Dharma Ransomware Uses AV Tool to Hide Activities

blog.trendmicro.com/trendlabs-security-intelligence/dharma-ransomware-uses-av-tool-to-distract-from-malicious-activities/

May 8, 2019

Ransomware

Trend Micro recently found new samples of Dharma ransomware using a new technique: using software installation as a distraction to help hide malicious activities.

By: Raphael Centeno May 08, 2019 Read time: (words)

The Dharma ransomware has been around since 2016, but it has continued to target and successfully victimize users and organizations around the world. One high profile attack happened in November 2018 when the ransomware infected a hospital in Texas, encrypting many of their stored records; luckily the hospital was able to recover from the attack without paying the ransom. Trend Micro recently found new samples of Dharma ransomware using a new technique: using software installation as a distraction to help hide malicious activities.

Dharma ransomware actors abuse AV tool

New samples of Dharma ransomware show that it is still being distributed via spam mail. Typical of spam, the message pressures users into downloading a file. If a user clicks on the download link, they will be prompted for a password (provided in the email message) before getting the file.

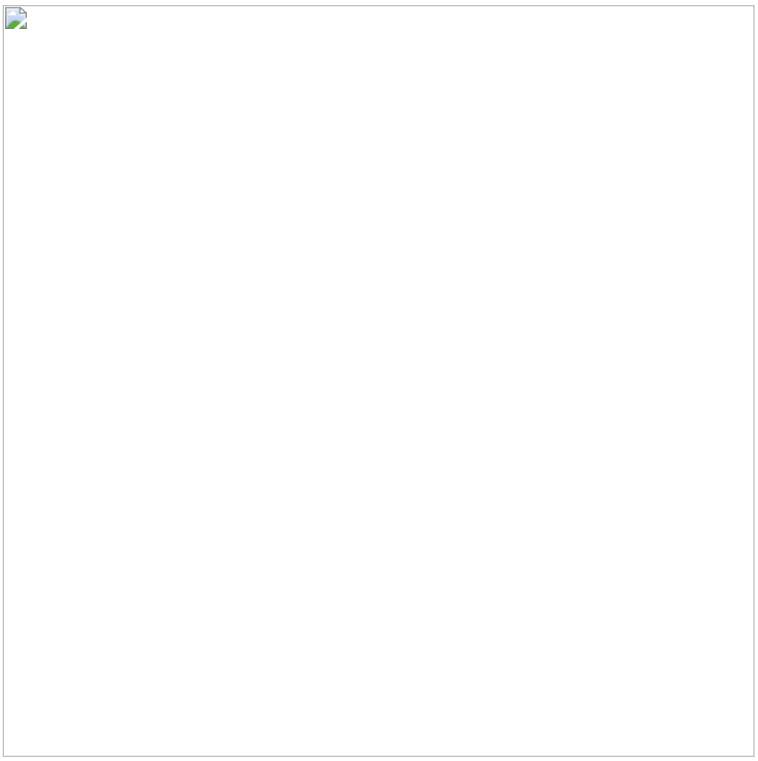

Figure 1. Dharma ransomware infection chain

The downloaded file is a self-extracting archive named *Defender.exe*, which drops the malicious file *taskhost.exe* as well as the installer of an old version of ESET AV Remover renamed as *Defender_nt32_enu.exe*. Trend Micro identifies *taskhost.exe* as a file connected to the Dharma ransomware (detected as RANSOM.WIN32.DHARMA.THDAAAI)

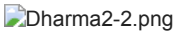

Figure 2. Spam mail for Dharma ransomware

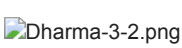

Figure 3. Running the self-extracting archive (Defender.exe)

The ransomware uses this old ESET AV Remover installer, which appears unmodified based on initial scanning, to divert attention as it encrypts files on the victim's device. When the self-extracting archive runs, Dharma starts encrypting files in the background and the ESET AV Remover installation begins. The user will see the ESET GUI onscreen, a distraction from Dharma's malicious activities.

