sententia
a different way of thinking

Information Security Incident Report

Ransomware Investigation

WARATAH
Strata Management

Client	Clyde & Co / Waratah Strata Management Pty Ltd
Date	26 March 2019

CONTACT INFORMATION

JP Clemence | *CEO*

ISO/IEC 27001 / ISLA 1019457

Sententia Pty Ltd | ABN 12 093 486 876

T. 02 9994 2700

isva@sententia.com.au

CONTRIBUTORS

Peter Stoll | Principal

ISO/IEC 27001 / ISLA 1019491

Manoj Mandal | *Senior Technical Consultant*

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Waratah Strata Management Pty Ltd (Waratah) has experienced a malware attack resulting in the encryption of shared files within their infrastructure. The investigation into the incident has revealed the following scenario:

1. A brute force attack was enacted over RDP with a varied set of random and known accounts.
2. A malicious toolset was used to create a new account.
3. The new account was then used to upload ransomware.
4. Shared data was subsequently encrypted with the goal of extracting a ransom for decryption.
5. A bitcoin ransom was paid through a 3rd party known to Waratah.
6. After payment was made, there was no response from the Threat Actor.
7. Waratah eventually recovered their data via a re-image procedure.

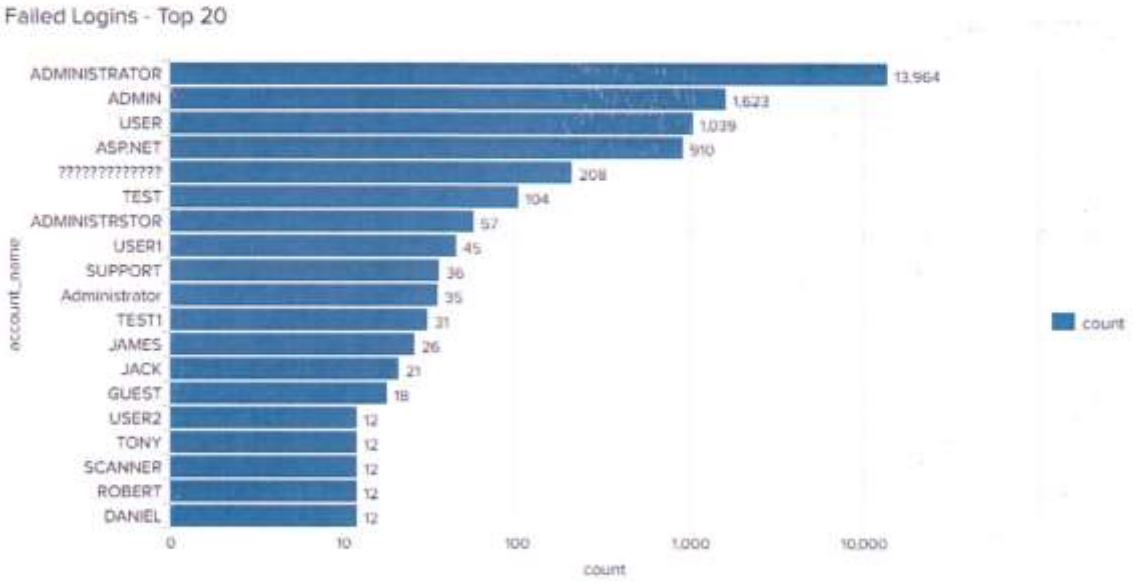
FORENSIC INVESTIGATION OBSERVATIONS

BRUTE-FORCE OVER RDP

The Threat Actor gained access to the Waratah infrastructure through a sustained brute-force attack, specifically against one of its servers, WSMHS1. This type of attack is defined by the attempts at login of any number of common or guessed usernames and password combinations.

An example of this activity can be seen in the graph below, taken from the only existing security logs *after* the Incident. While these are not the actual attempts which contributed to this Incident, it illustrates an important point. During the timeframe *between 15 February and 17 February 2019*, the Insured was still at risk, as there were continued attempts at brute-force access. These "Top 20" figures represent failed login attempts made by external, internet-based sources, in opposition to non-brute force attempts made from within the organisation, such as a forgotten or mis-typed password.

The remediation action to close all non-essential inbound ports would have resolved this issue.



