Security Alert: Royal Ransomware Targeting Firewalls

By Leeann NicoloApril 11, 2023

Starting in January 2023, Coalition Incident Response, Inc. (CIR), a technical forensic and remediation firm, began to see increased instances of Royal Ransomware impacting policyholders. Royal Ransomware is a sophisticated malware strain often associated with a group of highly experienced threat actors with documented similarities to former members or associates of the Conti cybercriminal gang.

This increase in activity impacting cyber insurance policyholders was extremely concerning since, in most of CIR's past experiences with the Royal Ransomware strain, the demands entered the millions, with the highest demand Coalition's claim team has seen reaching above $2 million.

Our claims team has received claims from multiple policyholders experiencing almost the same type of attack. CIR began looking for similarities between these seemingly disparate instances since all the victims were from different industries, different regions, and different-sized companies.

A common thread

The ransomware variant detected by CIR appears to have similar indicators of compromise (IOCs) shared between each impacted policyholder. As we looked for consistencies across the multiple cases, we noticed a unique parallel: **all of the companies were using an end-of-sale (EOS) firewall appliance.**

EOS is the last day to order the product directly from a vendor, and for a period of time after the EOS date, the vendor may provide updates and support. In contrast, end-of-life (EOL) products are no longer supported by the original vendor and cannot be upgraded or patched.

In all cases, the impacted organizations didn't have their firewall logging retention set long enough to investigate fully. Logging retention is extremely important as it allows a forensic team to piece together the details of the attack in order to prevent it from recurring.

In each of the cases that CIR investigated, we also discovered virtual private network (VPN) compromises. The threat actors appeared to be gaining access to the victim organizations' VPNs and connecting a device named "Kali" to act on objectives. Kali Linux is a platform that supports information security tasks like penetration testing, security research, computer forensics, and reverse engineering. Both cyber criminals and security administrators widely use it. The VPNs were all managed by the firewall device.

If you have any kind of firewall installed, keep reading

CIR has noticed an uptick in attacks exploiting firewalls, leading, in some cases, to the encryption of an entire network. In other cases, the attack pattern is simpler, wherein the threat actor sends a phishing email, harvests credentials, and then accesses the external-facing VPN.

In cases like these, acting fast is key. For example, one of our policyholders contacted us via phone just as the threat actor was scanning their network. Even though the attackers were able to access some data successfully, the policyholder effectively **avoided data encryption by starting the investigation within two hours of identifying the suspicious activity**.

What should you do?

One of the most critical actions an organization can take to help avoid these risks is to **patch, patch, patch**. Organizations should always ensure they use the most up-to-date versions of their firmware and software.

A best practice is to remove your firewall and move toward Secure Access Service Edge (SASE) technology to protect your network perimeter. The SASE security model allows IT teams to consolidate many networking and security functions into a single cloud service that restricts access based on user, device, and application identity.

SASE uses a zero-trust network access component, meaning *all* users must be authenticated before being granted access to an application or data. This helps prevent unauthorized access, contain breaches, and limit a threat actor's lateral movement on the network should a breach occur. Due to SASE's cloud-based nature, its implementation has the additional benefit of removing the need to maintain the underlying infrastructure.

If a firewall is necessary for your organization's security defenses, you should upgrade the firewalls as often as the budget allows to ensure you are using new-and-improved technology. Enforcing multi-factor authentication on a firewall is also crucial.

Assessing your risk with Coalition Control

At Coalition, we continue to learn about the new tactics employed by this powerful ransomware group, and others like it, so we can continue to advise our broker partners and policyholders and help them to create the best defense possible.

Through CIR and our other security experts and researchers, Coalition continues to monitor active exploitations and other incidents that impact or may potentially impact cyber policyholders. With Active Insurance, cyber policyholders that obtain coverage through Coalition have the added benefit of receiving real-time security alerts during their policy term as incidents and vulnerabilities evolve.

And if the worst happens, Coalition is standing by and ready to help, providing tools and resources to help mitigate losses and remediate damages.

To access your risk management dashboard and understand your on-demand scanning capabilities, log in to Coalition Control.

---

brief summary of such insurance products. Policy obligations are the sole responsibility of the issuing insurance carrier. The descriptions provided herein are solely for informational purposes and are not to be construed as advice of any kind or the rendering of consulting, financial, legal, or other professional services from Coalition. Any action you take upon the information contained herein is strictly at your own risk. Coalition will not be liable for any losses and damages in connection with your use or reliance upon the information.
