

Hacker Intelligence Initiative, Monthly Trend Report #5

Hacker Intelligence Summary Report – Monitoring Hacker Forums

As a part of Imperva's hacker intelligence initiative, we monitor hacker forums to understand many of the technical aspects of hacking. Forums are the cornerstone of hacking – they are used by hackers for training, communications, collaboration, recruitment, commerce and even social interaction. Forums contain tutorials to help curious neophytes mature their skills. Chat rooms are filled with technical subjects ranging from advice on attack planning and solicitations for help with specific campaigns. Commercially, forums are a marketplace for selling of stolen data and attack software. Most surprisingly, forums build a sense of community where members can engage in discussions on religion, philosophy and relationships.

Hacking has become a group activity. Technical complexities have made hacking too difficult for any single individual to conduct attacks successfully – as recently evidenced by the hacking team called Lulzsec. For hackers participating in illegal activity the challenge is to preserve anonymity while finding and communicating with partners. To remove this obstacle, hackers have developed numerous hacker forums worldwide. The precise number is unknown, but there are likely several thousand. Some are quite large with nearly 250,000 members (though many are dormant) while others are smaller and quite exclusive with just dozens of hand-selected participants. And not all participants may be engaging in illegal activity, they may simply be technically curious or in search of community. Many forums are in English but attract an international group. Due to obvious anonymity requirements, hackers don't identify themselves or their nationality. But it is safe to assume that forums host a very internationally diverse group.

To date, we are not aware of any studies that have been performed on hacker forums – yet the value of studying these forums can help security professionals build better defensive strategies. Moreover, forums give interesting insight into the personalities and drivers that compel hackers. For parents and even law enforcement, there may be lessons to help spread the word that hacking for profit is wrong.

Methodology

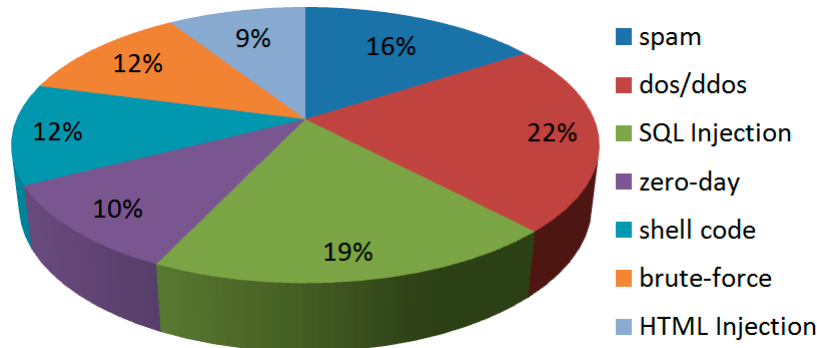
Imperva's analyzed one of the largest-known hacker forums with roughly 250,000 members. Known as "content analysis," Imperva used the forum's sophisticated search capability to analyze chats by topic using specific keywords. Specifically, we summarized the volume of threads addressing a multitude of topics.

Though there are many forums that are small and solely focused on committing cybercrime, we don't have access to these. The site we examined is not a hardcore crime site, but it's not entirely softcore either. New hackers come to this site to learn and on the other hand more experienced hackers teach to gain "street cred" and recognition. In the past, this forum has helped security researchers identify illicit cyber activity. Typically, once hackers have gained enough of a reputation they go to a more hardcore, by-invite-only forum.

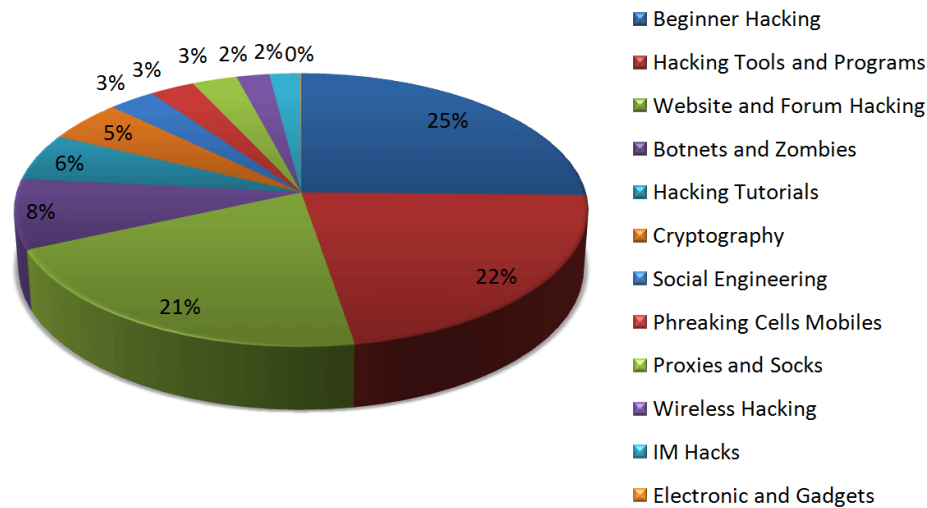
Key Findings:

Finding #1: The most discussed topics in forums are SQL injection, 19% of all discussions, and DDoS with 22% of discussions.

