



Royal ransomware investigation: How to brace for the sharp increase

Jan 11, 2023 15:00 CET

Royal ransomware investigation: How to brace for the sharp increase

- Logpoint research reveals what organizations should monitor for to safeguard against the rapid increase in royal ransomware attacks
- The Royal ransomware group has leaked data of more than 60 victims since November 2022

COPENHAGEN, Denmark & BOSTON, January 11, 2022 – Royal ransomware entered the stage in 2022 and quickly became a nuisance for cyber analysts. Logpoint's research team has investigated the ransomware to uncover how analysts can detect and respond to the developing threat.

"Royal stands out as a ransomware provider because it doesn't have affiliates. The ransomware uses various tactics and techniques to reach its goal, like redirecting users using Google ads, sending phishing emails, and personal interactions based on callback phishing," says Doron Davidson, VP Logpoint Global Services. "Despite the many ways to gain initial access, the ransomware deploys in later stages, providing organizations with an opportunity to detect it before it wreaks havoc."

Logpoint's investigation revealed that Royal stops services and kills processes to set up a precondition for the ransomware to detonate. Adversaries use scheduled task functionality to facilitate single or repetitive execution of malicious codes, launching the ransomware. The malware enumerates shared resources on the network to encrypt the share folder and deletes volumes of shadow copy of the drives to prevent recovery from them.

To protect your organization against Royal ransomware, Logpoint recommends:

- Monitoring the infrastructure for stopped services and killed processes
- Monitoring for the creation of scheduled tasks and related events using the schtasks binary
- Monitoring for access to multiple share folders in a short span from the same user and hosts

"It's important that organizations have the right cybersecurity resources in place," says Doron Davidson. "Leveraging the technology advancements in cybersecurity can accelerate threat detection, investigation, and response. For example, automatic incident detection and response can improve cyber intelligence and reduce cyber risk. Investing in advance in Penetration Testing and similar cybersecurity services will reduce the need to pay for Royal's Pentesting services."

Read Logpoint's blog post about Royal ransomware [here](#) and get an in-depth vulnerability analysis, means to detect and respond to the threat, and insights about incident investigation and response.

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's [SIEM](#) and [NDR](#) technologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit <http://logpoint.com>.

Contacts



Maimouna Corr Fonsbøl

Press Contact

Head of PR

PR & Communications

mcf@logpoint.com

+45 25 66 82 98