Ransomware: REvil & the Increased Targeting of Law Firms

In May of 2020, a New York law firm made headline news when it was revealed that the REvil ransomware group (also known as Sodinokibi) had hacked their systems and were demanding a ransom.

This was a major news event not because of the size of the firm (a boutique), but because:

a) they are the premier powerhouse law firm to the entertainment world's biggest stars of music, Hollywood & television, and

b) the ransom initially demanded was USD 21,000,000 which then doubled to USD 42,000,000 – one of the highest known ransom demands[1]

Who are the Hackers?

REvil is a known hacking group that has been active for some time and has been named in several ransomware attacks on a variety of targets including financial institutions, recently hitting a major travel exchange entity and a South American bank. The group has not been associated with any specific target sector, but is known for having adopted a modus operandi called "double lever extortion" that was first observed with another ransomware group called Maze in late 2019.

Double lever extortion usually involves penetrating and mapping the network of the victim (sometimes using automated hacking tools), exfiltrating as much data as possible and then launching ransomware. The ransomware is highly sophisticated, and the hackers have proven quite successful in penetrating and encrypting backups, giving them considerable leverage for demanding a ransom.

The "double lever" involves the hackers also holding the victim's data and if the victim refuses to pay for the decryption key, the hackers threaten to release or sell that data on the dark web.

The Maze ransomware group is known to have targeted **law firms** (at least 5 victim firms reported) as has a group known as Ryuk (2 firms), and REvil is known to have attacked at least 3 firms.

1 **Article - LA Times**

Impact on Law Firms

The attack on the New York law firm was part of a dramatic escalation in the targeting of law firms that has taken place in the last 12 months and demonstrated several emerging and concerning trends:

- There appears to be a developing recognition that law firms are a repository of highly sensitive and valuable information and are therefore a desirable target (REvil were quick to release the names of several major music stars and the President of the US, in an attempt to pressure the victim firm into paying the ransom)
- The hackers are using very sophisticated techniques to penetrate networks, identify and target backup systems for ransomware deployment and to exfiltrate data
- Hackers are becoming more sophisticated in their understanding of the value of the information they are stealing and the impact that they can have on the victim's business and are pricing their ransoms accordingly
- There is an understanding that many of the victims have **cyber insurance** and while there is no evidence that this is exacerbating the problem, it is playing to the hackers' interests in facilitating a rapid turnaround once the demand is made

Is Cyber Insurance Exacerbating the Problem?

The question of whether or not cyber insurance is encouraging this type of crime and whether the hackers are specifically identifying cyber insurance policies and using the information to shape their demands, is an interesting debate.

> *"Currently, there is no evidence to support this claim and this speculation is based primarily on suspicion and rumour. There have been references to an instance in which the hackers are alleged to have known of the existence of a cyber policy and shaped their demands accordingly, but there is no empirical evidence to support the rumour."*
>
> Tom Ricketts, Senior Vice President and Cyber Risk Leader, Aon

On the other hand, the existence of cyber insurance is supporting the provision of expert and experienced cyber extortion negotiation resources, who are familiar with the different hacker groups and can advise on their reliability in terms of delivering a working decryption key in return for the ransom. These experts understand what the hackers will accept and can leverage the hackers' interests in speed of resolution and anonymity into negotiating down the ransom demanded. In one recent instance, the negotiation team correctly identified weakness in the hackers' position and were able to negotiate settlement at 10% of the initial demand.

It is not impossible that hackers that have exfiltrated a victim's data could search for and find a cyber insurance policy and then identify how much insurance the victim has and structure their demands accordingly. However, this would be time-consuming and difficult to do; even if they could correctly identify the cyber insurance policy they would have to find and identify the limit of insurance applicable to extortion. It seems unlikely that a hacker, particularly one that is holding sensitive data in addition to the decryption key, would go to this additional time-consuming effort when what they are seeking is a rapid turnaround with the highest return achievable in the shortest time.

Should Law Firms Invest in Cyber Insurance?

All the evidence, and particularly the experience of the insurers, indicates that law firms are being increasingly targeted by cyber criminals (in a report on ransomware dated July of 2020, anti-malware company Emsisoft stated "organisations in the legal, healthcare and financial sectors have been frequently targeted[2]"). Ransomware attacks have increased dramatically and experts are also reporting a substantial increase in other types of attack.

Cyber criminals appear to have learned that law firms hold a great deal of valuable information, whether as proxies for their clients (IP & trade secrets, personal information) or as a key party in high value transactions.

It is therefore important for firms to invest in cyber-security and to participate in information-sharing forums such as the Legal Services Information Sharing and Analysis Organization (LS-ISAO) to keep abreast of the trends in the threat environment. Equally important is to be prepared with an Incident Response Plan (IRP) that is regularly exercised and tested.

Alongside these, it is essential to have a **cyber insurance programme** that will mobilise and pay for the resources necessary to respond to a cyber incident when it happens.

To discuss any of the topics raised in this article, please contact **Tom Ricketts**.

2 **https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/**