Top 7 attacks discussed in a large hacker forum in the last year (# threads with keyword)

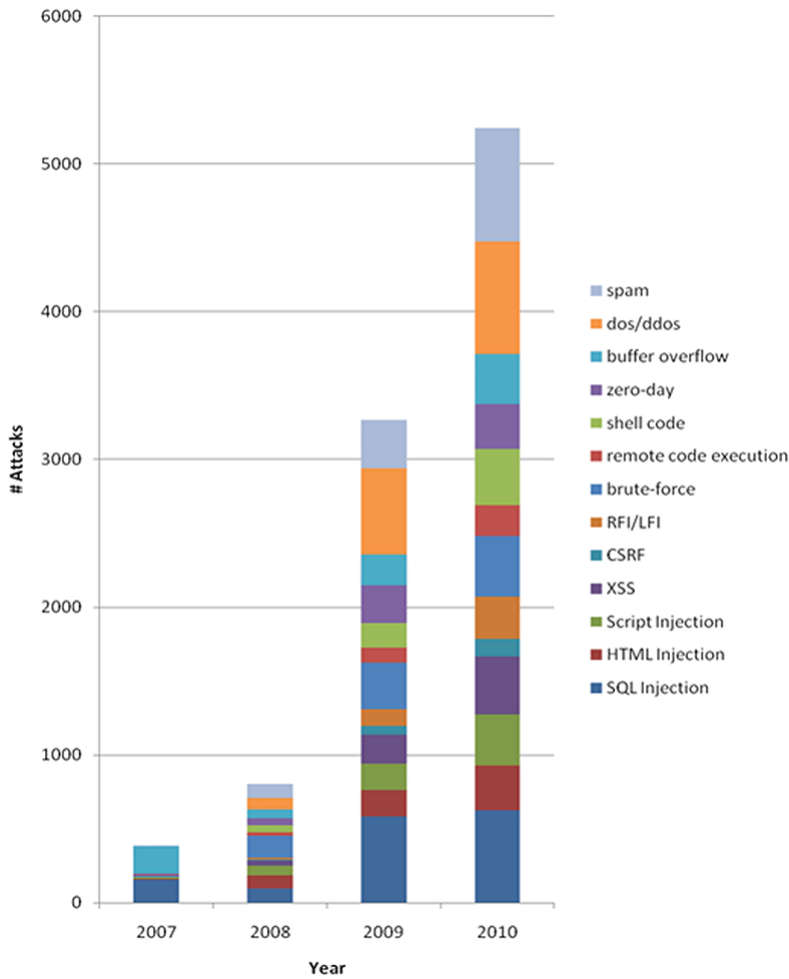


Finding #2: Hackers devote most of their time, 25%, towards discussing beginning hacking. The strongest category with nearly 25% of discussions was on hacking tutorials. This means there's a strong, steady interest in content to learn hacking, ensuring a steady supply of new talent. Other hacks, such as botnets and zombies, were prominent but website hacking more than tripled the next highest topic.



