Inside "Phobos" Ransomware: "Dharma" Past & Underground

advanced-intel.com/post/inside-phobos-ransomware-dharma-past-underground

AdvIntel July 24, 2020

By Bridgit Sullivan

BY BRIDGIT SULLIVAN

Phobos is an increasingly dangerous and credible ransomware threat that usually targets business and occasionally customers.

What is Phobos Ransomware?

Phobos is a type of Advanced Encryption Standard (AES) ransomware that was first seen in October 2017 but became increasingly active in 2019. Also referred to as Phobos NextGen or Phobos Not Dharma, Phobos ransomware is extremely similar to the Dharma and Crysis ransomware family due to the same Dharma codebase. It is an offline file-encoding virus that targets Windows operating systems. Phobos is offered as a Ransomware-as-a-Service

(RaaS) package on the top-tier Eastern European forums. Phobos is an increasingly dangerous and credible ransomware threat that usually targets business and occasionally customers.

How Does it Work?

There are multiple ways for Phobos ransomware to end up on your device. The payload can be distributed as an attachment through traditional phishing schemes, through open and poorly secured Remote Desktop Protocol (RDP) connections, and through fake system updates. There are multiple ways that Phobos gains access to RDP connections: by using brute-force to get RDP credentials, using stolen or bought RDP credentials, or through an insecure connection on port 3389. Once deployed, the payload locks the victim's files and then places two ransom notes–one .txt and one .hta–on their desktop. In addition to locking the victim's files, Phobos deletes any shadow copies or backups of the files, as well as the system, restore point.

As soon as the victim views the .hta ransom note, which pops up automatically, negotiations can begin with Phobos operators. While most ransom notes are unique to the type of ransomware being used, the rhetoric in the ransom notes that Phobos places on the victim's desktop are identical to the one that Dharma used. The only difference between the notes is that in Phobos' ransom note they have placed their name on the note, effectively branding it as theirs.

The ransom note offers an email for the victim to contact the operator to negotiate the ransom. Once the victim has reached out, the initial response from Phobos is, again, a copy of the initial response that Dharma used. However, Phobos has added a section that aims to convince the victim to pay another 0.1 Bitcoin (BTC) for the operator to give the victim security advice, on top of the amount in BTC the victim is being asked to pay to decrypt their files. Before paying the ransom, the victim is instructed to send 5 files below a certain size to be decrypted for free.

The average ransom ranges from $5,000-$6,000, but it must be paid in Bitcoin. However, this amount is because as negotiations continue and the ransom is still not paid, the ransom is increased from the original amount of usually $3,000. The average negotiation period between a victim and a Phobos operator lasts about 8 days. This is a longer average negation period than other ransomware syndicates usually have, which could be due to unorganized and unprofessional amateur hackers using Phobos. Phobos is sold as RaaS packages on the Dark Web, which gives hackers and cybercriminals with little to no skill the ability to deploy effective and established ransomware. Victims have found that it was difficult to get their files decrypted and on multiple occasions, the decryption tool was not provided after the ransom was paid.

Phobos and the Underground

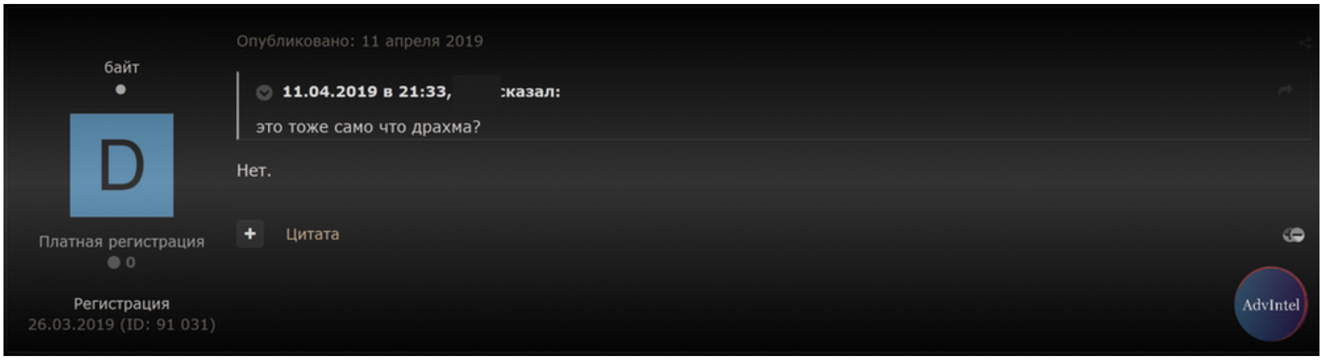
Phobos operates with a RaaS (ransomware-as-a-service) model. On April 11, 2019, with using their representative on underground forums announced that they were looking for affiliate partners to use their ransomware, Phobos. This was the beginning of a long forum thread, with posts as recent as February 2020 that give insight into how Phobos has evolved over the past year. The initial post by its representative from April of last year was meant to entice new partners to use Phobos; they detailed how the software works, how to get in touch with Phobos developers, and some of the guidelines for using the ransomware.

