Cybersecurity, Cyber Attack

FlawedGrace RAT

21 Mar

FlawedGrace is the name of a Remote Access Threat (RAT) that is part of the menacing arsenal of the financially motivated cyber criminals gang known as TA505 (or Hive0065).

The group has been active since at least 2014 and is among the most prolific with multiple attack campaigns attributed to it.

Another distinguishing feature of TA505 is its propensity to implement frequent changes to both their TTP (tactics, techniques, and procedures), as well as the types of malware threats.

The group was observed carrying out massive email spam campaigns delivering the Dridex Banking Trojan, before moving on to distributing the Locky and Jaff Ransomware threats, the TrickBot Banking Trojan, and more.

FlawedGrace details

The first time the FlawedGrace RAT was detected by researchers was in November 2017.

It is a powerful RAT written in the C++ programming language.

It can recognize multiple incoming commands from a Command-and-Control server sent over a custom binary protocol using port 443.

You can instruct the threat to retrieve additional damaged modules and then load and run them.

It can also download and extract chosen files, collect sensitive information about the user, such as passwords and more.

In the latest attack operations carried out by TA505, an updated version of the FlawedGrace RAT has been implemented.

While full change analysis is still ongoing, researchers have so far observed that the threat now uses encrypted strings and obfuscated API calls.

Another difference was found in how the threat stored its configuration.

The initial or default configuration is stored on the system as an encrypted resource.

It is then split into two: a current configuration instance placed in a mapped memory region and a persistence mechanism placed in the registry.

FlawedGrace is distributed via phishing

A massive phishing campaign has been identified targeting a large number of companies across Europe by spreading the FlawedGrace malware.

According to Proofpoint security researchers, the attacks of the new FlawedGrace variant would begin with a series of waves of a few emails, delivering only several thousand messages at each stage, before escalating to tens or hundreds of thousands malicious e-mail messages.

The TA505 group has a proven track record in targeted attacks on research institutes, banks, retail businesses, energy companies, healthcare institutions, airlines, and government agencies.

The malware infection chain

Even in the case of the new FlawedGrace RAT variant, malicious activities begin with the opening of attachments containing malware in phishing messages that typically refer to COVID-19 updates, insurance claims, or notifications on Microsoft OneDrive shared files.

The success of the latest phishing campaign, in particular, depends on users enabling macros after opening malicious Excel attachments distributed by criminal hackers.

Activating the macro then allows you to download n covert MSI files to retrieve the loaders for the next stage of the attack chain where the updated version of FlawedGrace RAT is delivered, which incorporates support for encrypted strings and covert API calls.

The criminal group behind FlawedGrace

The wave of attacks recorded in the last months of 2021 is also significant for its change in the TTP used by criminal hackers, which include the use of intermediate loaders, scripts in unusual languages such as Rebol and KiXtart instead of Get2, a downloader previously deployed by the group to perform reconnaissance and download and install final stage RAT payloads.

According to Proofpoint researchers, TA505 is an established financially motivated threat actor known for conducting malicious email campaigns on a scale never seen before.

The group regularly changes its TTP and is considered a trendsetter in the world of cybercrime.

Additionally, the mutability of malware combined with TA505's ability to be flexible, focusing on what is most profitable and adapting its TTP as needed, makes the actor an ongoing threat.

How to defend yourself

The spread of the FlawedGrace RAT malware represents the most evident part of yet another large-scale phishing attack, characterized in this case by its mutability.

The first tip to protect yourself from this new threat is, therefore, to carefully consider the opening of unknown attachments from untrusted e-mail addresses.

At the same time, it is always very important to avoid the activation of potentially harmful macros on your device.

In this sense, it is useful to have a team of experts able to safeguard the security of the cyber perimeter.

It is also important, especially in the corporate context, to ensure that one's employees maintain a high level of awareness of possible threats, periodically alerting them to new attacks in progress.

Finally, consider adding the threat IoCs published by Proofpoint researchers to your security systems.