Ransomware 2.0

White Paper

By Shaun Thomas Barnett

Executive Summary

The global pandemic has seen the rapid evolution of the traditional working environment, with more people working from their home office, and an increase to the number of online meetings rather than the standard board room meeting. Similarly, the evolution of ransomware to what is now being considered ransomware 2.0 has businesses and individuals scrambling to secure their data.

Ransomware 2.0 is a relatively new concept and employs a double extortion model where a ransom must be paid to prevent both data loss and data leakage. The new model has supplemented the ever-emerging Ransomware as a Service (RaaS) model where even non-technically minded cyber criminals can launch cyber-attacks on systems. New and improved state of the art detection techniques that have been developed for traditional ransomware could serve beneficial in the new ever-changing threat landscape that now includes ransomware 2.0. Tools such as EldeRan, RansomWall and RansHunt possess features and capabilities that are essential in the early identification and eradication of ransomware.

Behaviour Analysis

Key differences exist between the behaviour of traditional ransomware and what is now being called ransomware 2.0. While traditional ransomware focuses on encrypting data on your device, and/ or locking your data away and prompting you to pay a ransom to regain access, ransomware 2.0 doesn’t just lock you out of your data. Ransomware 2.0 will also steal a copy of your data and threaten to release it publicly if you don’t cough up the payment requested. Ransomware 2.0 attacks require an extra level of skill for threat-actors, as the data they are after is generally business critical and is not going to be found on the device that is their initial foothold into a network (Crandall, 2020).

To successfully pull off a ransomware 2.0 attack, the threat-actor is required to conduct lateral movement techniques, such as credential theft, network discovery, open port discovery and identifying vulnerable objects within the network (Crandall, 2020). Achieving this cannot be necessarily completed automatically, and thus there has been a significant increase in the number of ransomwares requiring hands-on keyboard intrusions, meaning the attackers are interacting directly with your network and/or devices, working to maximise the impact of the ransomware, and thus increasing the likelihood of you paying the ransom.

Another behavioural characteristic of ransomware 2.0 is it desire to interact with a human. Traditional ransomware aimed to quickly infect a device, encrypt the local data, and then prompt the victim for payment to decrypt the data. However, defence mechanisms, such as Anti-Virus or End-Point Protection meant that most traditional ransomwares were automatically stopped. Ransomware 2.0 aims to deceive these automatic defences, by ensuring its interacting with a human target. This is completed by using tools such as CAPTCHA tests to lure in its victim. This technique allows threat-actors to ensure their attack will not be stopped by automated defences and exploits the additional possibility of human error through clicking malicious links or downloads (Yoo & Graf, 2020)

Criminal Business Model

The business model of attackers is straight forward, making money with the least amount of effort required. This model is easily achieved in ransomware attacks, as, once the ransomware is built, the attackers can sit back and watch as more and more people fall victim to their attack, and a percentage of those pay up the ransom (Bar-Yosef, 2010). Ransomware 2.0 still capitalises on that model, and takes advantage of the basic rule of business, which is increasing revenue, while reducing cost.

To increase the diversity of the ransomware threat landscape, attackers are taking advantage of the growing popularity of Ransomware as a Service (RaaS). RaaS is a service model that allows sophisticated ransomware, developed by talented threat actors, to be sold to other attackers. This service allows a new breed of cyber criminal's access to the ransomware business. These new cyber criminals no longer need to be extremely technical to launch a cyber-attack, rather they hire a service, and reap the rewards. Additionally, the RaaS model provides its customers with training, reference materials to successfully plan and deploy a cyber-attack (Renshaw, 2021). This new evolution in the criminal business model means that it's never been easier to make money, with minimal effort.

There are three key purchase models of RaaS that have emerged in its development over past years. These models are known as subscription, affiliate, and purchase. Subscription is where a RaaS provider receives a pre-determined amount of cryptocurrency for a period of usage, independent of the outcome of the use of the ransomware. Affiliate refers to a model where the RaaS provider receives a recurring fee, like that of the subscription model, plus a percentage of the earnings from the ransomware attacks, this model can be seen below in Figure 1.

