Case Study-The new ransomware that targets Windows and Linux systems, Cicada3301

Leonardo Oliveira Pereira
University of Coimbra, Department of Informatics Engineering, Portugal
uc2020239125@student.uc.pt

***Abstract*—This case study analyses Cicada3301, a ransomware variant that was created using the Rust programming language. Drawing comparisons to the BlackCat ransomware, Cicada3301 introduces unique innovations, marking an evolution in ransomware-as-a-service (RaaS) operations. This paper explores the ransomware's origins, technical functionality, and broader implications for cybersecurity, alongside with practical countermeasures. It emphasizes the critical need for proactive defences, collaboration among stakeholders, and continuous adaptation to fight ransomware threats in an increasingly interconnected digital world.**

Keywords—Cicada3301, Ransomware, BlackCat, Rust

I. Introduction

Ransomware has capitalized into one of the most common and tormented types of cyber-crime in this rapidly changing world of cybersecurity. Ransomware, which is a type of malicious software that encrypts data and makes it inaccessible until a ransom is paid to the attacker, has affected individuals, organizations, and even critical infrastructure over the past years in many instances disrupting entire departments due to heavy financial and operational losses incurred. The newest addition to this trend of threat is Cicada3301 — a highly sophisticated ransomware strain named after an alleged internet phenomenon whose origins are somewhat mysterious. Though it is uncertain if there actually is any link to the ransomware and original Cicada 3301 group that posted these puzzles, the name does capture attention and suggests a meticulous approach by its makers [5].

The purpose of this paper is to conduct a thorough examination concerning the Cicada3301 ransomware, covering its origins, technological functionality and damage it can do to individual as well as an enterprise level. It will also discuss its impact on the future of cyber-security and why it is already time for, to be more proactive in defence against the ever-growing threat of ransomware. This research attempts to add Cicada3301 into the body of knowledge related to ransomware threats and help emphasize the dire need for collaboration in order to mitigate their effects.

II. How does Cicada3301 works?

Cicada3301 first appeared in June 2024 and has since claimed more than 30 victims, predominantly small and medium-sized businesses (SMBs) in the healthcare, hospitality, manufacturing/industrial and retail sectors, located in North America and the UK [1].

Cicada3301 is no different from other ransomware in that the starting point is phishing attacks to extort a user's credentials in order to potentially access Remote Desktop Protocol (RPD) endpoints and infect cooperating systems [2].

When an organization is infected by Cicada3301, a greeting message is sent informing it that its most important data and files have been downloaded from the company's network and then encrypted. Later, another message is sent saying that the Cicada group has proof that the data was stolen and that it can be recovered by buying the decryption tool. The payment is made with cryptocurrencies, specifically Bitcoin and Monero [5], and in addition to the decryption tool it also offers help to rebuild the infrastructure and prevent other attacks of the same kind in the future. In the event of payment not being made on time, the group will publish the stolen data on its blog and will also send it to the regulated authorities in the company's country, as well as to its customers, partners and competitors [4].

As previously mentioned, the origins of this ransomware are somewhat mysterious. However, security researchers claim that it resembles the ALPHV BlackCat ransomware but Cicada3301 distinguishes itself with significant innovations, particularly in how it executes and integrates compromised credentials, marking an evolution in ransomware tactics [4] [5].

III. Security Properties

Although it's not just a BlackCat clone, Cicada3301 was also written in Rust. Rust is a programming language that has gained popularity over time due to its speed, security options, and ability to compromise both Windows and Linux machines. Due to these characteristics, Rust-based ransomware has become a nightmare for security teams, as it is more difficult to detect and reverse-engineer than ransomware written in more common languages, making Cicada 3301 a stealthy and dangerous threat. Given that Rust-based ransomware is also new, there aren't many tools to analyse or block it [3].

Similar to the BlackCat, Cicada3301 "features a well-defined parameter configuration interface, registers a vector exception handler, and employs similar methods for shadow copy deletion and tampering" [5]. The two ransomware were also compiled using the same set of tools, most likely due to the fact that the new Ransomware-as-a-service (RaaS) group has either already seen the BlackCat code base or is using the

same developers [1]. In addition, and according to Ramos-Beauchamp, besides using the same toolset, Cicada3301 also reuses some of the IPs that BlackCat used to use alongside the psexec executable for lateral movement [2].

