CNS CYBER INTELLIGENCE REPORT

Threats/vulnerabilities: Trends in ransomware attacks against legal and accountancy sector, April to June 2020

Date of issue: 02/07/2020
Reference Number: TF.20.036

Context

CNS analysed data publicly available for ransomware attacks believed to have been conducted or reported between 2nd April and 30th June 2020. This report provides analysis of the trends and tactics observed in ransomware attacks globally which were against organisations in the legal and accountancy sector.

Key Points

- Legal and accountancy is the third most targeted sector by ransomware between April and June 2020, two UK organisation's targeted out of 12 total attacks worldwide.
- All ransomware attacks in that period featured 'double extortion': encrypting the network and leaking stolen data publicly
- Stolen data being sold online by ransomware groups and advertised on social media may be first public indication of an attack
- Sodinokibi ransomware responsible for more attacks against legal and accountancy sector; group have website dedicated to auctioning off stolen data from attacks

Analysis of ransomware attacks

1. Ransomware is a form of cyber-attack, normally carried out by criminal groups for financial gain. A target organisation's network is penetrated by the attackers, either through sending an email to persons in the organisation that contains malicious software (malware) or through exploiting a vulnerability in the organisation's network. The malware enters the network and the attackers conduct reconnaissance and further activity to achieve the right access and accounts to execute the ransomware. Once this is done, the target organisation's network is encrypted and effectively unusable until either a ransom is paid or the organisation reverts to backups to bring the network online.
2. CNS surveyed publicly reported ransomware attacks in second quarter 2020, from 2nd April to 30th June. Figure 1 shows the most targeted industries in Q2:

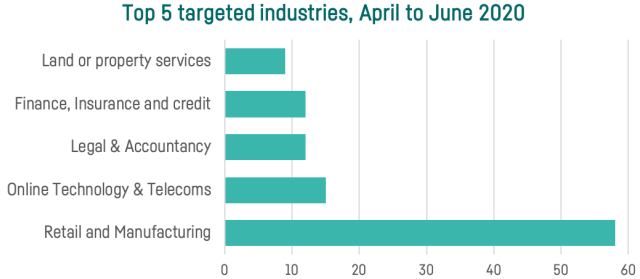

Figure 1 - The five most targeted industries by ransomware April to June.

3. The legal and accountancy sector was the third most targeted by ransomware, with the sector being targeted in 8% of all ransomware attacks. Of the twelve attacks against the legal and accountancy sector, two were against UK-based firms.

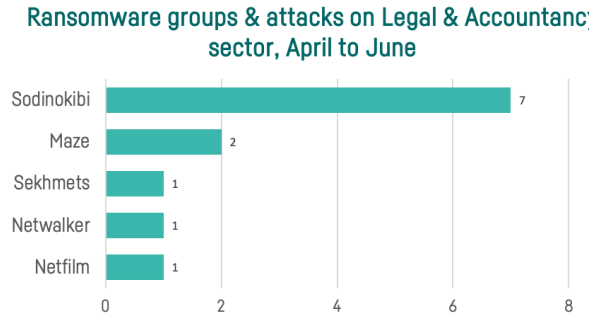

Figure 2 - Number of ransomware attacks against legal and accountancy sector attributed to ransomware groups.

4. All of the ransomware attacks against legal and accountancy were performed by groups that commit 'double extortion' – please see figure 3:

Figure 3 - Overview of typical timeline of a double extortion ransomware attack.

5. Double extortion first became a prominent tactic as a further method to make money from late-2019 onwards[i]. As part of the ransom demands to the victim, the attackers also threatened to leak the stolen data onto the internet. The intention is to shame victims into paying a ransom, even if the appropriate backups were in place to mitigate a traditional ransomware attack.
6. Many double extortion attacks lead to sensitive data being publicised on social media. In Q2 2020, there was an increasing trend for the publication of screenshots of the stolen data, by criminals and security researchers (see figure 4 for an example). This means that often the first public indication that a company has been hit by ransomware will be stolen sensitive information appearing on social media.