INBOUND FIREWALL RULES

Of additional interest are inbound router rules, which clearly indicate and allow for open Remote Desktop Protocol (RDP) ports. It was via RDP that the brute-force attack occurred.

Destination/port	Translated destination/port	Notes
Public IP/63389	192.168.0.135/3389	RDP
Public IP/63390	192.168.0.10/3389	RDP
Public IP/64441	192.168.0.251/64441	RDP
Public IP/17990	192.168.0.251/17990	HP ILO remote console
Public IP/63391	192.168.0.3/3389	RDP

These ports have since been closed as a reactive measure to this Incident.

WWW ACCOUNT

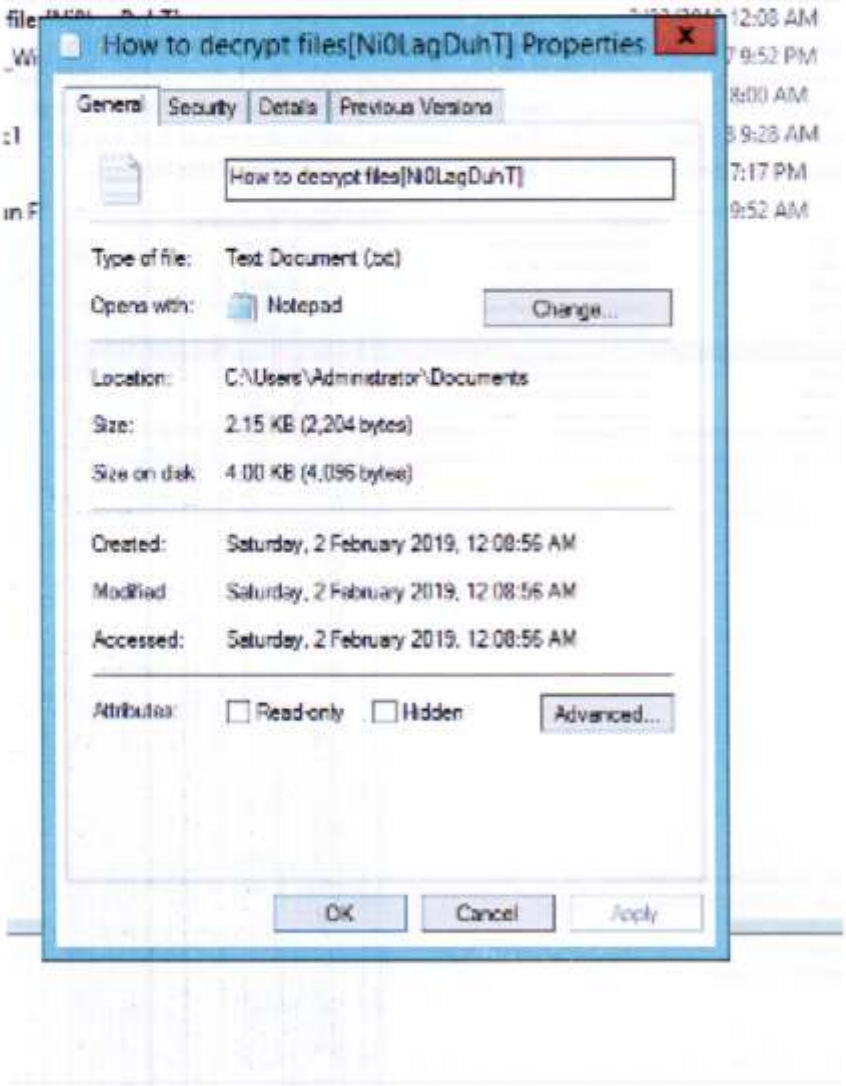
With the Threat Actor achieving brute-force success with the 'Administrator' account on the server WSMHS1, a malicious toolkit was then used to create a 'www' account on 01-February-2019 11:58:53 PM AEST. Evidence of this activity can be shown through the SAM Registry Hive for the Administrator account as displayed below. To alleviate confusion, it should be noted that all times in this audit facility are displayed in UTC.

