



## Weekly Intelligence Summary

**In the spotlight:** Luna ransomware, utilizing an unusual encryption scheme, becomes the newest ransomware in trend of malware written in RUST programming language. A new remote access trojan, ApolloRAT, uses Discord as its Command and Control (C&C) Server. BlackBasta ransomware group has claimed responsibility for an attack on German building materials manufacturer, Knauf Group, Juniper Networks released a security update addressing several vulnerabilities that impact multiple products, including Junos Space, Contrail Networking and NorthStar Controller. Atlassian released a patch for CVE-2022-26138, a critical hardcoded credentials vulnerability in Confluence Server and Data Center.

See attachment for full Threat Intelligence Summary and don't forget to check out our [Son of a Breach podcast](#) to hear more from Critical Start security experts.

Thank you,  
Critical Start

The Cyber Threat Intelligence Summary is not intended for redistribution outside of your organization. To provide objective, robust and quality intelligence, the Critical Start Cyber Threat Intelligence Team uses a variety of analytical techniques in our production, primarily Analysis of Competing Hypotheses (ACH), A&B Teaming, and Key Assumption Checks. Our team is highly educated in how to guard against biases, such as groupthink, confirmation bias and mirror imaging, and our work is subjected to rigorous peer review. To learn more about our Analytical Techniques, see our cyber threat intelligence blogs at: <https://criticalstart.com/blog>