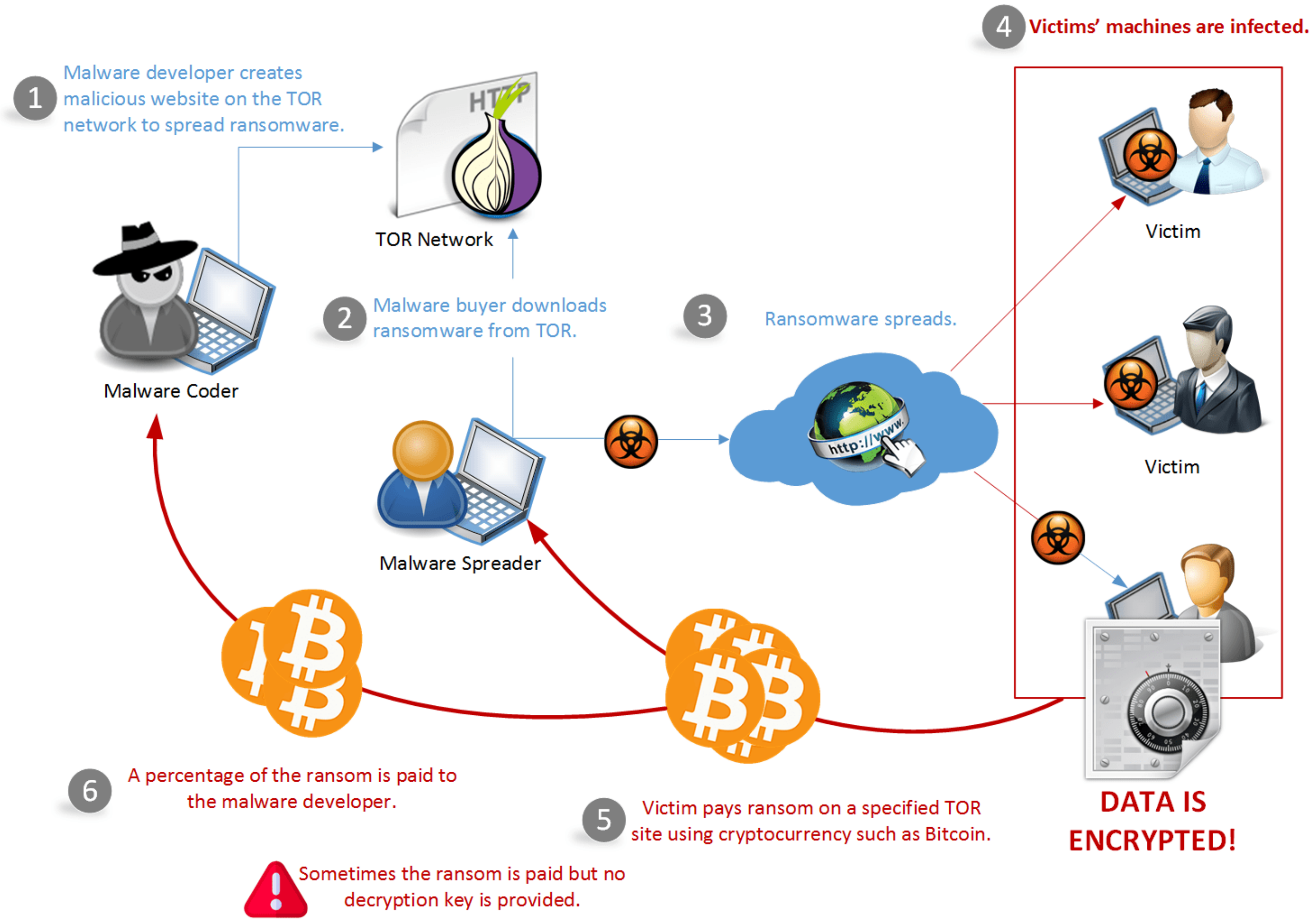
4 Victims' machines are infected.
1 Malware developer creates malicious website on the TOR network to spread ransomware.
HTTP
TOR Network
Victim
Malware Coder
2 Malware buyer downloads ransomware from TOR.
3 Ransomware spreads.
http://www.
Victim
Malware Spreader
6 A percentage of the ransom is paid to the malware developer.
5 Victim pays ransom on a specified TOR site using cryptocurrency such as Bitcoin.
DATA IS ENCRYPTED!
Sometimes the ransom is paid but no decryption key is provided.