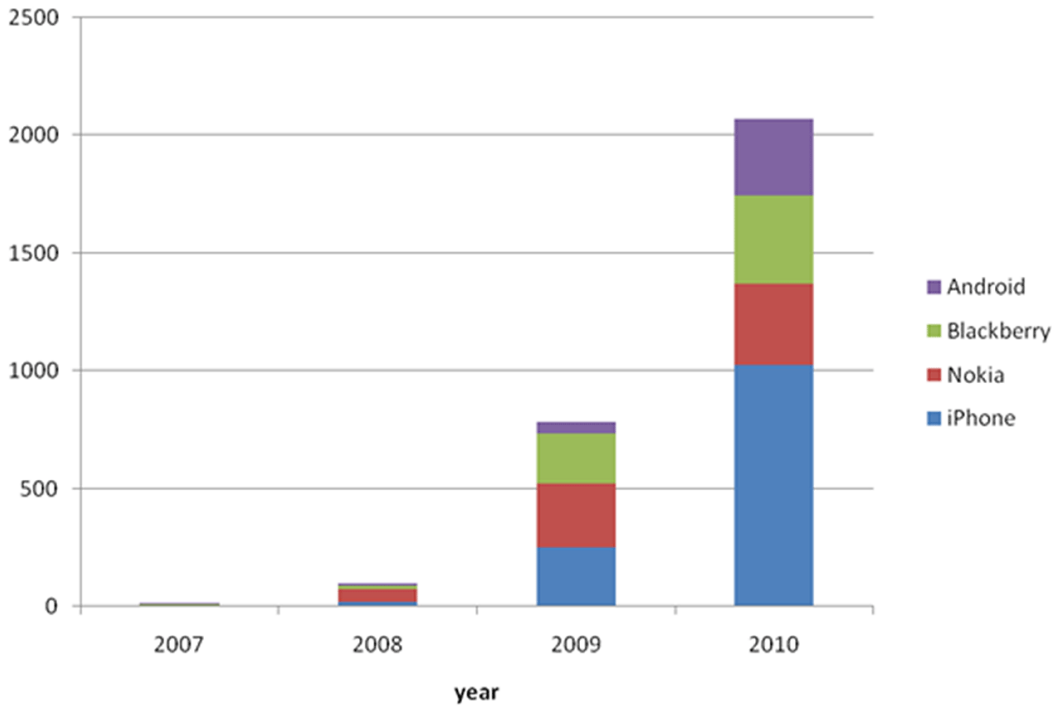
Finding #3: Attack discussions have grown exponentially over a four-year period, growing an average 157% since 2007. The fastest growing topics were DDoS, SQL injection and spam.

Growth of discussion topics by year



Finding #4: Mobile hacking has seen very strong growth in discussion forums, with iPhone hacking leading the way.

Growth of discussion of mobile platforms by year

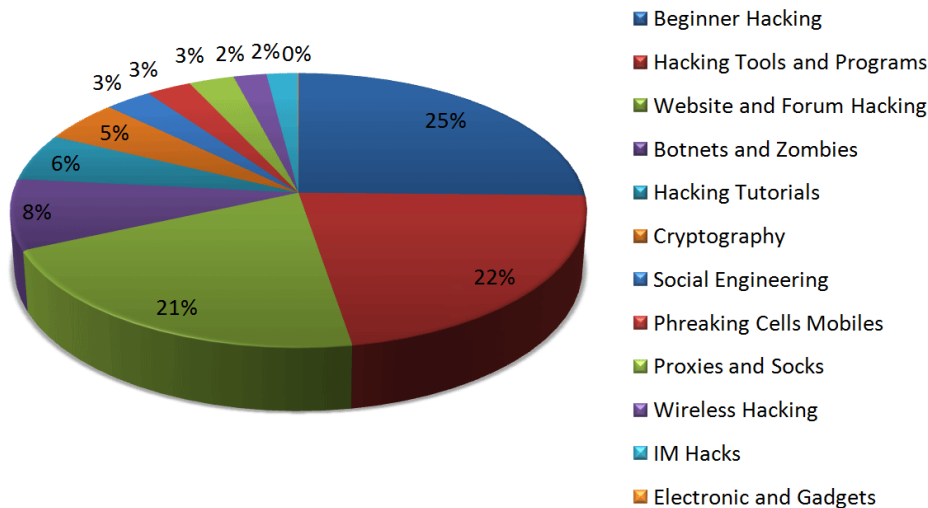


A Trip To the Dark Side

As we have mentioned, hacker forums serve several functions: training, communications, collaboration, recruitment, commerce and even social interaction.

1. Training – Forums help aspiring hackers learn the trade technically and nontechnically. Our analysis shows that training comprises the most frequented topic with 25% of total discussion threads.