After sneaking into Cicada3301's control panel, Grupo-IB was able to identify some differences between the two ransomwares, with Cicada3301 having only six command line options, having no embedded configuration, having a different naming convention in the ransom note, and its encryptor requires entering the correct initial activation key to start. According to Group-IB, "In contrast, where the access key is used to decrypt BlackCat's configuration, the key entered on the command line in Cicada3301 is used to decrypt the ransom note". Cicada3301 was designed to target multiple architectures and several operating systems and uses ChaCha20 and RSA encryption with configurable modes, shuts down virtual machines, terminates specific processes and services, eliminates shadow copies, encrypts network shares and increases overall efficiency by running dozens of simultaneous encryption threads. Finally, the threat entity is still recruiting affiliates and those interested in joining the organization will be given access to a web interface panel with news about the malware, victim management, chats, account information and an FAQ section [1] [6].

IV. Security Measures

Both Cicada3301 and other ransomware are a real threat to organizations, so it's important to reduce and mitigate the risks. Here are some practical steps to safeguard business from ransomware like this [3]:

- **Regular Backups:** One of the most effective ways to fight ransomware is to make regular backups of your data. If you do get hit, restoring the files from the backups will prevent you from paying a ransom. In order to prevent ransomware from striking, it's important to keep at least one backup offline.
- **Enable Multi-Factor authentication (MFA):** With MFA a second layer of protection is added, by requiring two or more forms of authentication (e.g. a password and a code sent to a user's phone), to ensure that hackers will have a much harder time breaking in.
- **Scan for vulnerabilities:** Regularly scanning the equipment that is connected to the network helps to identify vulnerabilities or missing updates, thus preventing hackers from taking advantage of them.
- **Keeping software up-to-date:** Have the latest security and system vulnerability patches is paramount since cybercriminals often target weaknesses in outdated software.
- **Educate the employees:** As employees are often the first line of defence, it's imperative to keep staff informed about phishing attacks and other social engineering techniques, as phishing is often the entry point for ransomware and therefore it's vital to have a cybersecurity training programme.
- **Use Advanced Security Tools (EDR):** Threats like Cicada3301 need new strategies to be defended. Endpoint Detection and Response (EDR) tools are designed to detect unusual activity in your network and respond quickly. It is crucial to choose tools specifically designed to fight advanced threats like ransomware written in new programming languages.
- **Prepare an Incident Response Plan:** Developing a response plan that isolates the affected systems, reports the attack to the law enforcement, informs stakeholders, among others, makes it possible to act quickly and minimize the damage if an attack happens.

In addition to these security measures, there are others such as hiring threat hunting services, creating strong and unique passwords, and reporting ransomware attacks to CISA, a local FBI field office or a Secret Service field office [4]. All these measures together make us better protected against Cicada3301 and other ransomware, but it's important to remember that all security isn't enough, as new and more sophisticated threats will continue to emerge, so we must be informed, proactive and take the appropriate precautions.

V. Conclusion

Cicada3301 is a good example of how ransomware are evolving, through cross-platform attacks, advanced encryption mechanisms and stealthy operations on Rust. That similarity to BlackCat, as well as some innovations of its own, shows the continued trend of sophistication found in ransomware-as-a-service (RaaS). They say the strain underscores the need for basic cybersecurity practices: regular backups to bring back lost files, multifactor authentication, vulnerability scanning, employee training, advanced detection tools and an incident response plan.

In conclusion, ransomware like Cicada3301 will require organizations, cybersecurity experts, and law enforcement to work together. Cicada3301 presents a great challenge, but with the right strategies in place, like enhanced defences, increased awareness, and timely information sharing, the dangers surrounding such threats can be mitigated as we navigate an interconnected digital world.

References

[1] Ionut Arghire. Blackcat ransomware successor cicada3301 emerges - securityweek. https://www.securityweek.com/blackcat-ransomware-successor-cicada3301-emerges/, October 2024. (Accessed on 11/24/2024).

[2] Doug Bonderud. Has blackcat returned as cicada3301? maybe. https://securityintelligence.com/news/has-blackcat-returned-as-cicada3301/, October 2024. (Accessed on 11/24/2024).

[3] Katie Boquetti. New rust-based cicada 3301 ransomware - cyberhoot. https://cyberhoot.com/blog/new-rust-based-cicada-3301-ransomware/, September 2024. (Accessed on 11/24/2024).

[4] Graham Cluley. Cicada ransomware - what you need to know — tripwire. https://www.tripwire.com/state-of-security/cicada-ransomware-what-you-need-know, September 2024. (Accessed on 11/24/2024).

[5] Michael Gorelik. Decoding the puzzle: Cicada3301 ransomware threat analysis. https://blog.morphisec.com/cicada3301-ransomware-threat-analysis, September 2024. (Accessed on 11/22/2024).

[6] Nikolay Kichatov and Sharmine Low. Encrypted symphony — group-ib blog. https://www.group-ib.com/blog/cicada3301/, October 2024. (Accessed on 11/24/2024).