The post begins by describing Phobos as a “popular offline cryptolocker.” Phobos representative continues by detailing that the software is run completely offline–it does not require an internet connection to run–and while it is running it does not attract additional attention. In addition, when the infected device is turned on and off, Phobos will automatically scan for the presence of connected external and network devices, and if it finds any it will encrypt their data. The Phobos representative also discussed other aspects of their software, including its productivity, automatic functions, and file encryption. They also mentioned that this ransomware could not be used to target Russian or Commonwealth of Independent State (CIS) entities. Throughout the post, the ransomware administrator emphasized that Phobos is secure, easy to use and that there is a direct line of communication between partners and developers, no intermediaries necessary.

Despite their best effort to peddle Phobos ransomware, its representative was met with skepticism and accusations by many prominent members of the forum. In mid-April 2019, the ransomware representative responded to a post and defended Phobos ransomware. They explained that the software had been updated on April 4, 2019, and again emphasized their open channels of communication between affiliates and developers. This was not the first instance of criticism and questioning of the ransomware on the thread.

Phobos and Dharma

One prominent underground forum user brought up the similarities between Phobos and Dharma. Simply put, the user asked if this ransomware was also Dharma. The ransomware representative quickly responded that it was not. In May 2019, over a month after this exchange, the Phobos representative posted that a new software update had been released and that they were continuing to recruit affiliate partners. They were again met with comments that Phobos and Dharma are the same, this time by the GandCrab themselves.



Опубликовано: 11 апреля 2019

байт

Платная регистрация

0

Регистрация
26.03.2019 (ID: 91 031)

11.04.2019 в 21:33, [redacted] сказал:

это тоже само что драхма?

Нет.

Image 1: Phobos team denies being the same as Dharma. This denial triggered harsh responses from the community, illustrating the toxicity and over-competitiveness of the current ransomware black market.

Following this criticism, the ransomware representative posted a longer explanation of the differences between Dharma and Phobos in June of 2019. According to the group's spokesperson, Phobos is based on Dharma, but it is "written from scratch" and offers better security. They again emphasize that Phobos is constantly being updated and improved.

Two months later, on June 16, 2019, the ransomware representative again updated the thread and described the Phobos' new update. They referred to the update at "version 2.7." They described the update as:

