HC3: Analyst Note
December 07, 2022 TLP:CLEAR Report: 202212071400

Royal Ransomware

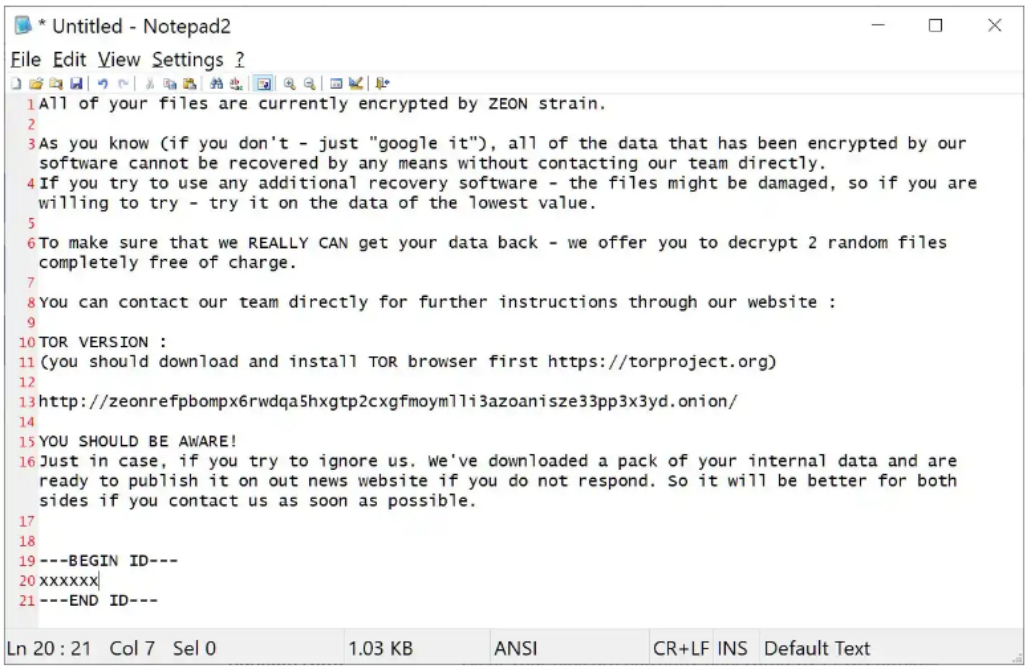
Executive Summary

Royal is a human-operated ransomware that was first observed in 2022 and has increased in appearance. It has demanded ransoms up to millions of dollars. Since its appearance, HC3 is aware of attacks against the Healthcare and Public Healthcare (HPH) sector. Due to the historical nature of ransomware victimizing the healthcare community, Royal should be considered a threat to the HPH sector.

Report

Royal ransomware was first observed in September 2022. Once infected, the requested demand for payment has been seen to range anywhere from $250,000 U.S. Dollars (USD) to over $2 million USD. Royal is an operation that appears to consist of experienced actors from other groups, as there have been observed elements from previous ransomware operations. While most of the known ransomware operators have performed Ransomware-as-a-Service, Royal appears to be a private group without any affiliates while maintaining financial motivation as their goal. The group does claim to steal data for double-extortion attacks, where they will also exfiltrate sensitive data.

Once a network has been compromised, they will perform activities commonly seen from other operations, including deploying Cobalt Strike for persistence, harvesting credentials, and moving laterally through a system until they ultimately encrypt the files. Originally, the ransomware operation used BlackCat's encryptor, but eventually started using Zeon, which generated a ransomware note that was identified as being similar to Conti's. The ransom notes appear in a README.TXT, which also contains a link to the victim's private negotiation page. This note was later changed to Royal in September 2022.



Zeon ransom note

Source: BleepingComputer

HC3: Analyst Note
December 07, 2022 TLP:CLEAR Report: 202212071400

The Royal ransomware is a 64-bit executable that is written in C++ and targets window systems. The ransomware works to delete all Volume Shadow Copies, which provides a point-in-time copy of a file. With these, you can quickly recover deleted or changed files stored on a network. It will encrypt the network shares that are found on the local network and the local drives. The files are encrypted with the AES algorithm, with the key and IV being encrypted in the RSA public key, which is hard coded into the executable. The malware can either fully or partially encrypt a file based on its size and the '-ep' parameter. Once the files are encrypted, it will change the extension of the files to '.royal'.

Multiple actors have been spreading Royal ransomware, but in a report from Microsoft, it is also being distributed from DEV-0569. The group has been delivering the malware with human-operated attacks and has displayed innovation in their methods by using new techniques, evasion tactics, and post-compromise payloads. The group has been observed embedding malicious links in malvertising, phishing emails, fake forums, and blog comments. In addition, Microsoft researchers have identified changes in their delivery method to start using malvertising in Google ads, utilizing an organization's contact forum that can bypass email protections, and placing malicious installer files on legitimate looking software sites and repositories.

Analyst Comment

Royal is a newer ransomware, and less is known about the malware and operators than others. Additionally, on previous Royal compromises that have impacted the HPH sector, they have primarily appeared to be focused on organizations in the United States. In each of these events, the threat actor has claimed to have published 100% of the data that was allegedly extracted from the victim.

Outside of the techniques addressed in this report, HC3 continues to see the following attack vectors frequently associated with ransomware:

- Phishing
- Remote Desktop Protocol (RDP) compromises and credential abuse
- Compromises of exploilted vulnerabilities, such as VPN servers
- Compromises in other known vulnerabilities

The following sources contain indicators of compromise:

- https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware
- https://securityscorecard.pathfactory.com/research/the-royal-ransomware
- https://blog.polyswarm.io/royal-ransomware

References

Abrams, Lawrence. "New Royal Ransomware emerges in multi-million dollar attacks". Bleepingcomputer. Sep 29, 2022. https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/

Polyswarm Tech Team. "Royal Ransomware". Polyswarm. Dec 1, 2022. https://blog.polyswarm.io/royal-ransomware

Greig, Jonathan. "Microsoft: Royal ransomware group using Google Ads in campaign". Therecord. Nov 18,

2022. https://therecord.media/microsoft-royal-ransomware-group-using-google-ads-in-campaign/

Pasca, Vlad. "A Technical Analysis of Royal Ransomware". Securityscorecard. https://securityscorecard.pathfactory.com/research/the-royal-ransomware

Microsoft Security Threat Intelligence. "DEV-0569 finds new ways to deliver Royal ransomware, various payloads". Microsoft. Nov 17, 2022. https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

Imano, Shunichi. Slaughter, James. "Ransomware Roundup: Royal Ransomware". Fortinet. Oct 12, 2022. https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback