Australian Journal of Defence and Strategic Studies

Volume 4, Number 1 (2020)

ISSN 2652-3728 (PRINT) 2652-3736 (ONLINE)
https://www.defence.gov.au/ADC/Publications/AJDSS
https://doi.org/10.51174/AJDSS.0401

Ransomware 2.0: an emerging threat to national security

Mohiuddin Ahmed, Sascha Dov Bachmann, Abu Barkat Ullah and Shaun Barnett

Published online: 8 July 2022

The *Australian Journal of Defence and Strategic Studies* is published twice a year by the Australian Department of Defence. It is the flagship academic journal of the Australian Defence Force. ADC Publications are managed by the Centre for Defence Research on behalf of the Australian Defence College.

PO Box 7917 CANBERRA BC ACT 2610 Tel + 61 02 6266 0352 Email cdr.publications@defence.gov.au
Web www.defence.gov.au/adc/publications/ajdss

Ransomware 2.0: an emerging threat to national security

Mohiuddin Ahmed, Sascha Dov Bachmann, Abu Barkat Ullah and Shaun Barnett

Introduction

The global Covid-19 pandemic has seen the rapid evolution of our traditional working environment; more people are working from home and the number of online meetings has increased. This trend has also affected the security sector. Consequently, the evolution of ransomware to what is now being described as 'Ransomware 2.0' has governments, businesses and individuals alike rushing to secure their data.

Australia, as an open market economy and democracy, is both dependent and reliant on the internet and online security for our prosperity, way of life and the functioning of our democracy. Cyber security as a prerequisite for our ever-increasing interconnectivity is under assault from cyber attacks and malicious cyber activity being conducted by states and 'hybrid actors', such as cyber criminals and syndicates. *Australia's Cyber Security Strategy 2020* identified these threats as posing a risk Australia's national security, social cohesion and prosperity, stating: 'Well-equipped and persistent state-sponsored actors are targeting critical infrastructure and stealing our intellectual property.'[1] Consequently in 2021, the Australian Government launched its *Ransomware Action Plan* to 'ensure that Australia remains a hard target for cybercriminals'.[2] This short commentary provides a short overview of Ransomware 2.0 threats to

1 Peter Dutton MP, 'Minister's Foreword', *Australia's Cyber Security Strategy 2020*, Department of Home Affairs: Australian Government, Canberra, 2020, p 4. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australia%E2%80%99s-cyber-security-strategy-2020

2 Department of Home Affairs (Home Affairs), *Ransonware Action Plan*, Australian Government, Barton ACT, 2021, p 6. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-ransomware-action-plan

our cybersecurity and online safety, which can have serious implications for our national security.

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. Many new and improved detection techniques that have been developed for traditional ransomware are beneficial in this new ever-changing threat landscape. These include tools such as EldeRan, RansomWall and RansHunt, which 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 locking your data away until you pay a ransom to regain access, Ransomware 2.0 encrypts your data and steals a copy, threatening to release it publicly if you do not 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.[3]

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 identify vulnerable objects within the network.[4] This cannot necessarily be achieved automatically, and thus there has been a significant increase in the number of ransomwares requiring hands-on keyboard intrusions. This means the attackers are interacting directly with your network 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 its 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, antivirus software can flag such ransomwares and can automatically stop their execution. Ransomware 2.0 aims to deceive these automatic defences, by ensuring its interacting with a human target. This is completed by using tools to lure in victims, such as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) tests. This technique allows

3 Carolyn Crandall, 'Derailing Ransomware 2.0 requires a little trickery', *Security* [eMagazine], 16 September 2020, accessed 7 March 2022. https://www.securitymagazine.com/articles/93303-derailing-ransomware-20-requires-a-little-trickery

4 Crandall, 'Derailing Ransomware 2.0 requires a little trickery'.

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.[5]

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. Once the ransomware is built, the attackers can sit back and watch more and more people fall victim to their attack, and a percentage of those pay up the ransom.[6] Ransomware 2.0 still capitalises on that model and takes advantage of a basic rule of business, increasing revenue while reducing costs.

To increase the diversity of the ransomware threat landscape, attackers are taking advantage of the growing popularity of the 'Ransomware as a Service' (RaaS) model that allows sophisticated ransomware, developed by talented threat actors, to be sold to other attackers. This service allows a new breed of non-technically minded cybercriminals access to the ransomware business. These new cyber criminals simply hire a service and reap the rewards. Additionally, the RaaS model provides its customers with training and reference materials to successfully plan and deploy a cyber-attack.[7] This evolution in the criminal business model means that it has never been easier to make money with minimal effort.

There are three key purchase models of RaaS that have emerged in its development over the past decade.[8] These models are known as subscription, affiliate and purchase. Subscription is where a RaaS provider receives a predetermined amount of cryptocurrency for a period of usage, independent of the outcome of the use of the ransomware. Similar to the subscription model, in the affiliate model the RaaS provider receives a recurring fee and a percentage of the earnings from the ransomware attacks (this model can be seen in Figure 1). The third model, the purchase model, is where the RaaS provider simply sells a ransomware package to a buyer for a one-off price.

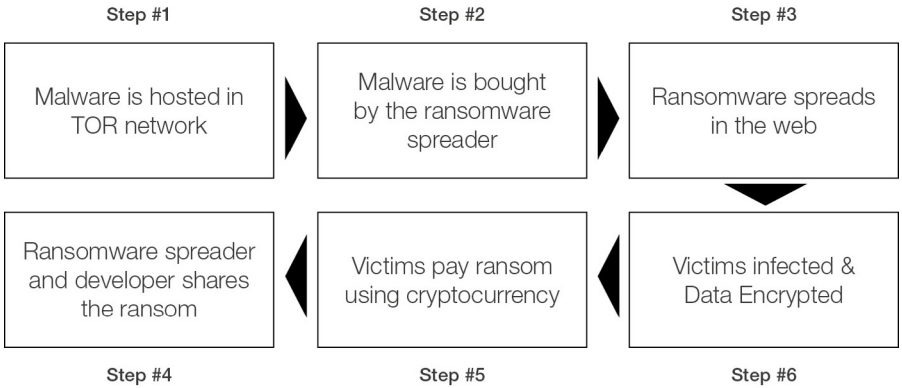
5 Danny Bradbury, 'Double trouble: how Ransomware 2.0 puts your data under threat', *Infosecurity Magazine* [eMagazine], 11 March 2021, accessed 7 March 2022. https://www.infosecurity-magazine.com/magazine-features/double-trouble-ransomware-data/

6 Noa Bar-Yosef, 'An inside look at hacker business models', *Security Week*, 19 October 2010, accessed 7 March 2022, https://www.securityweek.com/inside-look-hacker-business-models

7 Sean Renshaw, Ransomware-as-a-service: A new business model for cybercriminals, RSM US [website], accessed 7 March 2022, https://rsmus.com/insights/services/risk-fraud-cybersecurity/ransomware-as-a-service-a-new-business-model-for-cybercriminals.html

8 Bar-Yosef, 'An inside look at hacker business models'.

Figure 1: RaaS Affiliate Model [9]



Detection techniques

Detecting ransomware at the earliest stage of infection has never been more important than 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 or face extortion to prevent your data being released on the internet. Below are three detection techniques that can assist in the battle against ransomware evolution. These detection techniques utilise an array of methods to stop ransomware in its tracks, including both static and dynamic analysis.[10] Static analysis refers to when the ransomware is analysed without being executed, whereas 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: application programming interface (API) calls, registry key modification and additions, directory operations, analysis of dropped files and the strings of executables. This presupposes that ransomware possesses and executes behaviours that are significantly different to that of harmless software. Research on EldeRan revealed that it has a 96.34% detection rate in ransomware families that it is familiar with, while having a 93.3% detection

9 This is a very generic overview of the RaaS. For more details see gbhackers.com. Balaji N, 'Ransomware-as-a-Service – now anyone can download free ransomware that is available on dark web', gbhackers.com, 18 February 2018, accessed 7 March 2022, https://gbhackers.com/ransomware-as-a-service-2/

10 Damien W Fernando, Nikos Komninos and Thomas Chen, 'A study on the evolution of ransomware detection using machine learning and deep learning techniques', *IoT*, 2020, 1(2): 551–604. https://doi.org/10.3390/iot1020030

rate on ransomware families that it has not seen before (including the likes of Ransomware 2.0).[11] These detection rates are competitive with the detection rates of modern antivirus systems. The research points out that ElderRan 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. The system employs five layers to conduct analysis; the first being a static analysis layer, followed by a trap layer then the dynamic analysis layer.[12] The final two layers are a backup and machine-learning layer. Overall, it is a comprehensive approach that combines several detection methods to build its multilayered approach, arguably its greatest strength. Additionally, the backup layer provides a further protection layer. However, this is only useful in traditional ransomware attacks, where data is only encrypted on the device and not stolen. Regardless, RansomWall has a detection rate of 98.25%. 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, which have been built from the analysis 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.[13] 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 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. Due to its ability to detect key ransomware behaviour and

11 Fernando et al., A study on the evolution of ransomware detection using machine learning and deep learning techniques', p 564.

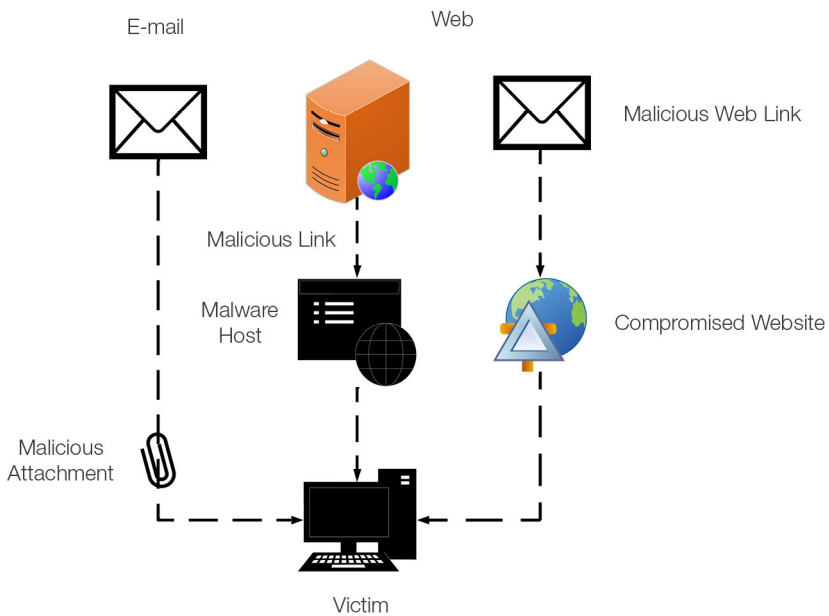
12 Fernando et al., A study on the evolution of ransomware detection using machine learning and deep learning techniques', p 565.

13 Fernando et al., A study on the evolution of ransomware detection using machine learning and deep learning techniques', p 568.

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 a network or system, known as an attack vector. A generic overview of these attack vectors is showcased in Figure 2 (more details can be found in the blogpost by Justin Vaicaro).[14]

Figure 2: Ransomware Attack Vectors[15]



Lessons for Australia

Speaking on occasion of the release of an advisory co-authored by the Australian Cyber Security Centre and partners from the US and UK in February 2022, Australia's Assistant Minister for Defence, Andrew Hastie MP, warned of the rise

14 Justin Vaicaro, 'Incident response ransomware series – part 2', *TrustedSec* [website], 30 October 2019, accessed 7 March 2022, https://www.trustedsec.com/blog/incident-response-ransomware-series-part-2/

15 Vaicaro, 'Incident response ransomware series – part 2'.

of ransomware attacks as a form of grey-zone tactic that has manifested in the post-COVID security landscape.[16]

It is imperative to investigate the available cryptocurrencies, how criminals take advantage of anonymity and potential solutions to track such entities. In recent times, only a handful of investigations have been conducted to de-anonymise crypto-transactions and identify the actual receiver of ransomware payments. While these are primarily heuristics and works in progress, it is critical to determine whether cybercriminals are state-based actors.

From Australia's national security perspective, this has become even more critical since the AUKUS nuclear submarine deal was announced last year, which attracts more cybercriminals to attack Australian critical infrastructure, homes and businesses.[17] Such attacks can originate from hybrid actors such as states, criminal organisations or both. This threat may become even more exacerbated with the Russian invasion of Ukraine and Australia's announcement of cyber assistance, provision of humanitarian and lethal aid and the imposition of sanctions. Subsequently, the ACSC has warned of an increase of ransomware attacks and their potential as a national security threat.[18]

Given Defence's ever-increasing partnerships with critical civilian partners in terms of research, defence procurement and services, the potential for Ransomware 2.0 attacks will have multiple objectives: from economic damage (ransom) to our wider defence partnership networks to testing the resilience of our IT networks, in respect to malware and other malicious cyber operations. The economic consequences alone can seriously affect the success of Australia's business and industry partnership with Defence. There is also the potential for espionage and intellectual property theft linked to such malware attacks. Given the 'hybridity' of both attacker and the cyber threat (malware, ransomware etc.) both cyber resilience and cyber awareness are fundamental first steps toward meeting the challenge.

Cyber resilience requires not only a whole-of-government approach but also the inclusion and cooperation of the commercial and civil sectors, as part of any

16 Andrew Hastie MP, *Australia US and UK stand together to confront global ransomware threat* [media release], Australian Government, 10 February 2022, accessed 7 March 2022, https://www.minister.defence.gov.au/minister/andrew-hastie/media-releases/australia-us-and-uk-stand-together-confront-global-ransomware

17 Adam Creighton, 'Australia more exposed to cyber attack after AUKUS: Karen Andrews', *The Australian*, 16 December 2021.

18 Australian Cyber Security Centre (ACSC), *Australian organisations encouraged to urgently adopt an enhanced cyber security posture* [webpage], Australian Signals Directorate, 23 February 2022, accessed 16 May 2022. https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture

comprehensive cybersecurity approach. 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.

Raising awareness is the prerequisite of such an approach, something this short commentary hopes to contribute to.