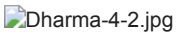

Figure 4. Software installation distracts from the ransomware's activities

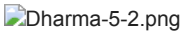

Figure 5. Software installation runs on a different instance than malware

The AV Remover is a working tool that goes through the familiar installation routine if it is executed. However, the ransomware will still encrypt files even if the installation is not started. The malware runs on a different instance than the software installation, so their behavior is not related.

The tool is legitimate software bundled with the malware, so user interaction is necessary to fully install it. The ransomware will run even if the tool installation is not triggered, and the tool can be installed even if the ransomware does not run. The installation process seems included just to trick users into thinking no malicious activity is going on.

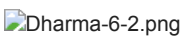

Figure 6. The ESET installer file also has a valid digital signature, so this also helps it stay under the radar

Cybercriminals have a history of abusing authentic tools, and this recent Dharma tactic of using an installer as a diversion or screen of legitimacy is simply another method they are experimenting with. This new version is designed to trick users and allow the ransomware to stealthily operate in the background. As malware authors continue to adopt layered evasion tactics and malicious techniques, users also have to adopt stronger and smarter security solutions to protect their assets.

ESET was informed of this research before publishing and issued this response:

The article describes the well-known practice for malware to be bundled with legitimate application(s). In the specific case Trend Micro is documenting, an official and unmodified ESET AV Remover was used. However, any other application could be used this way. The main reason is to distract the user, this application is used as a decoy application. ESET threat detection engineers have seen several cases of ransomware packed in self-extract package together with some clean files or hack/keygen/crack recently. So this is nothing new.
In the specific case described by Trend Micro, the ransomware is executed right after our remover application, but the remover has a dialogue and waits for user interaction, so there is no chance to remove any AV solution before the ransomware is fully executed.

How to defend against ransomware

There has been a growing awareness about ransomware as well as improved solutions for organizations and users, which contributes to ransomware's continuing decline. However, as proven by the new samples of Dharma, many malicious actors are still trying to upgrade old threats and use new techniques. Ransomware remains a costly and versatile threat; earlier this month a ransomware family was spotted targeting vulnerable Samba servers. This particular ransomware first emerged as a threat targeting victim's network-attached storage device before it evolved to target other devices.

Users and organizations should prepare for Dharma and similar threats by adopting good cybersecurity hygiene. Some best practices to follow include:

- Secure email gateways to thwart threats via spam and avoid opening suspicious emails.
- Regularly back up files.
- Keep systems and applications updated, or use virtual patching for legacy or unpatchable systems and software.
- Enforce the principle of least privilege: Secure system administrations tools that attackers could abuse; implement network segmentation and data categorization to minimize further exposure of mission-critical and sensitive data; and disable third-party or outdated components that could be used as entry points.

- Implement defense in depth: Additional layers of security like application control and behavior monitoring helps thwart unwanted modifications to the system or execution of anomalous files.
- Foster a culture of security in the workplace

Indicators of Compromise

File Name	SHA256	Detection
Defender.exe	a5de5b0e2a1da6e958955c189db72467ec0f8daaa9f9f5ccc44e71c6c5d8add4	Ransom.Win32.DHARMA.THDAAA
taskhost.exe1	703b57adaf02eef74097e5de9d0bbd06fc2c29ea7f92c90d54a0b9a01172babe	Ransom.Win32.DHARMA.THDAAA
Defender_nt32_enu.exe1	0d7e4d980ae644438ee17c1ea61ac076983ec3efb3cc9d3b588d2d92e52d7c83	normal ESET AV remover
packager.dll	083b92a07beebbd9c7d089648b1949f78929410464578a36713033bbd3a8ecea	normal
panmap.dll	9ada26a385e8b10f76b7c4f05d591b282bd42e7f429c7bbe7ef0bb0d6499d729	normal
sspisrv.dll	f195983cdf8256f1d1425cc7683f9bf5c624928339ddb4e3da96fdae2657813d	normal
sstpsvc.dll	39d3254383e3f49fd3e2dff8212f4b5744d8d5e0a6bb320516c5ee525ad211eb	normal

Content added to Folio