7. Figure 4 is a screenshot from social media of a ransomware group selling the stolen data of two law firms. The data was obtained in ransomware attacks between April and June 2020. In the screenshot at the top is a countdown clock. Ransomware groups will put a time limit on the sale of the data, to pressure the victim to pay and also to enable the group to auction the data to the highest bidder. Once the countdown has finished, the groups will often publicise all the information to exert further pressure on victims, especially if they have refused to pay the ransom.

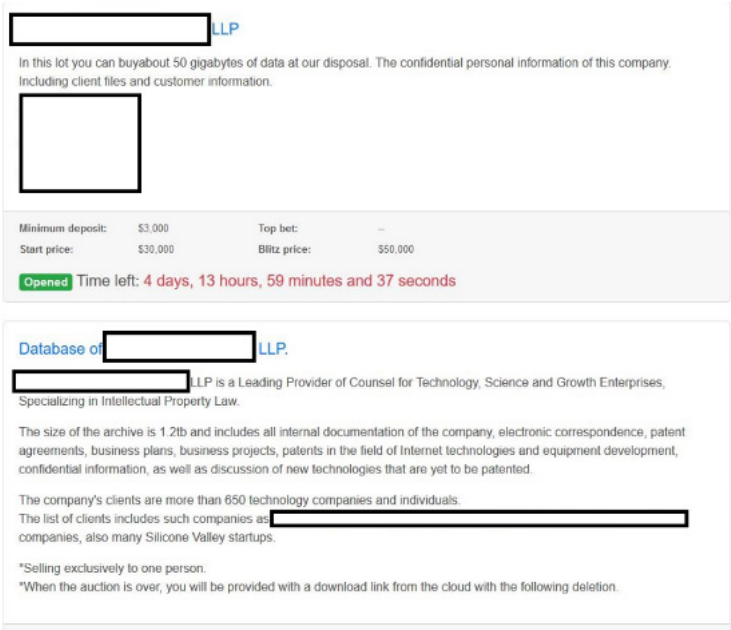

Figure 4 - Screenshot of a ransomware group advertising the sale of sensitive data from two law firms targeted by ransomware between April and June 2020. The details of the companies and clients have been hidden[ii].

8. As per figure 2, most of the ransomware attacks against the legal and accountancy sector were conducted by the Sodinokibi ransomware group, also known as the REvil group. Sodinokibi are believed to be linked to a now-withdrawn form of ransomware, GandCrab. GandCrab was retired in mid-2019 after the group claimed they had made more than $2 billion from their attacks[iii]. Sodinokibi ransomware was seen active from approximately the same time GandCrab was retired, and similarities in the coding make researchers believe the people responsible for both ransomware strains are linked[iv].
9. Sodinokibi have begun to auction off stolen data from their ransomware attacks to the highest bidder on a dedicated website, with the starting prices ranging from $50 000 to $100 000[v]. The criminals behind Sodinokibi are believed to be based in the former Soviet Union, possibly Russia, and it is believed there is little chance of them being extradited to the USA (where most of their victims are located), therefore they are effectively operating beyond the reach of law enforcement. Sodinokibi, like many other ransomware strains, operates as Ransomware-as-a-Service (RaaS). RaaS is a business model used by ransomware groups to sell access to their software to other less technically able criminal groups, who use the software in their own attacks, with a proportion of the profits paid back to the ransomware developers as a subscription.

---

i. https://www.coveware.com/blog/marriage-ransomware-data-breach
ii. https://twitter.com/AtlasCybersec/status/1270130087346737152/photo/1
iii. https://www.bankinfosecurity.com/ransomware-as-gandcrab-retires-sodinokibi-rises-a-12788
iv. https://any.run/malware-trends/sodinokibi
v. https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-CERT-EU-THREAT-MEMO-Ransomware-auctions-v1.1.pdf