LOGPOINT

Logpoint has collated a report highlighting the TTPs and IoCs applied by Cactus to create alert rules to detect methods the group uses

Nov 27, 2023 09:00 CET

Cactus: Defending against a ransomware newcomer

- **Cactus emerged in March this year and has since built an extensive portfolio of high-profile victims.**
- **Logpoint has analyzed Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IoCs) to establish defenses.**

COPENHAGEN, Denmark, November 27, 2023 – Cactus has emerged as a sophisticated ransomware group with a severe impact on its victims. The newcomer first appeared in March 2023 and has entered the top 10 groups with the most monthly victims, ranking at number 7 with 58 victims as of November. The group is focusing on substantial payouts and targets large commercial entities.

“Cactus is a good example of ransomware groups employing increasingly sophisticated TTPs in their attacks. What stands out in this case is that the malware encrypts itself to evade detection,” says Bibek Thapa Magar, Logpoint Security Analytics Engineer. “The smooth way of avoiding defenses shows that the group is good at the game. Cactus has quickly made a significant impact, using double extortion, compromising sensitive data, and leaving victims with limited choices.”

Cactus is a sophisticated ransomware with unique features such as auto-encryption and a consecutive change of file extensions post-encryption, making it more challenging to identify affected files. It employs the well-known and easily “unpackable” UPX packer and divides encrypted files into micro-buffers, possibly to speed up the management of encrypted data streams.

Logpoint has collated a report highlighting the TTPs and IoCs applied by Cactus to create alert rules to detect methods the group uses. According to Kroll, Cactus exploits known vulnerabilities in VPN appliances to gain initial access and establishes commands and control with SSH. The group attempts to dump LSASS and credentials from web browsers to escalate privilege. Ultimately, Cactus gets access to target computers using Splashtop or AnyDesk and creates a proxy between infected hosts using Chisel before encrypting files.

“Cactus is a good reminder that basic cyber hygiene is important, but it also highlights that monitoring and detection is key to protecting against newer ransomware,” says Bibek Thapa Magar. “If activity is detected, security analysts should investigate and make sure it doesn’t spread by disabling virtual private networks (VPNs), remote access servers, single sign-on resources, and public-facing assets before engaging in containment, eradication, and recovery to minimize the impact.”

Logpoint’s security operations platform, Converged SIEM, contains extensive tools and capabilities for identifying, evaluating, and mitigating the impact of Cactus Ransomware. In addition to an alert rule package to help detect Cactus activity, Logpoint offers capabilities enabling security teams to automate essential incident response procedures.

Read Logpoint’s full report about Cactus here and get a deep dive into the group’s attack design and how to detect and respond to the threat.

About Logpoint

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 SIEMand NDRtechnologies 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