|  |  |  |
| --- | --- | --- |
| ALERT 15.02.2024UNCLASSIFIED | Backmydata Ransomware | Icon  Description automatically generated |

During the night of 11 to 12 February 2024 there was a ransomware cyber attack on the Romanian Soft Company (RSC) [www.rsc.ro](http://www.rsc.ro), which develops, manages and markets the **Hippocrates computer system (a.k.a. HIS)**. According to DNSC data, the attack disrupted the activity of **26 Romanian hospitals** which used the **Hippocrates** IT system:

1. Pitesti Pediatric Hospital
2. Buzău County Emergency Hospital
3. Slobozia County Emergency Hospital
4. Pitești County Emergency Hospital
5. Târgovişte County Emergency Hospital
6. “Dr. Constantin Opriş” County Emergency Hospital Baia Mare
7. The County Emergency Clinical Hospital "Sf. Apostol Andrei" Constanţa
8. Colțea Clinical Hospital, Bucharest
9. “Dr. Alexandru Gafencu” Military Emergency Hospital Constanța
10. Sighetu Marmației Municipal Hospital
11. Medgidia Municipal Hospital
12. Azuga Orthopedics and Traumatology Hospital
13. Băicoi City Hospital
14. Emergency Clinical Hospital Plastic Surgery, Reparatory and Burns Bucharest
15. C.F. Clinical Hospital no. 2 Bucharest
16. Chronic Disease Hospital Sf.Luca
17. Hospital of Pneumophysiology Roșiorii de Vede
18. Fundeni Clinical Institute
19. Institute of Cardiovascular Diseases Timișoara
20. Institute of Fonoaudiology and Functional Surgery ORL “Prof. Dr. D. Hociotă”, Bucharest
21. Oncological Institute "Prof. Dr. Al. Trestioreanu" Bucharest (IOB)
22. Iaşi Regional Institute of Oncology (IRO Iasi)
23. Sanatorium of Pneumophysiology Brad, Hunedoara
24. Medical Center MALP SRL Moinești
25. Santa Clinic Mitreni Medical Center (jud. Călărași)
26. Smeeni Chronic Disease Hospital, Buzău

BACKMYDATA

The malware used in the attack is **Backmydata ransomware application** that is part of **the Phobos malware family**, known for propagating through **Remote Desktop Protocol (RDP) connections.**

**Backmydata** is designed to encrypt target files using a complex algorithm. Encrypted files are renamed with the extension **.backmydata**. After encryption, the malware provides **two ransom notes (info.hta** and info.txt**)** with details **of** the steps to be followed to contact the attackers and determine the details for the ransom payment.

**The Phobos ransomware family evolved from Dharma/Crysis ransomware, and since it was first observed in 2019, it has undergone minimal changes despite its popularity among cyber attacker groups**[[1]](#footnote-2)**.**

**Phobos is a Ransomware-as-a-Service (RaaS) where developers and affiliates are not closely linked, but collaborate to distribute malware on a large scale, targeting various organisations and individuals. Phobos is noted for its evasion techniques and the use of simple but effective mechanisms to achieve operational objectives. Its decentralised structure complicates efforts to counter its operations and identify attackers.**

**Common variants of Phobos (such as Eking, Eight, Elbie, Devos and Faust) demonstrate the adaptability and diversity of this ransomware family. Affiliates use similar Tactics, Techniques, and Procedures (TTPs) to implement Phobos, which typically has the objective of infecting servers with an important role in the target infrastructures, in order to exert pressure on victims to pay the ransom.**

**In Romania, the health sector was also targeted in 2019 and 2021 by complex financially motivated cyberattacks involving the use of Phobos malware**[[2]](#footnote-3)**.**

**Phobos encrypts the data using the AES 256 algorithm**[[3]](#footnote-4) **for multiple extension files and sends a ransom note in the following form:**



**In the case of Romanian hospitals ransomware attack with Backmydata we have no indication of data exfiltration so far.**

**In popular versions, Phobos stops its execution and self-eliminates itself from storage devices if it identifies the use of Cyrillic characters in the operating system, which is common to Russian-speaking malware developers.**

**Attackers use the *getsession* platform in communication with victims. The application uses end-to-end encryption and decentralised architecture to guarantee privacy and reduce the risk of interception of messages.**

RECOMMENDATIONS

The **Directorate strongly recommends that no one pays the ransom to the attackers!** The payment of the ransom does not guarantee that the data will be recovered and encourages cybercrime.

**We recommend the implementation of the following specific cybersecurity measures:**

* **Limiting the use of RDP service on network stations and servers and taking additional measures to secure this type of service;**
* **Using complex passwords and changing them periodically;**
* **Making backups of critical data and storing it either offline or on a different segment of the network;**
* **Isolating and retaining encrypted data in the event that an online decryption application could occur.**

**We recommend the implementation of the following general cybersecurity measures:**

* **Increased vigilance,** which is the main asset available to an ordinary user at any time. Attention should be paid to verifying incoming emails, especially those containing suspicious attachments or links!
* **Scan with a security solution** installed on your device, or one available for free online, for **suspicious** **links or attachments** in your mailbox. Don't forget to apply the updates to these security solutions on time!
* **Suspicious emails should be reported to the IT department** for isolation and investigation. Periodically check the rules of your email account, which can be set for automatic forwarding of all messages, which could lead to a data leak if there is an infection.
* **Emergency update of operating systems**, antivirus software, web browsers, email customers and Office programs.
* **Access to the network should be continuously monitored** by those responsible in IT departments, thus it can be determined in a timely manner whether an infection with **a malicious program** has occurred.
* **Installing an application control solution.** System administrators may consider installing such software that provides white list of applications and/or directories. Thus, only approved programs are allowed to run, while others are restricted, being a good security practice in protecting an IT system.
* **Create system restoration points and back-up files. It is recommended to periodically create such restoration points and back-up for important files using a portable or cloud storage medium. Thus, it is possible to return to an uninfected state of the system or quickly recover files in case of a successful infection or malfunction of the system.**
* **Regular training sessions with staff. They are necessary for both awareness/prevention and to know what to do in cases where cybersecurity incidents happen so that they are managed effectively.**
* **Do not hesitate to contact the Directorate**, if you suspect that devices within your entity have been compromised or you are subject to a cyber attack.

**alerts@dnsc.ro**

Phone 1911

1. [Understanding the Phobos affiliate structure and activity](https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/) [↑](#footnote-ref-2)
2. [Cyberattack with the Phobos ransomware app (sri.ro)](https://www.sri.ro/articole/atac-cibernetic-cu-aplicatia-ransomware-phobos) [↑](#footnote-ref-3)
3. Algorithm for which there is no decryption method [↑](#footnote-ref-4)