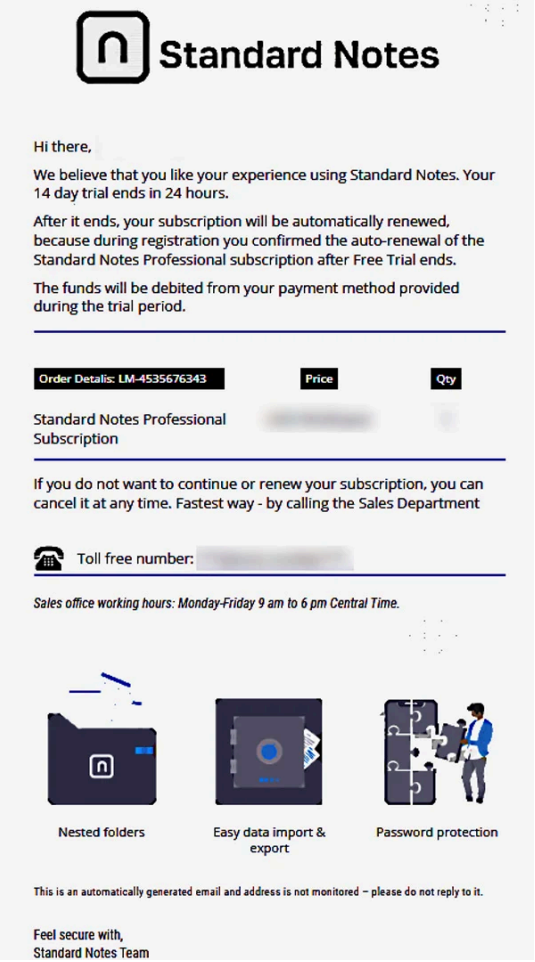
The Royal operation has been operating in the shadows, not using a data leak site and keeping news of their attacks quiet.

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**

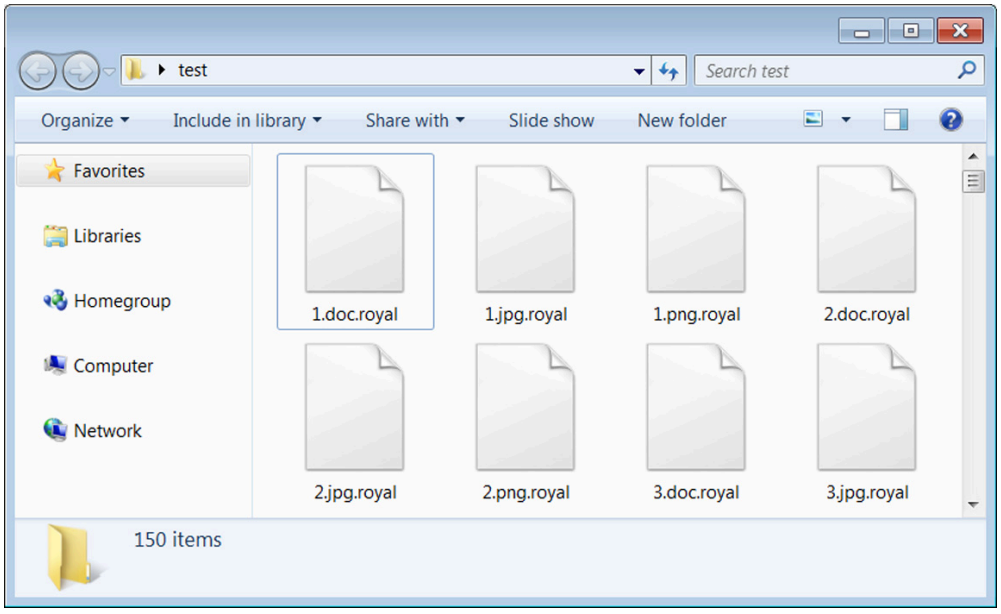
*Source: AdvIntel*

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.