The 'www' account is often used in the introduction of the '(enc)' malware kit, a variant of which is involved in this Incident. This account existed only long enough to upload and deploy the (enc) ransomware, after which the account was removed, along with all profiles, metadata, and .dat information. There is evidence from the Terminal Services audit logs that indicate a timeline of activity, with first login occurring at 11:59 PM 01-February, and session end at 3:33 AM 02-February. There is no evidence to suggest any other accounts were accessed during the timeframe of this Incident.

RANSOMWARE

Based upon the timestamp of the ransom note, the encryption was most likely complete on 02-February-2019 12:08:56 AM. The encryption extension is '_enc1', further indication of a prevalent type of ransomware.

A bitcoin ransom was subsequently paid to the Threat Actor in the equivalent amount of AUD $5,052.03. After this payment was made, there was no response from the Threat Actor.

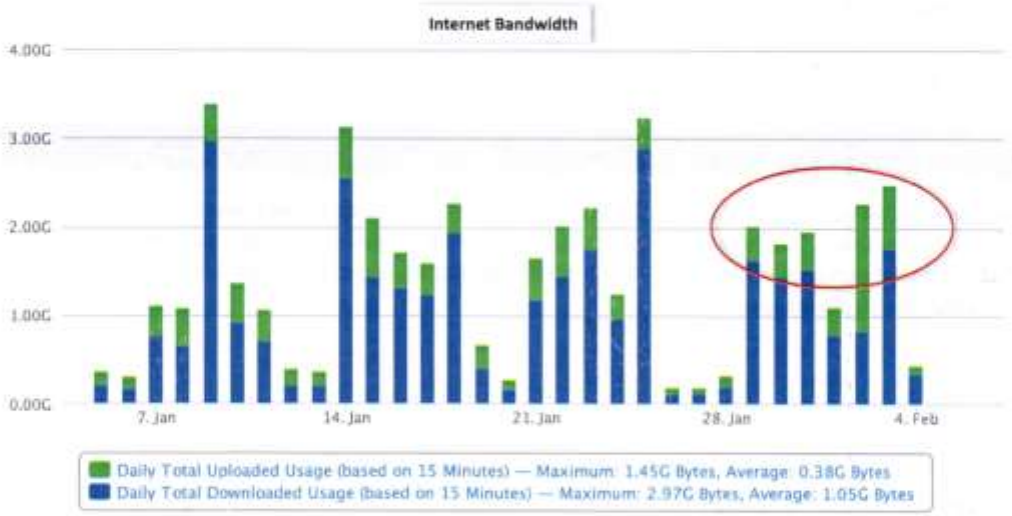


DATA EXFILTRATION

There is no evidence to suggest any data exfiltration has occurred. The Threat Actor accessed one server and created a new account. That account was then used to download malware to the server for the direct purpose of encrypting data, with the goal of extracting a ransom. After the data was encrypted, the new account was deleted from the system.

Furthermore, an examination of the internet usage logs for the time period in question reveals no significant additional traffic around the time of the Incident. The additional 2GB which is present on the morning after the Incident is related to the upload of encrypted and sample files for data recovery, as referenced by the Waratah IT Service Provider.

If data exfiltration had been a goal of the attack, there would be a significant increase in upload activity the moment after the breach occurred, which would be evident in the usage data logs.



REACTIVE MEASURES

As a matter of risk reduction and urgency, Sententia has asked Waratah's IT Service Provider to disable all inbound Remote Desktop Protocol traffic from the internet. A more secure method of connectivity should be implemented, such as a multi-factor authenticated VPN, for example.

Outbound traffic should be limited to only those connections that are required.

AVAILABLE EVIDENCE

All observations in this report are based upon Windows Event log files, gathered at the time of Incident Reporting. Our investigations rely on audit trails that are configured by the host administrator; the depth of an investigation depends upon the level of auditing that has been put in place by the client, before the incident has occurred.

Sententia has been able to determine a timeline of events, *to the best of our ability*, and establish a professional opinion into the matter, as expressed in this report. However, a deeper understanding of the exact actions of the Threat Actor is not possible due to a lack of evidence and an incomplete audit trail.

DISCLAIMER

This report has been prepared at the request of Clyde & Co in accordance with the terms of engagement as detailed mutually by Clyde & Co and Sententia. Other than our responsibility to Clyde & Co, neither Sententia nor any member or employee of Sententia undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.