DoppelPaymer ransomware gang rebrands as the Grief group

July 29, 2021

After a period of little to no activity, the DoppelPaymer ransomware operation has made a rebranding move, now going by the name Grief (a.k.a. Pay or Grief).

It is unclear if any of the original developers are still behind this ransomware-as-a-service (RaaS) but clues uncovered by security researchers point to a continuation of the "project."

DoppelPaymer's activity started to decline in mid-May, about a week after DarkSide ransomware's attack on Colonial Pipeline, one of the largest fuel pipeline operators in the U.S.

With no updates on their leak site since May 6, it looked like the DoppelPaymer gang was taking a step back, waiting for the public's attention to ransomware attacks to dissipate.

However, security researchers last month pointed that Grief and DoppelPaymer were names for the same threat.

Fabian Wosar of Emsisoft told BleepingComputer that the two shared the same encrypted file format and used the same distribution channel, the Dridex botnet.

source: Michael Gillespie

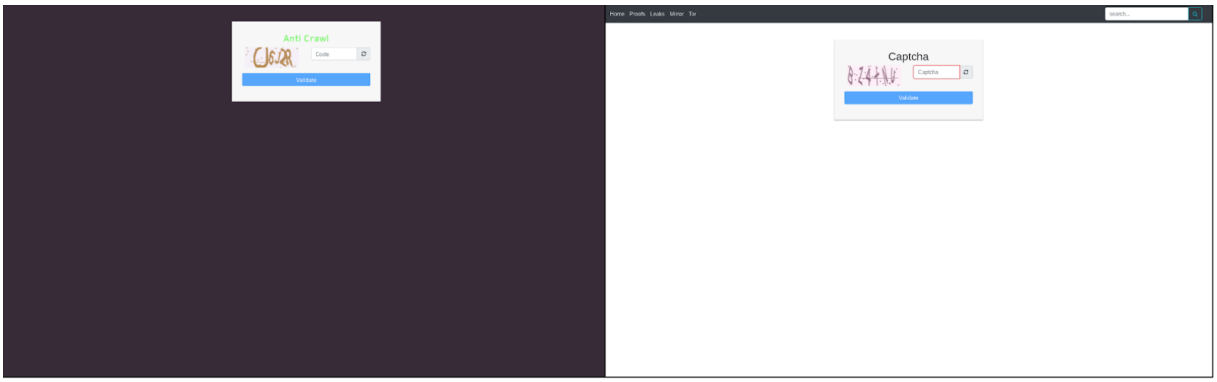
Despite the threat actor's effort to make Grief look like a separate RaaS, the similarities to DoppelPaymer are so striking that a connection between the two is impossible to dismiss.

News about Grief ransomware emerged in early June, when it was believed to be a new operation but a sample was found with a compilation date of May 17.

Malware researchers at cloud security company Zscaler analyzed the early Grief ransomware sample and noticed that the ransom note dropped on infected systems pointed to the DoppelPaymer portal.

> “This suggests that the malware author may have still been in the process of developing the Grief ransom portal. Ransomware threat groups often rebrand the name of the malware as a diversion” - Zscaler

The connection between the two extends further, to their leak sites. Although visually they could not be more different, similarities abound, like the captcha code that prevents automated crawling of the site.



Furthermore, the two ransomware threats rely on highly similar code that implements “identical encryption algorithms (2048-bit RSA and 256-bit AES), import hashing, and entry point offset calculation.”

Another similarity is that both Grief and DoppelPaymer use the European Union General Data Protection Regulation (GDPR) as a warning that non-paying victims would still have to face legal penalties due to the breach.

There is so little setting the two apart, and it’s mostly cosmetic, that malware researchers strongly believe that it’s the same operation under a different name.

For instance, Grief switched to Monero cryptocurrency, which could be a protective measure against potential action from law enforcement that could lead to seizing the ransom money already collected.

Another difference is that Grief ransomware uses the term “griefs” for the victim data leaked on their site either as proof of the compromise (“griefs in progress”) or as punishment for not paying the ransom (“complete griefs”).

At the moment, there are more than two dozen victims listed on the Grief leak site, showing that the threat actor has been busy working under the new name. It looks like the gang also claims the recent attack on the Greek city Thessaloniki, publishing a file archive as proof of the intrusion.

Zscaler says that “Grief ransomware is the latest version of DoppelPaymer ransomware with minor code changes and a new cosmetic theme,” adding

that the gang has kept in the shadow to avoid the level of attention that REvil got for breaching Kaseya and DarkSide for hitting Colonial Pipeline.

A ransomware gang rebranding is not necessarily looking to erase their tracks and may be doing it to avoid any government sanctions that would prevent victims from paying the ransom.

A short list of five hashes for the samples that Zscaler caught is available in the blog post.