Dark Web Threat Profile: Grief Ransomware Group

Published: 2021-11-02 · Archived: 2026-04-05 13:32:36 UTC

New **ransomware** called Grief was considered to be a new operation at first. Security researchers noticed that a new Grief gang carries similarities with the DoppelPaymer crew. On the other hand, DoppelPaymer was considered based on the BitPaymer ransomware (which first emerged in 2017) due to the connections in their code, ransom notes, and payment portals.

Grief: A Rebranding Story

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

Because there have been no updates on their leak site since May 6, 2021, it looked like the DoppelPaymer gang was taking a step back, waiting for the public's attention to **ransomware attacks** to disappear.

However, after months of silence, the DoppelPaymer ransomware gang appears to have rebranded itself to "Grief." News about Grief **ransomware** appeared in early June when it was believed to be a new operation, but later, researchers discovered a malware sample dated May 17.

Grief vs. DoppelPaymer: Their Similarities and Differences

Although the threat actor tried to make Grief look like a separate RaaS (Ransomware as a Service), the similarities to DoppelPaymer are so apparent that a connection between the two is impossible to dismiss. The sample found with a compilation date of May 17 contains the Grief ransomware code and the ransom note, but the link in the ransom note points to the DoppelPaymer ransom portal.

Groups' leak sites are almost identical, including shared code that displays a captcha to prevent automated crawling. The ransomware groups use similar code with the same encryption algorithms (2048-bit RSA and 256-bit AES), entry point offset calculation, and import hashing. Another similarity is the EU General Data Protection Regulation (GDPR) on their leak site to alert non-paying victims.

Log in Screen of Leak Sites Of Grief and DoppelPaymer

Comparison Table for the Differences between Grief and DoppelPaymer

Based on these similarities and very few differences, analysts have concluded that Grief is rebranding DoppelPaymer. The new effort by DoppelPaymer seems to be more about staying low profile than going complicated in nature.

Grief Wants to Play a Game: Their Pressure Tactics

Grief Ransomware gang said, “We wanna play a game” in a message posted to its Tor-hosted leak site on September 13, 2021. The statement says they will delete a victim’s decryption key if they hire a negotiation company. Grief is not the first **ransomware group** that came up with this approach.

As a new tactic for increasing the pressure on victims, the Ragnar Locker ransomware gang announced a warning on their darknet leak site. They stated that from this moment if any victim hires a recovery company for consultations or sends requests to the police, FBI, or investigators, they will consider this as a hostile intent and launch the publication of complete compromised data.

As another pressure tactic, there is a catchy reference to GDPR (General Data Protection Regulation) on their landing page. The group is trying to motivate victims to pay them earlier to prevent possible issues with European regulators, which is one of the extortion tactics. The GDPR allows the EU’s Data Protection Authorities to issue penalties of up to €20 million or 4% of annual global turnover (whichever is higher), which will be a higher price than a possible ransom payment to ransomware gang.

Homepage of Grief Ransomware Leak Site and The GDPR Regulation on It

Target Profile of Grief Ransomware Group

At present, there are over two dozen victims on the Grief leak site, and it looks like the actor has been busy, but still, their target profile cannot be determined certainly. However, it can be stated, according to their recent victims, that Grief has no moderate attitude towards schools, hospitals, or non-profitable charitable foundations such as Babuk does.

Also, According to the FBI notification, their origin gang DoppelPaymer’s initial targets were organizations in healthcare, emergency services, and education.

Grief Ransomware Gang Post Listed on SOCRadar’s DarkMirror

Tactics, Techniques, and Procedures (TTP) of Grief

Ransomware gangs usually destroy shadow copies (T1490 Inhibit System Recovery), but Grief is not observed doing this. Its reason could be that Grief was designed for the operator to delete shadow copies manually or for other reasons. It is vital because if a victim has shadow copies enabled on a machine, they may restore missed data. Grief setting the system to boot from safe mode with minimum services available and no network connectivity is remarkable because very few ransomware families do this.

Grief has a unique way of setting itself up for persistence. It adjusts a legitimate Windows Service configuration to run the malware. Grief chooses a legitimate Windows Service and replaces the ImagePath registry value of the service’s configuration to execute the **ransomware** again at the next boot (T1543.003 Create or Modify System Process: Windows Service). It guarantees that the next time the system begins, Grief operates again and returns the system to safe mode

- Discover your unknown hacker-exposed assets
- Check if your IP addresses tagged as malicious
- Monitor your domain name on hacked websites and phishing databases
- Get notified when a critical zero-day vulnerability is disclosed

Free for 12 months for 1 corporate domain and 100 auto-discovered digital assets.
Try for free
