David Murillo Santiago
IS-3513
15 October 2023

Challenge 3: MITRE ATT&CK

1. What is the purpose of the website located at the link above?

The website "https://attack.mitre.org" stands as a cybersecurity resource, dedicated to serving the needs of cybersecurity professionals and organizations. At its core, the site is designed to disseminate crucial knowledge regarding cyber threats, attack techniques, and adversary strategies. It is home to the MITRE ATT&CK framework, a comprehensive repository that categorizes and elaborates on diverse cyber attack methods. Its purpose is to provide extensive cyber threat intelligence, active support for incident response initiatives, security awareness, and facilitate research and education within the cybersecurity realm. By doing so, this website equips professionals with a deeper understanding of cyber threats, thereby enhancing their ability to mount effective defenses.

2. What is "GravityRAT?" What is its MITRE ATT&CK ID?

GravityRAT is a remote access tool (RAT). It is known for its malicious capabilities, and the anonymity of the actor. The malware has been involved in attacks targeting organizations and entities in India. Its MITRE ATT&CK ID is S0237. GravityRAT employs various tactics, such as using HTTP for Command and Control, stealing files with specific extensions, exploiting removable media, and employing dynamic data exchange (DDE) to infiltrate systems. It is also proficient in concealing indicators, listing running processes, and creating scheduled tasks for persistence. GravityRAT exhibits significant versatility, posing a formidable threat in the cybersecurity landscape. Organizations and professionals must remain vigilant in detecting and mitigating its activities to safeguard their systems and data.

3. Under "Techniques Used," What is technique T1497 .001?

Technique T1497 .001 involves "Virtualization/Sandbox Evasion: System Checks." It is a tactic used by GravityRAT to assess the environment it's operating in, specifically checking for signs of virtualization or sandboxing, such as strings like "VMWare," "Virtual," and "XEN." Also, it makes use of another check, examining the hardware's current temperature to determine if it's within a virtual machine environment. This technique is part of the malware's strategy to evade detection and analysis in a controlled environment like a sandbox or virtual machine.

4. Does GravityRAT support encryption? Which cipher is used? What is the key?

GravityRAT does indeed support encryption, specifically employing the Advanced Encryption Standard (AES) cipher. The key utilized for this encryption is "lolomycin2017." This encryption plays a pivotal role in the malware's operations. It serves to obfuscate and secure its malicious activities and communications. By utilizing AES, GravityRAT enhances its ability to evade

detection and analysis, as this encryption method is widely recognized for its robust security measures. This added layer of complexity ensures that its malicious actions remain concealed and protected from scrutiny, making it a formidable challenge for cybersecurity professionals striving to detect and mitigate its activities effectively.

5. Who are the actors responsible? Who has been the target?

The GravityRAT malware has resurfaced, posing a threat to Android users. GravityRAT targets Android users by disguising itself as legitimate messaging applications, with one of its notable traits being the ability to exfiltrate WhatsApp backup files, containing sensitive user data like messages and documents in an unencrypted form (The Hacker News https://thehackernews.com/2023/06/warning-gravityrat-android-trojan.html). The malware operators, known as 'SpaceCobra,' have taken advantage of deceptive tactics, such as creating counterfeit chat apps to distribute the malware. BingeChat and Chatico, two of the malicious apps, were distributed through rogue websites promoting free messaging services. Users were lured into downloading these apps through various tactics, including impersonating recruiters and creating fake personas on social media platforms like Facebook and Instagram (BlackHat Ethical Hacking https://www.blackhatethicalhacking.com/news/gravityrat-the-android-malware-threat-exploiting-whatsapp-backups/). Additionally, GravityRAT requests a series of intrusive permissions upon installation, including access to contacts, location, call logs, camera, and microphone. (BleepingComputer https://www.bleepingcomputer.com/news/security/android-gravityrat-malware-now-steals-your-whatsapp-backups/). Before a user even registers on BingeChat, the app secretly sends call logs, contact lists, SMS messages, device location, and basic device information to the threat actor's command and control server. The malware's interest in specific file extensions, such as image and document files, indicates its focus on WhatsApp Messenger backups (BleepingComputer https://www.bleepingcomputer.com/news/security/android-gravityrat-malware-now-steals-your-whatsapp-backups/). Furthermore, the latest version of GravityRAT can receive commands from its command-and-control (C2) server, enabling it to delete files, contacts, and call logs, which is unusual for Android malware (The Hacker News). To protect against these threats, users should follow best practices, including downloading applications only from trusted sources like Google Play, being cautious with permissions requested during installation, and ensuring their backup files are securely stored. It is essential to use sites like MITRE ATT&CK to remain informed about evolving threats to protect against potential breaches of sensitive information.

Citations

The Hacker News (https://thehackernews.com/2023/06/warning-gravityrat-android-trojan.html) - This article provided information about GravityRAT's ability to exfiltrate WhatsApp backup files, its deceptive tactics, the distribution of malicious apps like BingeChat and Chatico through rogue websites, and its capability to receive commands from the command-and-control (C2) server.

BlackHat Ethical Hacking (https://www.blackhatethicalhacking.com/news/gravityrat-the-android-malware-threat-exploiting-whatsapp-backups/) - This source contributed details about GravityRAT's deceptive tactics, specifically how it impersonated recruiters and created fake personas on social media platforms, along with its distribution methods.

BleepingComputer (https://www.bleepingcomputer.com/news/security/android-gravityrat-malware-now-steals-your-whatsapp-backups/) - Information from this article was included regarding GravityRAT's intrusive permissions requests upon installation, its data exfiltration behavior, and its focus on specific file extensions related to WhatsApp Messenger backups.

MITRE ATT&CK Framework (https://attack.mitre.org/) - This source served as a reference for information regarding the MITRE ATT&CK framework and its relevance to GravityRAT's techniques and encryption details.