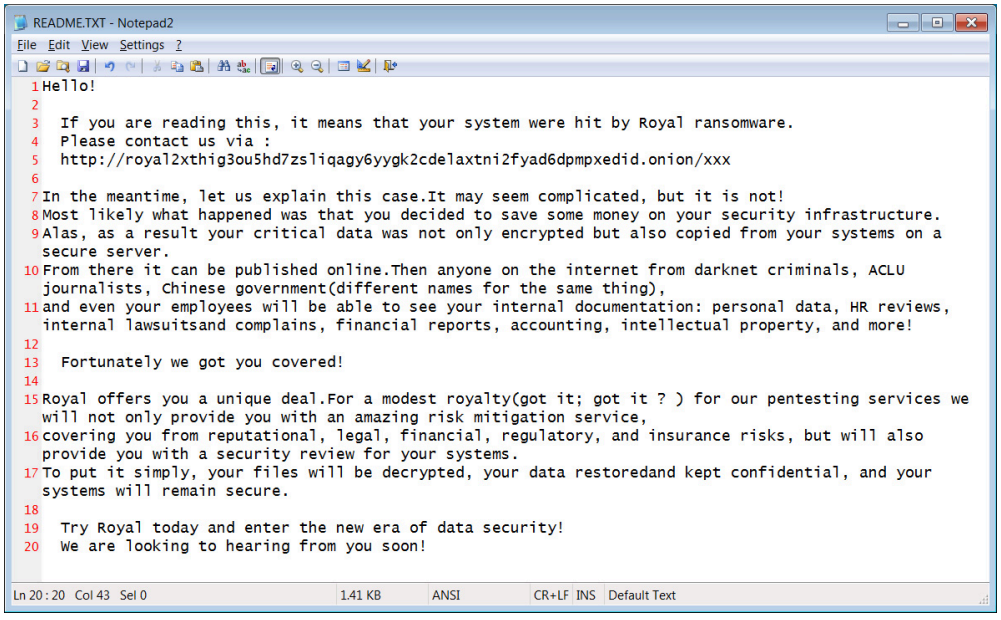



**Files encrypted by the Royal Ransomware**

*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 royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion. XXX in the ransom note below has been redacted but is unique to the victim.



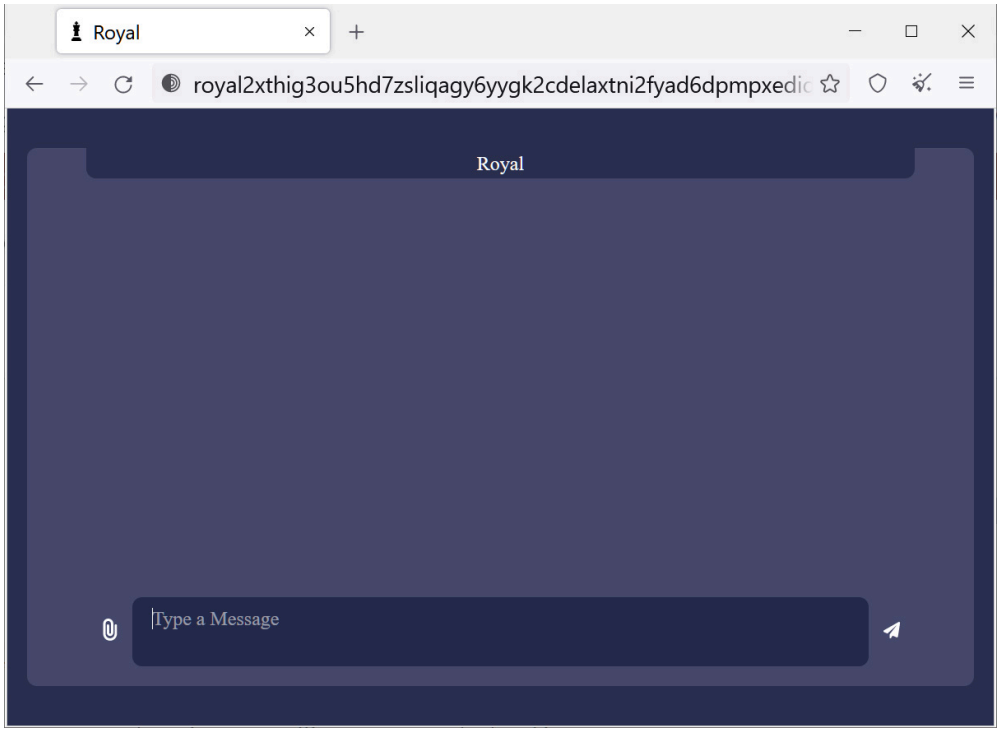

**Royal ransom note**

*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.*

---

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