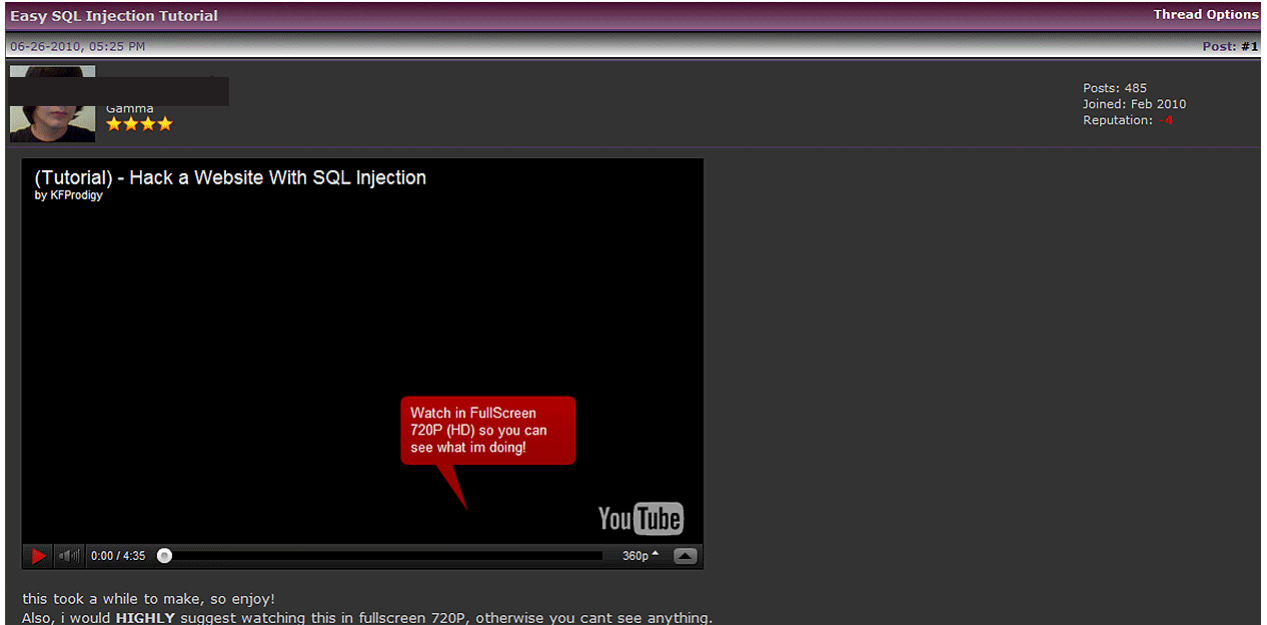
Most frequent popular topics: June 2010-June 2011. Note: sample was 241,881 total threads.



Technically, forums provide tutorials and videos for common hacking techniques such as SQL injection – the most common method to steal data.

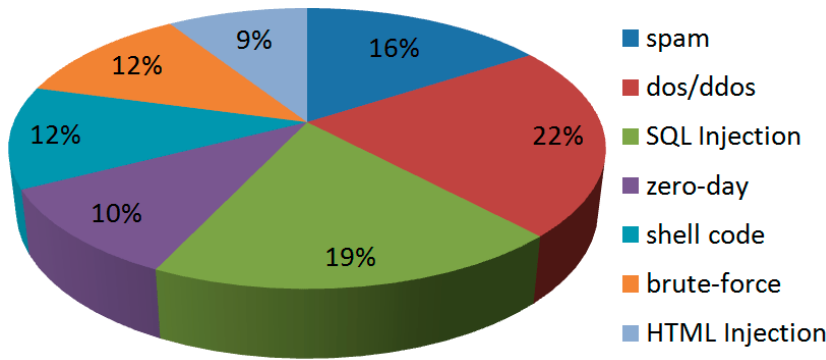


SQL injection tutorial:



DDOS was the most frequently discussed topic with 22% of threads with SQL injection a close second with 19%.

Top 7 Attacks discussed in HackForums.net in the last year (# threads with keyword)



Most frequent popular topics: June 2010-June 2011. Note: sample was 241,881 total threads.

However, a fair bit of nontechnical training takes place on forums. For example, hackers have developed extensive tutorials on "Social Engineering" which is described as "manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action."

A Beginner's Guide to Social Engineering
Thread Options

04-14-2009, 06:34 PM (This post was last modified: 10-12-2009 10:44 AM by Kn1ght.)
Post: #1

<3
★ ★

Posts: 54
Joined: Apr 2009
Reputation: 4

A Beginner's Guide to Social Engineering

By: UI2BAN

Contents:

1. Introduction to Social Engineering
2. Examples of Social Engineering
3. Methods of Social Engineering
4. Advantage of Social Engineering
5. Are You a Social Engineer?
6. Final Thoughts

[align=center][size=1]1. Introduction to Social Engineering

Before I get into the World of Social Engineering, please keep in mind that this guide was made for, but not limited to, beginners. So with that in mind, let's get this show on the road! So what exactly is social engineering? I'm sure this question has been asked a million times, you're probably even asking yourself this now! To cut around the BS and throw away the leftovers, social engineering is the act of manipulating people into revealing information or tricking the slave to performing actions that are beneficial to the user. That's it! To put it in simpler terms; ever trick someone into doing something dumb, or told a lie to get someone to tell you something, or even get your friend to lie for you to get "something" out of it? That's social engineering my friends! It's that simple, and *anyone* can do it, even the weird kid in your class that's deaf that tries to talk, but can't, but still tries anyway! Although social engineering is relatively easy to do, and can be used anywhere at any time, the very world of it is complex, there is no "one-way" to doing things. Your options are endless, so make use of it!

