Major web hosting providers become victims of ransomware

Reference: Memo [191114-1] – Version: 1.0
Keywords: ransomware, web hosting provider, managed service provider, disruption, extortion, SmarterASP
Sources: open sources

Key Points

- Outsourcing IT services such as web hosting, managed service providers and cloud service providers could increase the exposure of organisations to ransomware attacks.
- In 2019, over 10 web provider companies have already been victims of targeted ransomware incidents.
- Since the largest known paid ransom was from a web-hosting provider, cybercriminals will likely increase their efforts.

Summary

As reported[1] on 11 November, SmarterASP.NET, a major ASP.NET company with more than 440.000 customers, was hit by ransomware. Next to other smaller companies and organisations, SmarterASP.NET was the third major web hosting firm that went down because hackers breached their network and encrypted data on client servers. The attack did not just hit customer data, but also SmarterASP.NET itself. The company's website was down all for at least one day. While most users were using SmarterASP.NET for hosting ASP.NET sites, others using the company's servers as app backends to where they synchronised or backed up important data. The fact that not just public-facing web servers but also backend databases were hit prevented many clients from moving impacted services to alternative IT infrastructure.

Beside SmarterASP.NET, in July this year a second major web hosting provider iNSYNQ was infected by a version of the MegaCortex ransomware (see memo [190726-1]). The company is a cloud computing provider of virtual desktop environments. Furthermore, A2 Hosting, a well-known company offering a variety of hosting services, was hit in May. Its servers in Asia and North America were encrypted by a version of the GlobeImposter 2.0 ransomware. Both A2 and iNSYNQ took weeks to restore and fully recover customer data. Due to the sheer size of its customer base, SmarterASP.NET is likely to have a similar recovery timeline.

The table in the annex provides a list of recent high profile ransomware incidents that have hit managed service and web hosting providers in 2019.

Comments

Companies offering managed or hosted services are especially attractive for cybercriminals because they cannot afford to lose customers due to disruption of access to their services. According to ZDNet.com, until this date the largest ransomware payment ever made came from a web-hosting provider. In 2017, the South Korean web hosting company Nayana reportedly paid the amount of $1,14 million (worth of bitcoins) to cybercriminals following a ransomware attack.

Therefore, it should not be surprising that ransomware criminals are likely set to increase their effort to continue targeting such companies. Outsourcing IT services such as hosting and management could hence increase the exposure of organisations to ransomware attacks.

Nowadays, advanced cybercriminals executing ransomware attacks actively search for and delete backups prior to deploying ransomware. In this context, organisations should consider offsite backups as critically important. Organisations are advised to evaluate their back-up strategies regularly and perform assessments to ensure that their recovery is successful. Organisations should also implement strong authentication (i.e. multifactor) to access their managed or outsourced services.

[1] https://www.zdnet.com/article/major-asp-net-hosting-provider-infected-by-ransomware/

Date (2019)	Victim	Sector	Provider Type	Ransomware
November	SmarterASP		• Web-hosting provider	Unidentified
November	ConnectWise		• Technology solutions providers (TSPs) • Business-as-a-service business	Unidentified
October	Carolina Data Systems		• Managed services providers (MSP)	Unidentified
October	TrialWorks	Legal	• Documents management service provider	Unidentified
September	SCHOOLinSITES	Education	• Web-hosting provider • Content management service provider	Unidentified
August	PerCSoft	Dental clinics	• Records management service provider	REvil
August	22 Texas municipalities	Municipalities	• Software used by MSP exploited to infect networks	REvil
August	Continuum - Unidentified MSP		• Managed service provider	Unidentified
July	iNSYNQ		• Cloud service provider	MegaCortex
May	A2 Hosting		• Web-hosting provider	GlobeImposter 2.0