DoppelPaymer Continues to Cause Grief Through Rebranding

zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding

In early May 2021, *DoppelPaymer* ransomware activity dropped significantly. Although the DoppelPaymer leak site still remains online, there has not been a new victim post since May 6, 2021. In addition, no victim posts have been updated since the end of June. This lull is likely a reaction to the Colonial Pipeline ransomware attack which occurred on May 7, 2021. However, the apparent break is due to the threat group behind DoppelPaymer rebranding the ransomware under the name *Grief* (aka Pay OR Grief). An early Grief ransomware (aka Pay or Grief) sample was compiled on May 17, 2021. This sample is particularly interesting because it contains the Grief ransomware code and ransom note, but the link in the ransom note points to the DoppelPaymer ransom 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.

In this blog, we will compare the similarities between DoppelPaymer and Grief ransomware. Both ransomware leak sites are nearly identical, including shared code that displays a captcha to prevent automated crawling as shown in Figure 1.

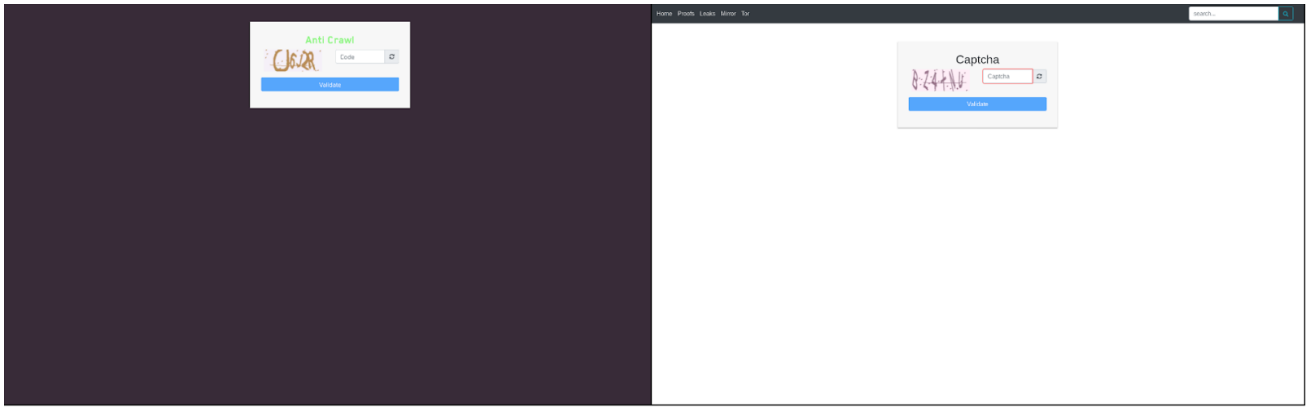

Figure 1. Grief ransomware (left) and DoppelPaymer (right) captcha

The main landing page has changed the term *latest proofs* to *griefs in progress* and *latest leaks* to *complete griefs*. The victim-specific leak page layouts are also identical as shown below in Figure 2 containing the victims URL, organizational description, images of stolen data, example stolen data files, and a list of machines that were compromised.