2. Examples of Social Engineering

Some tutorials get quite specific and provide case studies:

[Noob Friendly][Tutorial]Introduction to Social Engineering and Human Manipulation
Thread Options

06-26-2010, 03:05 AM (This post was last modified: 06-26-2010 12:51 PM by Ckt3.)
Post: #1

Introduction :

"Social engineering" is an act of psychological manipulation, it was popularized by hacker-turned-consultant Kevin Mitnick. The term had previously been associated with the social sciences, but its usage caught on among computer professionals and it is now a recognized term of art.

-How to social engineer a person ?

First to social engineer a person, you need to have as many information as you can about him, the most important ones are:

- 1- What makes him mad?
- 2- What makes him sad?
- 3- What does he really like?
- 4- What is his job?
- 5- What makes him always exited?

And sometimes, age helps. (You'll see that in the examples later on)

You need to have a special goal when you social engineer a person, I'm gonna first talk and give examples about social engineering and computer hacking, like to get information about everything related to accounts and things into the computer. Then, I'll talk and give examples about real life social engineering and mind manipulating.

Social engineering and Hacking a person:

Example 1 :
 slave : Male, 13 years old, he really likes playing online games and especially poker, winning in poker makes him always exited.
 Goal : Get his poker chips.
 Plan : Add him on IM or chat with him somewhere, say that you sell online poker chips i.e on Facebook (Now, because you said that you are a seller, he will talk to you seriously). He will probably ask for the price, let's say a very low price for a big quantity, but add to your reply that you need at least 24h before you get the poker chips. Ask him if he can wait because you will double them (" you will double them" -- > makes him exited) so now he will probably ask you :how much will you double them?" You say there is a secret cheat site, it's undetectable, and that you can double your chips in 24h (You must create a site with this form asking for Facebook mail and password, with some additional details like "What was your last server on poker, on Facebook?" etc.. and you should work on the design..) so he will probably ask for it, you should not give it directly..just wait till he asks for it twice and give it to him asking/begging him to not spread it and share it with others. And here you go, wait a second and check the results of your forms. Then, you'd have his account.

Example 2 :
 slave : Male, 28 years old, Business man.
 Note that you should always think about if the info you have can give you more tips and abilities to do in your plan. Like here, you will see that the plan will work simply because a business man is always busy and wont think an hour or two of your plan, since he has work, so you may need to know that this will help.
 Goal : Accessing his Paypal.
 Plan : Getting his mobile number, calling him from a public phone with a strange voice, (first you must call paypal to see what words they may say and you may use them..its better to be more real) So, you will say here : Hi it's paypal customer services department we got your mobile number regarding the account " his paypal email " and we're sorry to bother you but we had a database problem with our servers so we're trying to reset everything and get all the information back. You can get your paypal online as before, we're sorry for any inconvenience this may cause, can you please provide us with your old password ? We will email you a reset link so you can change it later on for more security.
 This should work, also remember to call him in a time where he cant be online so he wont go and check if he's paypal is online and working fine etc..

Example 3 :
 slave : Girl.
 Goal : Her Facebook.
 Plan : add her on IM (or if you already have her) Create a fake Facebook login page, talk with her a bit and tell her that she has a really ugly picture on Facebook and link her to it (your link .. the fake log-in one) and she will definitely go there because this always works on girls.

There are even tutorials on avoiding the grip of law enforcement. In the picture below, we see a guide to ensuring files on a hard drive are properly erased to prevent legal repercussions in the event of being incarcerated:

Stay safe as a hacker - Erase your tracks [File Shredding]
Thread Options

06-08-2011, 08:32 AM
Post: #1

Posts: 209
 Joined: Oct 2010
 Reputation: ▲

File shredding with exif

- In windows OS

Why do I need this?

When you do delete your files on your hard drive they are in fact **not** deleted. This meaning if the police or anyone else with some kind of disk recovery tool, accesses your PC, they can recover deleted files and use it as evidence against you. This could be all the CP you used to store, or the configuration files of some IRC-bawnet shit, or simply all the fucked up porn you never ever want you new GF to find.

How it works when you delete a file.

When you delete a file in windows it simply tells the system that the file is no longer needed and can be overwritten, but until this happens the file it self exist 100% on your hard drive. When space is need the system will simply use some of the space that the file obtained and thereby the file losses some bytes now 70% of the file exits, but this will still be enough to be used as evidence against you.

