Coordinated ransomware campaign in Spain

Reference: Memo [191015-1] – Version: 1.0
Keywords: Spain, Ryuk, ransomware, big game hunting.
Sources: Publicly available sources.

Key Points

- Ransomware is targeting municipalities in Europe.
- Multiple entities in Spain have seen significant outages because of the threat.
- These attacks can be seen as a continuation of the Big Game Hunting tactics observed elsewhere in the world.

Summary

A targeted ransomware campaign has affected multiple municipalities in Spain. Reportedly[1], the campaign started with a massive spear-phishing email campaign directed against various institutions and public entities in the Basque Country, several of which were severely affected by the ensuing ransomware infection. After that, the municipal government of Jerez in Andalusia announced that it had been hit by ransomware[2]. This incident was also preceded by a wave of Emotet malicious spam messages (malspam). The infected institutions became non-functional for a period of time, until all relevant equipment could be checked and brought back online. According to available reports, no ransom was paid.

Comments

In all of these cases, the debilitating attack reportedly begun with a high intensity Emotet email campaign. Emotet started out as a banking trojan in 2014 but has now developed a capability to spread additional malware and serves mainly as the delivery vector for other, more sinister payloads. Emotet can spread locally on a network. It also steals user credentials from other applications and tries to spread further by emailing itself to contacts found in the infected computer's address book.

The Ryuk ransomware, reportedly affecting Jerez, has a history of targeting private and public entities in 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. BGH impacts both private and public sectors and the typical targets are organisations that cannot afford to have any downtime. Ryuk is exactly such a type of threat, combining advanced automated attack techniques with manual hacking. According to Crowdstrike[3], in only four months, since Ryuk's appearance in August 2018 and until January 2019, the threat actors operating it netted over 705,80 BTC across 52 transactions for a total current value of 5.316.078,70 Euro. With the many Ryuk infection cases reported in 2019, the revenues generated by this malware have likely gone much higher since January 2019.

The Ryuk campaign in Spain is likely the first coordinated ransomware campaign targeting multiple European public entities at the same time. Previous efforts in Europe involving either Ryuk or some other ransomware have been limited to single entities, such as a municipality in Finland, a public administration in Ireland or a Norwegian aluminium producer.

In the US however, such coordinated campaigns targeting multiple municipalities and hospitals have unfortunately become quite common.[4]

Even if only few victims pay up, it is evident that ransomware is earning their distributors millions of euros. This makes holding someone else's files for a ransom a very lucrative business and is thus unlikely to go away in the foreseeable future.

For more on Emotet, please see CITAR-Flash-2019-017 (TLP:GREEN) and CITAR-Flash-2019-38 (TLP:AMBER).

[1] https://www.deia.eus/2019/10/01/sociedad/euskadi/un-ataque-masivo-de-correos-con-virus-afecta-a-diversos-entes-publicos-vascos
[2] https://andaluciainformacion.es/andalucia/851395/los-tecnicos-del-cni-confirman-que-no-hay-fuga-en-las-bases-de-datos/
[3] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
[4] https://www.bleepingcomputer.com/news/security/dch-hospital-pays-ryuk-ransomware-for-decryption-key/