Cyber threat advisory | Phobos ransomware launches new leak site and pivots towards double extortion

s-rminform.com/latest-insights/cyber-threat-advisory-phobos-ransomware-launches-new-leak-site-and-pivots-towards-extortion

Melissa DeOrio, Frank de Korte, Charlie Walker-Arnott

S-RM

21 May 2024

4 min read

In April 2024, S-RM's Cyber Threat Intelligence team identified a Faust operator, an affiliate of the Phobos ransomware-as-a-service group, utilising a new leak site, titled 'Space Bears', to extort a victim for a ransom payment. The emergence of the site follows other observations of Faust operators using the 8Base leak site as a place to post victim data. The discovery of the new site showcases Phobos ransomware teams' pivot toward data-theft and double-extortion to monetise their business.

Phobos operations

Since May 2018, the Phobos ransomware operation has amassed victims across the planet. It has historically targeted small to medium sized companies, often finding a foothold in an organization through unprotected or poorly protected Remote Desktop Protocol systems. A variant of the once-prevalent Dharma locker, Phobos locker is deployed under a Ransomware-as-a-Service (RaaS) operation, with versions of the malware being licenced out to separate teams, extort victims, and give the RaaS operators a cut of the profits. Some of the biggest names among these disparate teams, as identified by the extension on locked files, are the Faust, BlackRock and Devos groups.

In recent years, Phobos attacks have been characterised by two quirks rarely seen among modern day ransomware groups.

1. **Per-system extortion approach:** a new victim finds their files locked, with an email address and a unique-per- system ID appended to the filename. The ransom demand then depends on the total number of unique IDs provided. If a victim only needs to unlock one system, they receive a lower ransom demand, typically between USD 10,000 and USD 20,000. But unlocking more systems means paying more money.
2. **Historic disavowal of "double-extortion":** despite the tactic (threatening to publish stolen data as a second method of putting pressure on a victim) being de rigueur for years among big ransomware groups, Phobos has historically avoided the approach. In June 2023, an S-RM client even received the following assurance from the Faust team: "Your data is safe. We have not, and never do take data. You need not worry". Phobos victims could at least find some comfort knowing that, whatever other havoc the group had wreaked on their systems, they need not worry about data publication.

Despite these historical differentiators, since late 2023 Phobos operators have changed their habits and launched themselves into data extortion.

New leak site in Cy-Bear Space

S-RM has recently seen data obtained by the Faust team appear on the leak site of 8Base, a ransomware group whose activity began ramping up in mid-2023. Intelligence gathered surrounding the 8Base operations reveal that their site appears to be a 'leak site for hire', next to their own ransomware deployments, where other groups can 'partner' up with the organisation to host their stolen data for double extortion purposes. Other Incident Response parties have identified that data exfiltrated from a Phobos attack, locking files with the ".8base" extension, have later ended up on 8Base's site.

Following this, in February 2024 the US Cybersecurity and Infrastructure Security Agency (CISA) published a Joint Cybersecurity Advisory piece1 on Phobos' current operations, which signalled a move into double extortion for the first time. This advisory reported that various contributors had seen Phobos exfiltrating data, using tools such as MegaSync to upload data to an external cloud service.

Space Bears

Beginning in April 2024, S-RM has encountered the Faust operator sharing stolen data on a new leak site. This leak site is hosted on an Onion URL and uses the title 'Space Bears' (see Figure 1). While intelligence gathered suggest that other Phobos teams use this leak site to host the stolen data, it remains to be seen whether this is now the exclusive data leak site for the Phobos teams' operation. But what is clear is that the Phobos operation and the Faust team especially has moved firmly into the realm of double extortion.

Figure 1: Space Bears leak site logo.

At the time of writing, the leak site mentions 8 victims, with some posts already hosting stolen data.

So what?

The Phobos operation moving into double-extortion is a continuation of a trend: the encryption-only business model is over. Increasingly, ransomware groups have been more focused on data exfiltration than actual encryption as the primary method of extortion due to a high viability of payouts for stolen data. Organisations have become better at managing their backups, allowing them to recover in full after a devasting ransomware attack. It is likely that Phobos saw their success rates fall the last few years and made a choice to pivot into data exfiltration to continue earning money from their attacks.

This does mean that in cases where Phobos uses data exfiltration, victims may need to consider the implications of having their data accessed or stolen. Combined with the rise of criminal groups like Karakurt and BianLian performing data theft only as the primary extortion factor, organisations should take extra care to manage their sensitive data as well as their perimeter, to avert getting ransomed in the first place, but also to avoid having to pay a ransom.

Protection

The heightened focus on data theft across the ransomware ecosystem requires organisations to prioritise securing sensitive data to limit business impacts following an incident involving data-loss. Organisations can implement several measures to protect themselves against the impact of data theft. We recommend the following be implemented:

- Encrypt sensitive data in transit and at rest to prevent unauthorised access, in the event that sensitive data is intercepted by a third party.
- Implement strong Data Governance policies. Often organisations are not aware of the amount of data still available within their estate, especially years-old (ex-)employee records and sensitive personal identifiable information. Periodically deleting stale data according to a sensible data retention policy reduces the privacy impact that can occur from data theft.

- Regularly scan and monitor public-facing interfaces. Often Remote Desktop Protocol ports are opened by accident or misconfigurations, resulting in these far-reaching consequences. Quickly identifying these gaps will allow organisations to respond in time to this threat.
- Implement an Endpoint Detection and Response (EDR) solution across the estate. An EDR will help organisations with timely detection of malicious activity on systems, allowing for rapid response to prevent larger impact.

Please do not hesitate to contact S-RM if you have any questions on this development.

Subscribe to our insights

Get industry news and expert insights straight to your inbox.