Figure 1: RaaS Affiliate Model (Balajin, 2018)

Finally, the purchase model is simple, the RaaS provider sells a ransomware package to a buyer for a one-off price (Renshaw, 2021).

Detection Techniques

Detecting ransomware at the earliest stage of infection has never been more important that in the new war against ransomware 2.0. The earlier that ransomware is detected, the less likely it is that you are going to lose data to encryption and/or be extorted for money from the fear of your data being released on the world wide web. Below are three detection techniques that can assist in the battel against ransomwares evolution. These detection techniques utilise an array of methods to stop ransomware in its tracks, including both static and dynamic analysis. Static analysis refers to when the ransomware is analysed without being executed, while dynamic analysis occurs when the ransomware is being executed, usually in a testing environment.

EldeRan

EldeRan uses a sandbox environment (an isolated system for testing the behaviour of ransomware), to perform static and dynamic analysis of the following operations: API calls, registry key modification and additions, directory operations, analysis of dropped files and the strings of executables. It does this on the idea that ransomware possess and executes behaviours that are significantly different to that of harmless software. Research on EldeRan revelled that it has a 96.34% detection rate in ransomware families that it is familiar with, while having a 93.3% detection rate of ransomware families that is has not seen before (including the likes of Ransomware 2.0) (Ferando, Komninos, & Chen, 2020). These detection rates are competitive with the detection rates of modern antivirus systems. The research points out that EldeRan can detect ransomware infections at the earliest stages, a clear requirement for the detection of Ransomware 2.0.

RansomWall

Built as a layered system, RansomWall is designed and developed to detect ransomware attacks in real time. Designed for Windows operating systems, this system also makes use of a sandbox to conduct behavioural analysis, like EldeRan. The system employs five layers to conduct analysis, the first being static analysis layer, followed by the trap layer, then the dynamic analysis layer. The final two layers are comprised of the backup layer and the machine learning layer. Overall, it’s a comprehensive approach, combining several detection methods to build its multi-layered approach, arguably its greatest strength. Additionally, the backup layer provides a protection layer, however this is only useful in traditional ransomware attacks, where data is only encrypted on the device, and not stolen. Regardless, Ransomware has a detection rate of 98.25% (Ferando, Komninos, & Chen, 2020). What gives RansomWall its place as a detection technique is its comprehensive approach to detecting the behaviour of ransomware at its early stages of infection.

RansHunt

RansHunt is a detection framework that has been designed to identify the characteristics that are prevalent in a ransomware infection. This system employs both static and dynamic features, that have been built from the likes of 21 ransomware families. Research conducted on RansHunt demonstrated that the system had a 97.1% detection rate, with an extremely low 2.1% false-positive rate. While those figures are promising, what really gives RansHunt its place as a Ransomware 2.0 detection method it its ability to learn behavioural patterns, and its ability to detect the next generation of ransomware. The research on RansHunt continues to outline that the next generation of ransomware is what is known as a ransomworms. Like ransomware 2.0, ransomworms are a ransomware/ worm hybrid, with the ability to propagate across networks (Ferando, Komninos, & Chen, 2020). With its ability to detect key ransomware behaviour and use previous attacks to identify the next generation of ransomware, such as ransomworms and ransomware 2.0, RansHunt will be an extremely useful tool in the fight to protect your data.

Regardless of the use of these or other state of the art ransomware detection techniques, the threat of ransomware 2.0 is still underpinned by the fundamental problem of how the ransomware makes its initial entry to your network or system, known as an attack vector. Examples of these attack vectors can be seen below in Figure 2.

