Ransomware Roundup: Royal Ransomware

fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware

October 13, 2022

On a bi-weekly basis, FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

This latest edition of the Ransomware Roundup covers Royal ransomware.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows Users
Impact: Encrypts files on the compromised machine and demands ransom for file decryption
Severity level: High

Royal Ransomware

Royal is a reasonably new operation, having been around since at least the start of 2022. The object of the group and its malware is typical: gain access to a victim's environment, encrypt their data, and extort a ransom to return access to any files touched.

There does not appear to be a single stated infection vector. Instead, infection appears to depend on the individual victim.

The group hints in its ransom note that it means to employ the "double extortion" tactic of threatening to release data captured from the victim in addition to putting a victim's data out of reach via encryption unless a ransom is paid. This however has yet to be definitively proven.

In what appears to be a bit of tongue-in-cheek, the group suggests that its actions are a "pentesting service" and that it will provide the victim with a "security review."

Figure 1: Royal ransom note.

The ransomware itself is a 64-bit Windows executable written in C++.

It is launched via command line, suggesting that it is designed to be run via an operator after access to an environment is provided through another method.

There are two arguments that need to be passed to kick the encryption process off. "-path" determines what is to be encrypted, whether a single directory or an entire drive. "-id" appears to be how the group identifies its victims. This can be any 32-character string, as shown in Figure 2.

Figure 2: Executing Royal.

Regardless of whether either of these arguments are provided, the malware goes ahead and deletes the volume shadow copy off the system.

Figure 3: Royal deleting the volume shadow copy.

Interestingly, it appears that there is a third argument flag in the code that was either abandoned or provides functionality to a feature not yet implemented, "-ep".

Figure 4: All Royal command line arguments, including the unused "-ep" argument.

Royal appears to use the OpenSSL library to encrypt files to the AES standard. Encrypted files are renamed and given a ".royal" file extension.

Figure 5: Files encrypted by Royal.

Interestingly, it appears that a file may not be entirely encrypted in all circumstances. For example, a PDF used in a FortiGuard Labs test system showed some recognizable items after encryption.

Figure 6: Partially encrypted PDF file.

As shown in the ransom note in Figure 1, victims will be provided an ID and a unique Tor page to visit to contact the group about payment.

Figure 7: Royal Tor landing page.

A Tor landing page exists. However, it simply suggests viewing the readme file generated by the encryption process. It also offers a non-interactive contact form to message the group if someone decided to do so.

Figure 8: Tor landing page contact form.

Fortinet Protection

Fortinet customers are already protected from these malware variants through FortiGuard's, AntiVirus, FortiMail, FortiClient, and FortiEDR services, as follows:

FortiGuard Labs detects the known Royal ransomware variants with the following AV signature:

W32/PossibleThreat

IOCs

- 2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f
- 9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Our FREE NSE training: NSE 1 – Information Security Awareness includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

To effectively deal with the evolving and rapidly expanding risk of ransomware, organizations will need to make foundational changes to the frequency, location, and security of their data backups. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Cloud-based security solutions, such as SASE, to protect off-network devices; advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt malware mid-attack; and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be investigated to minimize risk and to reduce the impact of a successful ransomware attack.

As part of the industry's leading fully integrated Security Fabric, delivering native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings. These services are powered by our global FortiGuard team of seasoned cybersecurity experts.

Best Practices include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because payment does not guarantee that files will be recovered. According to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. And our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.