Waves of ransomware in December 2019

Threat Memo - TM 20-002 - Date: 06/01/2020 - Version: 1.0

TLP:WHITE

	Category	Type	Domains	Sectors	Confidence
FOR INFORMATION	Cybercrime	Ransomware	[EU] [EU near] [World]	Academic/University, Industrial, Telecoms, Managed service provider, Cloud service provider, Maritime services, Government/Administration	A1

Key Points

- Several high-profile ransomware attacks were observed in December 2019.
- Public and private organisations in several countries and sectors have been affected.
- In two cases, the ransom note reached $6M, the highest amount reported so far.
- In two cases, cybercriminals have leaked data belonging to their victim in an attempt to force the payment of the ransom.

Summary

In December 2019, distinct cybercriminal groups compromised the networks of different high profile public and private organisations to deploy ransomware. Victims are located in the US, Canada, Spain, the Netherlands, Germany, Australia and Argentina. They belong to various sectors including local governments/administrations, universities, managed service providers, cloud hosting services, maritime services, telecoms, and industry.

The most observed ransomware families have been Maze, Ryuk and Clop. In most cases, the amount of ransom demanded by cybercriminals has not been disclosed. However, according to reports, it reached the amount of $6M in at least two cases.

In two cases, cybercriminals used a new tactic in an attempt to force their victim to pay the ransom note: in addition to encrypting files to render them unusable, cybercriminals exfiltrated data and began to leak (portion of) the data.

The table in annex provides details on the most important ransomware cases in December 2019.

Comments

This series of attacks concludes a year marked by the emergence of a tactic called “big game hunting” (BGH, see memo [190916-1]). This scheme combines advanced, targeted attack techniques with ransomware to achieve substantial financial payoffs.

In the December series, a managed service provider (MSP) was again the victim of a ransomware attack. This MSPs’ targeting confirms another trend observed in 2019: an unidentified MSP in August, healthcare MSPs in August and November, Carolina Data Systems in October, and CyrusOne in December.

As regards maritime services, it is worth mentioning that already in 2018, the ports of San Diego (US) and the port of Barcelona (Spain) had reported ransomware infections within five days of each other (September 2018). Both incidents were later revealed to have been caused by the same Ryuk ransomware family.

Cybercriminals operating the Ryuk ransomware (one of the most active ransomware in 2019) are also known to have established a pattern of breaching educational entities, and the recent compromise of a German university indicates that this trend persists and extends beyond the US.

To infect their victims with ransomware, cybercriminals are using various techniques. In the case of Ryuk, cybercriminals have been deploying the Trickbot malware which serves as a first stage dropper for Ryuk. The Switzerland based non-profit organisation Abuse.ch has shared statistics on the Trickbot infections[1], indicating that almost a quarter of them are located in the US.

Finally, the leakage of (a portion of) data belonging to the victim, a new tactic employed by cybercriminals behind the Maze ransomware, could plausibly inspire other cybercriminals in 2020.

[1] https://twitter.com/abuse_ch/status/1208031390694092800

Annex

High profile ransomware attacks – December 2019

Date	Country	Sector	Amount	Malware	Comment
Dec 23	NL	Academic / University		Clop	**Maastricht University** became the victim[2] of a Clop ransomware infection that affected all of its Windows operating systems.
Dec 19	US	Cloud hosting Managed services	$6M	rEvil / Sodinokibi	**Synoptek**[3] (which provides services to more than a thousand customers nationwide) was infected by the rEvil ransomware. The company has reportedly paid a ransom demand.
Dec 18	CA	Insurance			In December, open sources reported[4] that an **insurance and financial services company** based out of Manitoba, Canada had been victim of the Maze ransomware with allegedly 245 computers encrypted during a cyberattack in October.
Dec 16	US	Maritime		Ryuk	A Ryuk ransomware infection affecting a **civil port authority** facility led to a disruption of camera and physical access control systems, and loss of critical process control monitoring systems[5].
Dec 14	US	Healthcare			**New Jersey's largest hospital** system announced that a ransomware attack disrupted its computer network and that it paid a ransom to stop it[6].
Dec 14	AU	Government / Administration			The **city of Onkaparinga** disclosed a Ryuk ransomware infection[7].
Dec 13	US	Government / Administration		Ryuk	The **city of New Orleans** became the victim of the Ryuk ransomware[8].
Dec 12	US	Cable manufacturer	$6M	Maze	Maze Ransomware operators claimed responsibility for a cyberattack against wire and cable manufacturer **Southwire**. After a ransom of 850 bitcoins, ($6 million) was not paid by Southwire, the cybercriminals published[9] a portion of their stolen data on a "news" site that the threat actors created.
Dec 8	DE	Academic / University		Ryuk	According to the Prosecutor General's Office in Frankfurt, the **University of Giessen** was breached[10] with Ryuk ransomware. Disruptions included inoperability of email and internet, as well as the inability to provide students with "degree certificates, transcripts of record or any other examination certificates."
Dec 6	US	Government / Administration		Maze	Around Dec 6, the **city of Pensacola** became the victim of a ransomware attack. By Dec 23, the cybercriminals purportedly released documents and data amounting to 2GB that allegedly originated from the city of Pensacola, likely as leverage toward the monetisation of the infection[11].
Dec 2	AR	Government / Administration			The San Luis Province in Argentina[12] provided details of a ransomware compromise of a local data center, which reportedly affected some provincial government information.
Nov 27	ES	Physical and digital security services	0.5 BTC per day of delay	Ryuk	**Prosegur**, a multinational provider of physical and digital security services, became the victim of the Ryuk ransomware. Cyber-physical assets, including ATMs, security alarms, and geolocation tracking devices, were reportedly unavailable for several days.

[2] https://www.maastrichtuniversity.nl/news/update-cyber-attack-um
[3] https://krebsonsecurity.com/2019/12/ransomware-at-it-services-provider-synoptek/
[4] https://www.bleepingcomputer.com/news/security/canadian-insurance-firm-hit-by-maze-ransomware-denies-data-theft/
[5] https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/
[6] https://nj1015.com/nj-largest-hospital-system-forced-to-pay-ransom-in-cyber-attack/
[7] https://www.adelaidenow.com.au/
[8] https://www.bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/
[9] https://www.bleepingcomputer.com/news/security/maze-ransomware-sued-for-publishing-victims-stolen-data/
[10] https://www.uni-giessen[.]de/index.html
[11] https://krebsonsecurity[.]com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/
[12] http://agenciasanluis.com/notas/2019/12/02/la-provincia-hara-una-denuncia-penal-por-el-ciberataque-al-data-center/