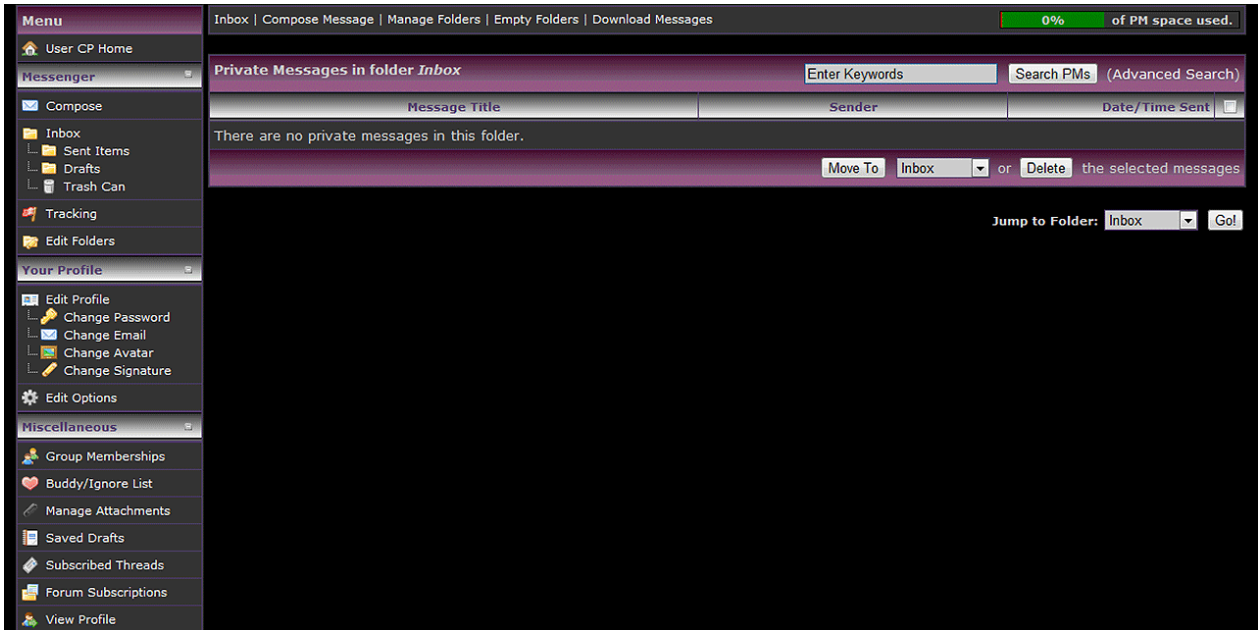
Let me give you a scenario to help me explain.

You are sitting in you moms basement with you epic windows machine pulled out, where you control this awesome 1337 h4x0r botnet with your RAT client. And you often browse HF where you brag about how many RAT installs you got, and post pictures of your epic 1337 defacements of different websites. You know that if the police finds the server file you used to infect people with, and the tutorial you downloaded from HF, or simply the internet history of your browser they got what they need. So you delete everything frequently.. but is it gone?

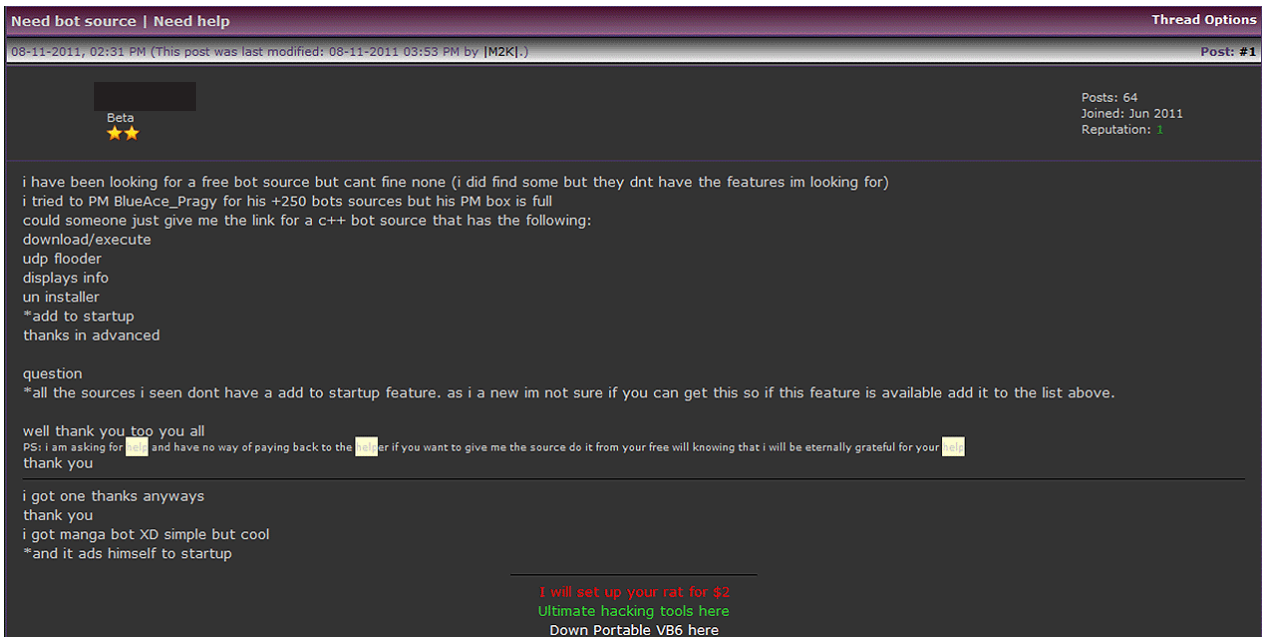
Disclaimer (Click to View)