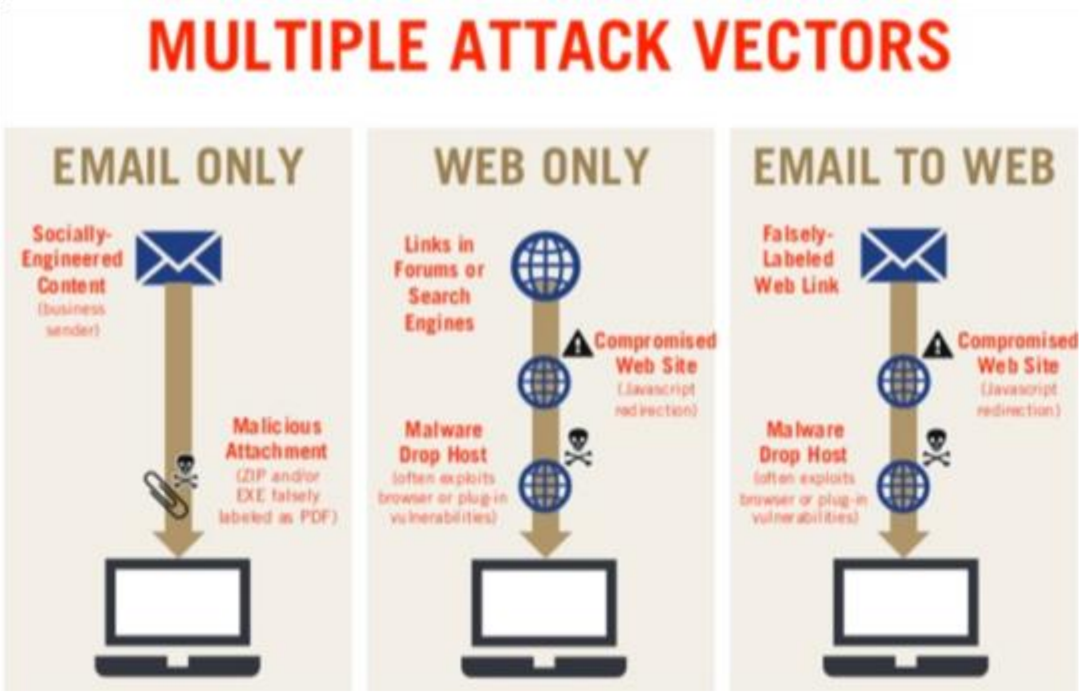

Figure 2: Ransomware Attack Vectors (Viacaro, 2019)

Continuing to educate the population about ransomware, and their attack vectors, such as phishing links or malicious sites, is a critical component of this battle. Similarly, continuing to employ a defence-in-depth model of network and system security also plays a role in defending against ransomware.

References

Balajin, N. (2018, February 18). *Ransomware-as-a-Service – Now Anyone can Download Free Ransomware that is Available on Dark Web*. Retrieved from GBHackers on Security: https://gbhackers.com/ransomware-as-a-service-2/

Bar-Yosef, N. (2010, October 19). *An Inside Look at Hacker Business Models*. Retrieved from Security Week: https://www.securityweek.com/inside-look-hacker-business-models

Crandall, C. (2020, September 16). *Derailing ransomware 2.0 requires a little trickery*. Retrieved October 16, 2021, from Security Magazine: https://www.securitymagazine.com/articles/93303-derailing-ransomware-20-requires-a-little-trickery

Ferando, D. W., Komninos, N., & Chen, T. (2020). *A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques.* MDPI: Department of Computer Science.

Renshaw, S. (2021, September 28). *Ransomware-as-a-service: A new business model for cybercriminals*. Retrieved from RSM: https://rsmus.com/what-we-do/services/risk-advisory/cybersecurity-data-privacy/ransomware-as-a-service-a-new-business-model-for-cybercriminals.html

Viacaro, J. (2019, October 30). *INCIDENT RESPONSE RANSOMWARE SERIES – PART 2*. Retrieved from TrustedSec: https://www.trustedsec.com/blog/incident-response-ransomware-series-part-2/

Yoo, J., & Graf, N. (2020, October 27). *Ransomware 2.0 – What to expect next*. Retrieved from AICPA: https://www.aicpa.org/interestareas/privatecompaniespracticesection/newsandpublications/the-practicing-cpa/ransomware-2-what-to-expect-next.html