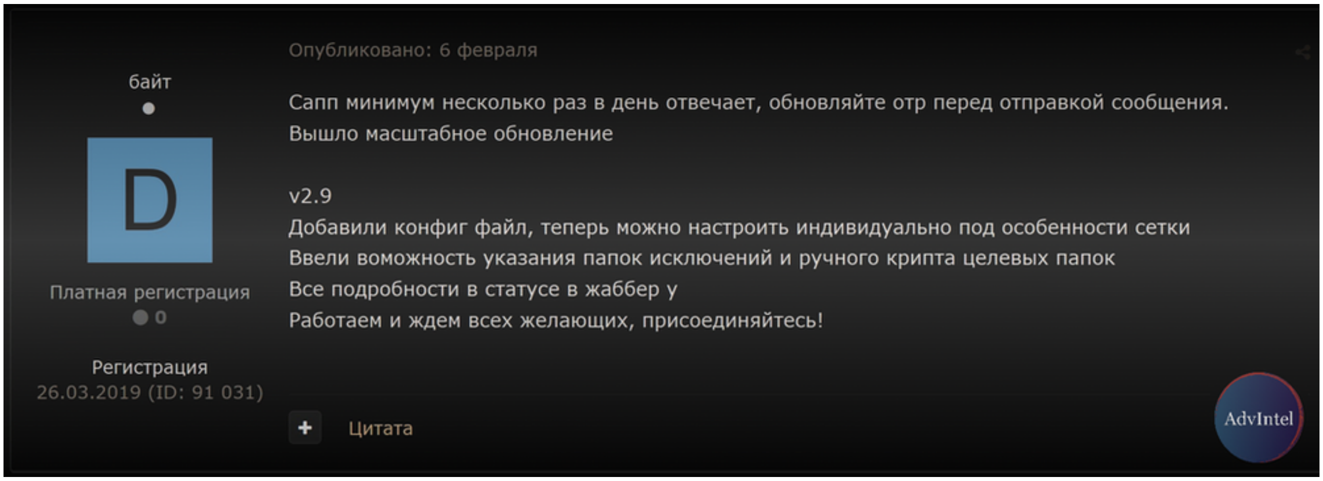
- Stable offline cryptolocker, written in C++ without STL, MSIL, CRT.
- Encrypts with the AES256 algorithm.
- Encrypts local, removable drives and network folders.
- There is the possibility of full and partial encryption.
- Deletes shadow copies and restore points.

- Closes processes blocking access to files.
- File size:
- 54kb (standard configuration with HTML page)
- 47kb (standard configuration without HTML page)
- It has a flexible configuration system, according to your desire you can configure:
- Lists of files that are encrypted
- Lists of critical files that are encrypted in the first place
- Disable partial encryption for critical files
- Lists of exceptions
- Lists of programs that need to be closed
- Bypass UAC, launch offers from the administrator, or work with the privileges with which it was originally launched
- Secure file deletion after encryption
- A message in the form of a text file, in the form of HTML, or both
- Message text and HTML code
- If you have [large] volumes [of access logs and credentials], we can modify the software to your needs.

Again, the ransomware representative encouraged interested parties to reach out to them via Jabber.

On February 6th, of this year, Phobos team again posted outlining the newest update to Phobos, “version 2.9.” This update added a configuration file and the option for users to specify exclusion files. The thread ends on February 11, 2020, when the representative again works to defend Phobos from critics and reiterate that the developers are always available through Jabber.

This is currently the latest version of this ransomware.



Опубликовано: 6 февраля

Сапп минимум несколько раз в день отвечает, обновляйте отр перед отправкой сообщения.
Вышло масштабное обновление

v2.9
Добавили конфиг файл, теперь можно настроить индивидуально под особенности сетки
Ввели воможность указания папок исключений и ручного крипта целевых папок
Все подробности в статусе в жаббер у
Работаем и ждем всех желающих, присоединяйтесь!

Image 2: Phobos team advertises the latest 2.9 version of the ransomware. The highlights include modular configuration as well as manual encryption folders of interest.

Conclusion

As one can see from the forum threads, Phobos is continuously evolving to be more effective while simultaneously recruiting new users. From previous accounts of negotiations, many Phobos operators are unskilled or unprofessional, but that does not make the use of this ransomware any less dangerous. As Phobos continues to evolve, there may be more updates to come on the ransomware in the coming months and throughout the year.

Indicators of Compromise (IOCs) (MD5) [1]

e59ffeaf7acb0c326e452fa30bb71a36

eb5d46bf72a013bfc7c018169eb1739b

fa4c9359487bbda57e0df32a40f14bcd

[1] https://blog.malwarebytes.com/threat-spotlight/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name/

Bridgit graduated with her B.A. in Political Science and Russian and Eastern European Studies, with a minor in Spanish, in June of 2020. In the future, she hopes to earn a J.D. and a graduate degree in Political Science or Global Affairs. While working with Advanced

Intelligence, LLC, her research has focussed on threat actors and the nexus between cybersecurity and humanitarianism.