▸ Thanos ransomware: criminal and disruptive attacks
  ▸ Key Points
  ▸ Summary
  ▸ Comments
  ▸ References

Thanos ransomware: criminal and disruptive attacks

Threat Memo - Date: 20/10/2020 - Version: 1.0

TLP:WHITE

	Category	Type	Domain(s)	Sector(s)	Confidence
FOR INFORMATION	Cybercrime, Cyberwar	Ransomware, Wiper	[EU], [World]	Pharmaceutical, Legal, Finance, Business services, Retail, Healthcare, Government	A1

Key Points

- Thanos is a ransomware-as-a-service offer used by different threat actors.
- A variant was used for financial gain against various victims in Europe in June 2020.
- Another variant was used in the Middle East and North Africa in July 2020.
- Israeli researchers believe that the Iranian MuddyWater state-sponsored threat actor may also have used a variant of Thanos against prominent Israeli entities in September.

Summary

According to the security firm RecordedFuture[1], Thanos is a ransomware-as-a-service offer that was first advertised for sale on underground forums in January 2020, by a threat actor with the alias “Nosophoros.” Thanos consists of a private ransomware builder that allows to generate new clients based on 43 different configuration options. Thanos variants are hence

highly likely to be used by multiple threat actors. This ransomware is currently under active development.

According to Proofpoint[2], in June 2020 a variant of Thanos, dubbed Hakbit, was used in a campaign targeting organisations in Austria, Switzerland, and Germany. Attackers demanded a payment of 250 Euros in bitcoin to unlock the encrypted files and provided instructions on how to pay the ransom. Victims belonged to the pharmaceutical, legal, financial, business service, retail, and healthcare sectors.

In early July 2020, according to Palo Alto Networks (PAN)[3], a Thanos disruptive ransomware campaign targeted two state-run organisations in the Middle East and North Africa. The attackers used a variant of Thanos that can overwrite the master boot record (MBR), preventing the victims from booting their systems. Fortunately, in these particular cases, the code responsible for overwriting the MBR had a bug: the ransom message contained invalid characters which caused an exception and thus stopped the malware operation. This left the MBRs intact, allowing systems to boot correctly.

While PAN cannot confirm the connection, they believe the actors who deployed the Thanos ransomware at the Middle Eastern organisations indicated above, also used a downloader they called PowGoop.

On October 15, the Israeli security firm ClearSky reported[2] that, in early September 2020, they had detected a PowGoop malware campaign targeting many prominent Israeli organisations. ClearSky has attributed the campaign to the Iranian threat actor Muddywater (aka TEMP.Zagros, Static Kitten, Seedworm). ClearSky also inferred from this PowGoop observation that the threat actor possibly had the objective to deploy the Thanos ransomware. In this Israel-focused campaign, attackers used two delivery tactics: (1) an exploit-based vector - they exploited known vulnerabilities in OWA and Microsoft Exchange servers (in particular CVE-2020-0688), or the ZeroLogon Windows vulnerabilities (CVE-2020-1472), (2) a social engineering-based vector - attackers delivered documents with embedded malicious macros.

Comments

The Thanos campaign of June 2020 in Austria, Switzerland, and Germany, as well as the July 2020 attacks in the Middle East and North Africa are likely motivated by financial gain. It is however worth noting that the technique used in July, overwriting the MBR, is a more destructive approach to ransomware attacks than file encryption, the technique used by large majority of ransomware families. The most notable of piece of ransomware overwriting the MBR was Petya in 2017. In the Petya case, the objective of the attackers was likely not financial gain. It was rather to cause targeted disruptions while obfuscating this goal within additional, indiscriminate attacks which were made possible by the worm nature of the malware.

As regards the September 2020 campaign attributed to MuddyWater, researchers have already reported on the active exploitation of ZeroLogon by this group. Since its inception in 2017, the primary goal of MuddyWater has been cyberespionage. If the link between their

recent campaign in Israel in September 2020 and the use of the Thanos ransomware variant (with MBR overwrite features) is confirmed, that would indicate an extension of the group's objectives towards disruptive operations.

References

1. https://www.recordedfuture.com/thanos-ransomware-builder/
2. https://www.proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland
3. https://unit42.paloaltonetworks.com/thanos-ransomware/
4. https://www.clearskysec.com/operation-quicksand/