GoldBrute botnet campaign is trying to hack 1.5 million RDP servers worldwide

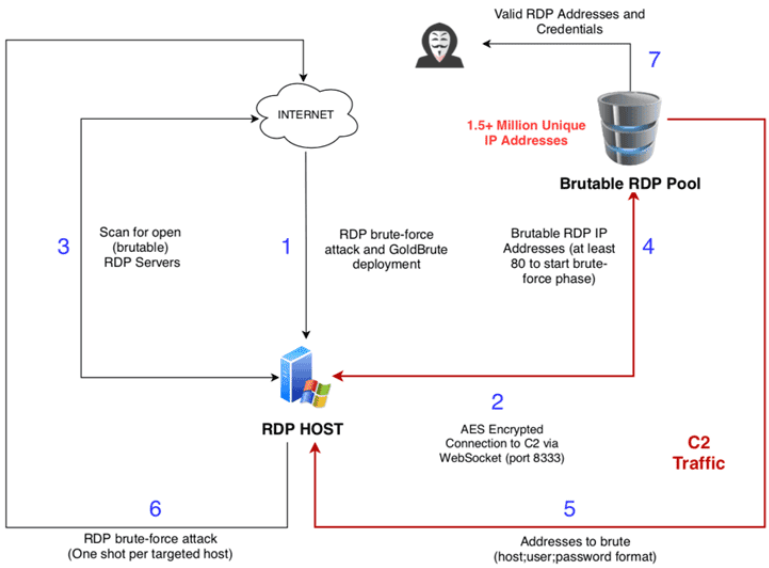
New security researchers discover an ongoing sophisticated botnet campaign, using brute-force methods targeting more than 1.5 million publicly accessible Windows RDP servers on the Internet.

New security researchers discover an ongoing sophisticated botnet campaign, using brute-force methods targeting more than 1.5 million publicly accessible Windows RDP servers on the Internet.

Named GoldBrute, botnet diagrams have been designed to gradually escalate, adding new cracked systems to its network, forcing them to find new available RDP servers and then proceed. brute-force.

To bypass security tools and malware analysts, attackers ordered each infected machine to target millions of servers with unique username and password sets. Therefore, servers will be brute-force attacked from different IP addresses.

This campaign was discovered by Renato Marinho at Morphus Labs. How it works is explained in the following steps:



How it works The GoldBrute botnet

Step 1 - After brute-force successfully an RDP server, the attacker installs the GoldBrute malware (based on JAVA) on the machine.

Step 2 - To control infected machines, the attacker uses a centralized, fixed command and control server to exchange commands and data via the WebSocket connection, which is encrypted with AES.

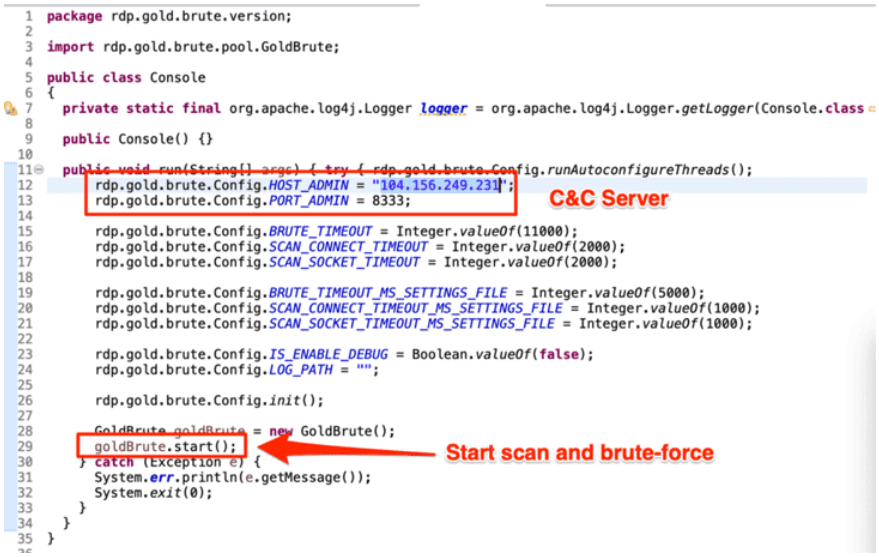
Steps 3 and 4 - Each infected machine then receives the first task of scanning and reporting a list of at least 80 new RDP servers that are publicly accessible and brute-force.

Steps 5 and 6 - The attacker then assigns each machine a unique set of usernames and passwords to perform the second task: using brute-force to attack the list of RDP targets that the system is infected with. continue to receive from C&C server.

Step 7 - When the test was successful, the infected machine reported the login information to the C&C server.

Currently, it is unclear exactly how many RDP servers have been compromised and involved in brute-force attacks against other RDP servers on the Internet.

According to The Hacker News, at the time of writing, a quick search by Shodan showed that about 2.4 million Windows RDP servers can be accessed on the Internet and perhaps more than half of these are being attacked.



Recently, security researchers have discovered two new security holes related to Remote Desktop Protocol (RDP), only one of which Microsoft patched, called BlueKeep.

BlueKeep (CVE-2019-0708) allows remote attackers to control RDP servers and if successfully exploited, can cause devastation around the world, potentially worse than those What WannaCry and NotPetya did in 2017.

The unpatched vulnerability in Windows could allow a client-side attacker to bypass the lock screen on remote desktop sessions (RD).

You finished reading the article "**GoldBrute botnet campaign is trying to hack 1.5 million RDP servers worldwide**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.