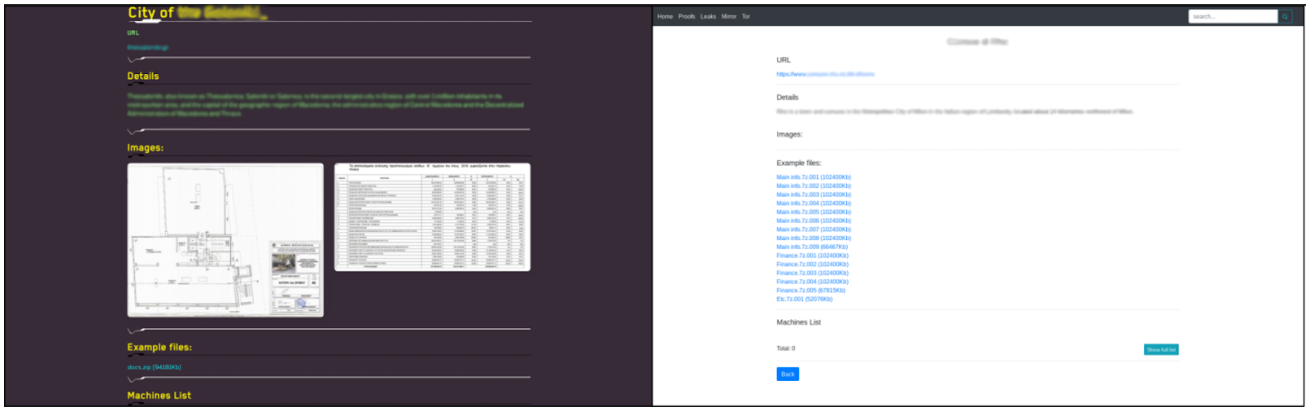

Figure 2. Grief ransomware (left) and DoppelPaymer (right) victim leak pages

The Grief ransom portal has some differences from the DoppelPaymer portal. In particular, the ransom demand payment method is made in Monero (XMR) instead of Bitcoin (BTC). This switch in cryptocurrencies may be in response to the FBI recovering part of the Colonial Pipeline ransom payment. The Grief ransom portal, however, kept the same live chat code that allows victims to resume a previous conversation or to start a new conversation as shown in Figure 3.

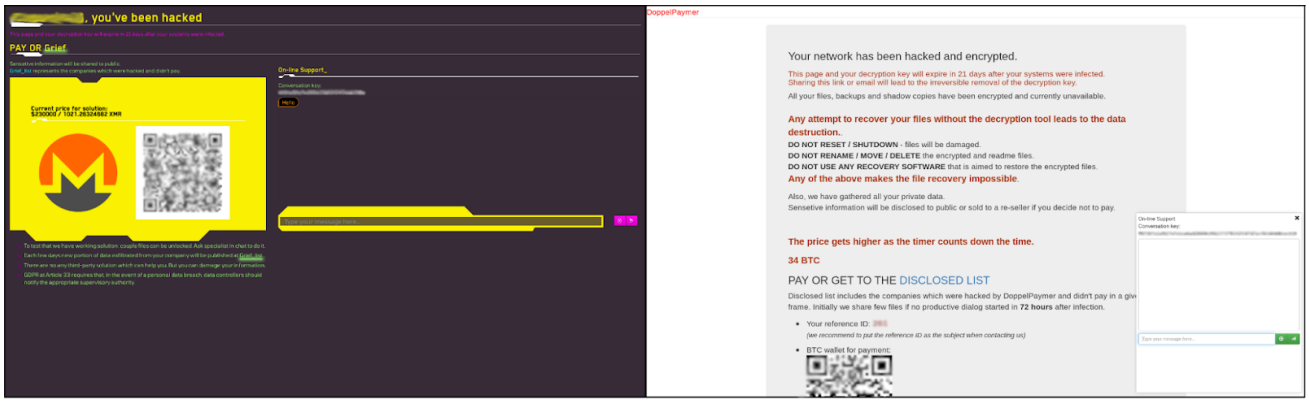

Figure 3. Grief ransomware (left) and DoppelPaymer (right) victim ransom portals

Grief ransomware portal and leak site also attempts to weaponize the European Union's General Data Protection Regulation (GDPR) to pressure businesses into paying a ransom to avoid potential fines.

The malware code differences between DoppelPaymer and Grief are also relatively minimal. Grief samples removed the embedded ProcessHacker binaries. However, Grief still retains the code to decrypt data from the binary's .sdata section. The Grief string encryption algorithm is similar to DoppelPaymer, except the RC4 key was increased from a length of 40 bytes to 48 bytes. The vast majority of the two codebases are very similar with identical encryption algorithms (2048-bit RSA and 256-bit AES), import hashing, and entry point offset calculation.

Conclusion

Grief ransomware is the latest version of DoppelPaymer ransomware with minor code changes and a new cosmetic theme. The threat group has been very active since the release of Grief in the middle of May 2021. However, they have been successful in maintaining a low profile so far. This is in light of recent high-profile attacks including the Colonial Pipeline hack by Darkside ransomware and the Kaseya supply-chain attack by REvil.

Indicators of Compromise (IOCs)

The following IOCs can be used to detect Grief ransomware.

Samples

SHA256 Hash	Module Name

b5c188e82a1dad02f71fcb40783cd8b910ba886acee12f7f74c73ed310709cd2	Grief ransomware sample
91e310cf795dabd8c51d1061ac78662c5bf4cfd277c732385a82f181e8c29556	Grief ransomware sample
dda4598f29a033d2ec4f89f4ae687e12b927272462d25ca1b8dec4dc0acb1bec	Grief ransomware sample
0864575d4f487e52a1479c61c2c4ad16742d92e16d0c10f5ed2b40506bbc6ca0	Grief ransomware sample
b21ad8622623ce4bcdbf8c5794ef93e2fb6c46cd202d70dbeb088ea6ca4ff9c8	Grief ransomware sample (early build)