redsense
INTELLIGENCE OPERATIONS

TLP:GREEN

Ransomware is dead, long live ransomware!

It seems to be a common misconception in business today that ransomware is dead or dying. The perception is that we haven't seen a huge daily deluge of new major businesses making eight figure payments to prolific centralized operations in the way that they were over the last few years. Incidents like Medibank feel less common. This perception is inaccurate at best, and dangerous at worst.

In terms of major incidents, the most prolific in the current mind will likely be the breach of MediBank. This large Australian firm is currently finding extortionists at their door, trying to extort a reported $10 million USD However, these large breaches are far from the truth. Industry myopia tends to leave those of us in the threat intelligence field feeling a false sense of security in times where the big breaches tend to be fewer and further between.

*IT SEEMS TO BE A **COMMON MISPERCEPTION** IN BUSINESS TODAY THAT RANSOMWARE IS DEAD OR DYING.*

Oftentimes, as the black hat vs white hat game of cat and mouse plays out, we find that the truth is that the risk has just moved elsewhere and as has been the case in the past, in this case deeper into the supply chain. Small and medium businesses are seeing a huge uptick in targeted ransomware attacks from former affiliates of the major ransomware groups that disbanded throughout 2022, and the risk these attacks pose both to consumers and to their larger business partners is substantial.

Let's take a look at one such group. The Venus ransomware group targets the often weak perimeter security of small and medium business, primarily through internet exposed Remote Desktop Protocol (RDP), and extorts victims for an average of 1 btc. This is hardly the massive bounties paid for things such as MediBank but it does speak to the mindset. As with other ransomware groups, these are talented hackers who are members of a broader underground ecosystem. The files, network connections and credentials found in these attacks are evaluated and resold, often for a high value when a pivot point into large business is found.

Currently Red Sense tracks dozens of active threat groups and observes routine patterns of activity around the release of new exploits or changes in the internet environment. At least a handful are always active while others take breaks. Due to the intergang ecosystem, it has the effect of a wider set of attack methodologies being deployed from diverse infrastructure and, therefore, efficacy against many technologies. The methodologies deployed, being in many cases simple use of legitimate authentication systems, often have the impact of

avoiding traditional security measures such as endpoint technologies, EDR and network security systems. When someone logs in with stolen credentials or a stolen session to a businesses remote access point, it is very unlikely to trigger alerts in any of these common response tools. Once inside, pivoting to domain administrator and disabling or uninstalling endpoint and defensive tooling is a common next step.

Additionally, we are starting to see the impacts of OFAC (Office of Foreign Asset Control). These regulations have started to be a consideration for large business when it comes to paying ransoms, and as such we see things like the group Daxin, who has some signs of being an eastern european group trying their best to appear to be a non-OFAC entity. Daxin was recently responsible for a series of medical sector attacks and they are far from done. We do not see small businesses with an immediate need to resume operations taking these regulations as seriously. However, they can still easily fall afoul of the mechanisms of enforcement for breaching these regulations which can come with significant financial and potentially criminal consequences.

For large businesses, it is critical to review extortion dumps for your intellectual property and potential knock on effects such as disclosed credentials, banking information, and network information. This is a time consuming and difficult task greatly simplified by engaging the right partners who are experienced in the collection and assessment of such data. As the drop points and methodologies continue to change, it can be a costly proposition to keep abreast of change.

For small and medium sized businesses, the idea of tackling threat intelligence can seem impossible or far too costly. An outsourced and scalable program is within reach for a business of any size.

Red Sense is offering a free consultation about these threats, how they are targeting your environment, and what we can do as a community to most effectively address and mitigate them for your business regardless of size or technical complexity.

Contact sales@redsense.com to schedule yours today.

ABOUT US

Red Sense, LLC is a veteran-owned small business (VOSB), that monitors and tracks significant events and forces within the Security space in order to provide our customers with deep insight into the myriad of new technologies, threat actors, software vulnerabilities and exploits, and sometimes suspect vendor sales pitches. RedSense offers vendor-agnostic and objective counsel to help address the evolving Security and Intelligence spaces.