An Overview of the DoppelPaymer Ransomware

By By: Trend Micro Research Jan 05, 2021 Read time: 4 min (1006 words)

Published: 2021-01-05 · Archived: 2026-04-05 17:08:53 UTC

In early December 2020, the FBI issued a warning regarding DoppelPaymer, a ransomware family that first appeared in 2019 when it launched attacks against organizations in critical industries. Its activities have continued throughout 2020, including a spate of incidents in the second half of the year that left its victims struggling to properly carry out their operations.

What is DoppelPaymer?

DoppelPaymer is believed to be based on the BitPaymer ransomware (which first appeared in 2017) due to similarities in their code, ransom notes, and payment portals. It is important to note, however, that there are some differences between DoppelPaymer and BitPaymer. For example, DoppelPaymer uses 2048-bit RSA + 256-bit AES for encryption, while BitPaymer uses 4096-bit RSA + 256-bit AES (with older versions using 1024-bit RSA + 128-bit RC4). Furthermore, DoppelPaymer improves upon BitPaymer's rate of encryption by using threaded file encryption.

Another difference between the two is that before DoppelPaymer executes its malicious routines, it needs to have the correct command-line parameter. Our experience with the samples that we encountered shows different parameters for different samples. This technique is possibly used by the attackers to avoid detection via sandbox analysis as well as to prevent security researchers from studying the samples.

Perhaps the most unique aspect of DoppelPaymer is its use of a tool called Process Hacker, which it uses to terminate services and processes related to security, email server, backup, and database software to impair defenses and prevent access violation during encryption. in order to prevent access violation during encryption.

Like many modern ransomware families, DoppelPaymer's ransom demands for file decryption are sizeable, ranging anywhere from US$25,000 to US$1.2 million. Furthermore, starting in February 2020, the malicious actors behind DoppelPaymer launched a data leak site. They then threaten victims with the publication of their stolen files on the data leak site as part of the ransomware's extortion scheme.

What is DoppelPaymer's routine?

DoppelPaymer uses a fairly sophisticated routine, starting off with network infiltration via malicious spam emails containing spear-phishing links or attachments designed to lure unsuspecting users into executing malicious code that is usually disguised as a genuine document. This code is responsible for downloading other malware with more advanced capabilities (such as Emotet) into the victim's system.

Once Emotet is downloaded, it will communicate with its command-and-control (C&C) server to install various modules as well as to download and execute other malware.

For the DoppelPaymer campaign, the C&C server was used to download and execute the Dridex malware family, which in turn is used to download either DoppelPaymer directly or tools such as PowerShell Empire, Cobalt Strike, PsExec, and Mimikatz. Each of these tools is used for various activities, such as stealing credentials, moving laterally inside the network, and executing different commands, such as disabling security software.

Once Dridex enters the system, the malicious actors do not immediately deploy the ransomware. Instead, it tries to move laterally within the affected system's network to find a high-value target to steal critical information from. Once this target is found, Dridex will proceed in executing its final payload, DoppelPaymer. DoppelPaymer encrypts files found in the network as well as fixed and removable drives in the affected system.

Finally, DoppelPaymer will change user passwords before forcing a system restart into safe mode to prevent user entry from the system. It then changes the notice text that appears before Windows proceeds to the login screen.

The new notice text is now DoppelPaymer's ransom note, which warns users not to reset or shut down the system, as well as not to delete, rename, or move the encrypted files. The note also contains a threat that their sensitive data will be shared to the public if they do not pay the ransom that is demanded from them.

DoppelPaymer will also drop the Process Hacker executable, its driver, and a stager DLL. DoppelPaymer will create another instance of itself that executes the dropped Process Hacker. Once Process Hacker is running, it will load the stager DLL via DLL Search Order Hijacking. Stager DLL will listen/wait for a trigger from the running DoppelPaymer process. DoppelPaymer has a crc32 list of processes and services it will terminate. If a process or service in its list is running, it will trigger the Process Hacker to terminate it.

Who are affected?

According to the FBI notification, DoppelPaymer's primary targets are organizations in the healthcare, emergency services, and education. The ransomware has already been involved in a number of attacks in 2020, including disruptions to a community college as well as police and emergency services in a city in the US during the middle of the year.

DoppelPaymer was particularly active in September 2020, with the ransomware targeting a German hospital that resulted in the disruption of communication and general operations. It also fixed its sights on a county E911 center as well as another community college in the same month.

What can organizations do?

Organizations can protect themselves from ransomware such as DoppelPaymer by ensuring that security best practices are in place. These include:

- Refraining from opening unverified emails and clicking on any embedded links or attachments in these messages.
- Regularly backing up important filesnews article using the 3-2-1 rule: Create three backup copies in two different file formats, with one of the backups in a separate physical location.
- Updating both software and applications with the latest patches as soon as possible to protect them from vulnerabilities.
- Ensuring that backups are secure and disconnected from the network at the conclusion of each backup session.
- Auditing user accounts at regular intervals — in particular those accounts that are publicly accessible, such as Remote Monitoring and Management accounts.
- Monitoring inbound and outbound network traffic, with alerts for data exfiltration in place.
- Implementing two-factor authentication (2FA) for user login credentials, as this can help strengthen security for user accounts
- Implementing the principle of least privilege for file, directory, and network share permissions.

Indicators of Compromise (IOCs)

Hash (SHA256)	Detection Name
624255fef7e958cc3de9e454d2de4ae1a914a41fedc98b2042756042f68c2b69	Ransom.Win32.DOPPELPAYMER.TGACAR
4c207d929a29a8c25f056df66218d9e8d732a616a3f7057645f2a0b1cb5eb52c	Ransom.Win32.DOPPELPAYMER.TGACAQ
c66157a916c7f874bd381a775b8eede422eb59819872fdffafc5649eefa76373	Ransom.Win32.DOPPELPAYMER.TGACAP