The Tutorial

2. Communications – The ability to communicate with anonymity is a cornerstone of hacking. Forums provide a platform for to discuss miscellaneous topics as well as host internet relay chats (IRCs) for real-time communications, often used when executing an attack. Below is an example of a forum’s “personal message” system (or PM):



3. Collaboration – Hacking has become more and more complicated with several components required to execute attacks. Forums provide a conduit for hackers to volunteer help and information regarding attack campaigns.




Part 2: <http://www.hackforums.net/showthread.php?tid=929223>

All credit goes to me (TheUnknown1) from experience and learning.

I can find out or dig information on anyone for a fee if you are interested in my services. PM me on how we can do business. I will be asking \$35 per person. I can track down a lost friend, find phone number of a person, find the address of a person, find their relatives, and more. I will include a full report for those interested in my services.

How to hack facebook
 Hack with cellphone (tut)
 Protect ur identity (tut)
 Prepare 4 anything (tut)
 Art of human hacking

- Recruitment – Keith Richards described the Rolling Stones’ success saying “It’s really teamwork, one guy supporting the others, and it’s all for one purpose, and there’s no flies in the ointment.” To illustrate his point, Keith explained that Mick Jagger’s solo album “Goddess In The Doorway” should have been titled “dog shit in the doorway.”¹ Likewise, hacking has become a group sport and its success depends on a quality team. To be successful, you need to have expertise in various areas such as web attacks, DDOS, malware, etc... If a single hacker finds or conceives of a potential target but only has some portion of the expertise required to successfully execute an attack, where do they go? Here a hacker group, calling themselves the Wraith, recruits members:



List of content

- *What is the Wraith?
- *The Requirements.
- *Disallowed activity in the group.
- *The user-bar.
- *The Application.
- *Leadership.
- *Important notices.

What is the Wraith?

The Wraith is the combination of years of achievements, skills, and power of all its members in one entity. We are a group of free-thinkers, hackers, philosophers, ordinary people that don't want to be manipulated and abused. We are a group that fight as one, bringing down with any means necessary those who oppress and discriminate others. Our goal is to fight to our last breath, freeing the world from the clutches of the corrupt and the evil.

The Requirements.

- * You must contribute to the group. This means posting regularly and aiding members when needed. Inactivity will be met with removal from the group.
- * You must be open minded. Acceptance of diversity is key to being a Wraith.
- * You must be respected by others. You must not have negative reputation.
- * You must be respectful to other Wraith members.
- * You must have decent grammar and spelling. Unreadable applications will be ignored.

Disallowed activity in the group.


- *Inactivity.
- *Scamming.
- *Infecting fellow members.

Recently, one forum participant, claiming to be a security researcher, hosted a hacking contest, RankMyHack.com, which was advertised on hacker forums. This effort took recruiting to a new level with a ranking system, similar to how eBay ranks sellers based on reliability:

Up until now, when you met another hacker on an IRC or forum, there was no way to indicate if that hacker had any skills what so ever, RankMyHack.com was built to give a clear indication of a hackers general abilities. It also serves the purpose of tracking a hackers hacking achievements under their current alias allowing for other hackers to quickly establish the calibre of hacker they are talking to. (Sic)


★▶▶ [HOT] RankMyHack.com - The Hacker Ranking System [+300 Users] ◀◀★
Thread Options

07-19-2011, 01:25 PM (This post was last modified: 08-22-2011 03:00 AM by sol@rs.)
Post: #1



Network Penetration Tester
★★★★★

Posts: 1,716
 Joined: Dec 2009
 Reputation: 100



May I officially present RankMyHack.com


What Is RankMyHack.Com?
RankMyHack.com is the worlds first dedicated hacker ranking and dueling system.

How Does It Work?
RankMyHack.com works by hackers submitting evidence that they have hacked websites in exchange for 'Ranking Points', the more popular the site you hack, the more ranking points you receive.

What Do Ranking Points Do?
Ranking points earn you a place on the RankMyHack.com leader board, the more high profile your hacks, the higher up the leader board you will be placed.

What Are Duels?
Ranking points can also be used to challenge other hackers to one on one hacker duels. Hacker duels consist of one on one digital combat where the hacker that can hack the most popular sites with in the specified time limit take a stake of their opponents total ranking points.

How Do I Share My Rank?
Your rank and hacker statistics are shown in the official RankMyHack.com signature shown below. This signature can be used on any MyBB or HTML supported forum/website to prove that you have the skills to back up your posts, and every user that signs up by clicking your banner earns you 100 ranking points. It couldn't be simpler!



```

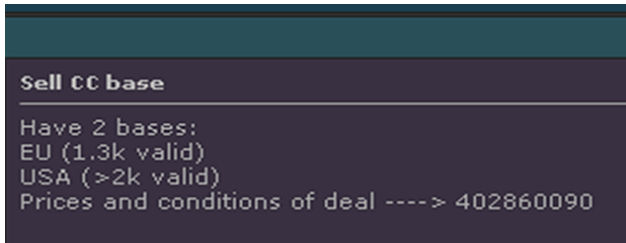
            [USER]: a01ar
            [RANK]: 16/118
            [RANK_POINTS]: 3000
            [SITES_HACKED]: 0
            [DUELS_HON1]: 0
            
```

How Do I Sign Up?
Anyone can sign up to RankMyHack.com providing they have a verifiable email address, to sign up go to RankMyHack.com and click 'Login/Register'

What Are You Waiting For?
You've talked the talk, now its time to walk the walk and join the future generation of hackers in the new front line for digital combat.

5. Commerce – A key function of hacker forums is commerce. Members can buy, sell or trade but in this case the goods are stolen data and attack software. In this case, the exchanges resemble the type of commerce seen on Craig's List where buyers contact sellers directly with no transaction engines processing the engagements.

When data such as credit cards, social security numbers or login credentials are stolen, the hacker will post the information, often with some evidence, to the forum for prospective buyers. Here, a hacker tries to sell credit card numbers:



Here, a hacker shows the full set of personal details as a proof that they have more:



Here, a hacker sells the database contents from dating site eharmony.com.

provider	Junior Member
provider is offline	
Join Date: Dec 2010	info: www.eharmony.com
Posts: 5	class: compromised db, compromised email channels
Reputation: 0 +/-	common price: \$2000 usd
	closer price: \$3000 usd
	additional: different parts of the infrastructure compromised
	contact: 80-90-50, eprovider@live.com

6. Social interaction – Since forums provide a sense of community, they are a natural location for social interaction. The anonymity in the forums allows blunt exchanges and questions. Topics can range from religion, philosophy, books, movies, TV, relationships, sex and even acts of revenge.

Here, a hacker discusses meditation:

01-29-2011, 12:59 AM Post: #3

I do it every day. Basic meditation is practicing how to clear your mind at will, which is useful because people just can't do that without practice. When you reach a point of enlightenment where you begin to question everything, you can become overwhelmed and not be able to focus on general life. Meditation helps "empty your cup", as Buddhist monks say, because when you clear your conscious mind it is like buying a new card of RAM for your computer. When your conscious mind is given information by the subconscious, he processes it rationally. When it has finished processing it, the subconscious stores that information and generates new information to be processed. If your conscious mind never empties itself after it is finished processing, first of all you will be so full that you can't focus on real life. Second of all you won't be able to take in anymore information from the subconscious to process.

Meditation can also be used to clear the conscious mind in order to generate thoughts intuitively. The more stuck you are on logic, the harder it becomes to think intuitively, which can lead to problems in your life. There are lots of spiritual aspects to meditation as well, but.. people turn their heads when people talk about that, which gives a good hint that they don't meditate! 😊

01-29-2011, 01:01 AM Post: #4

Yeah I've tried it. Didn't have any tremendous effect.

01-29-2011, 03:00 AM Post: #6

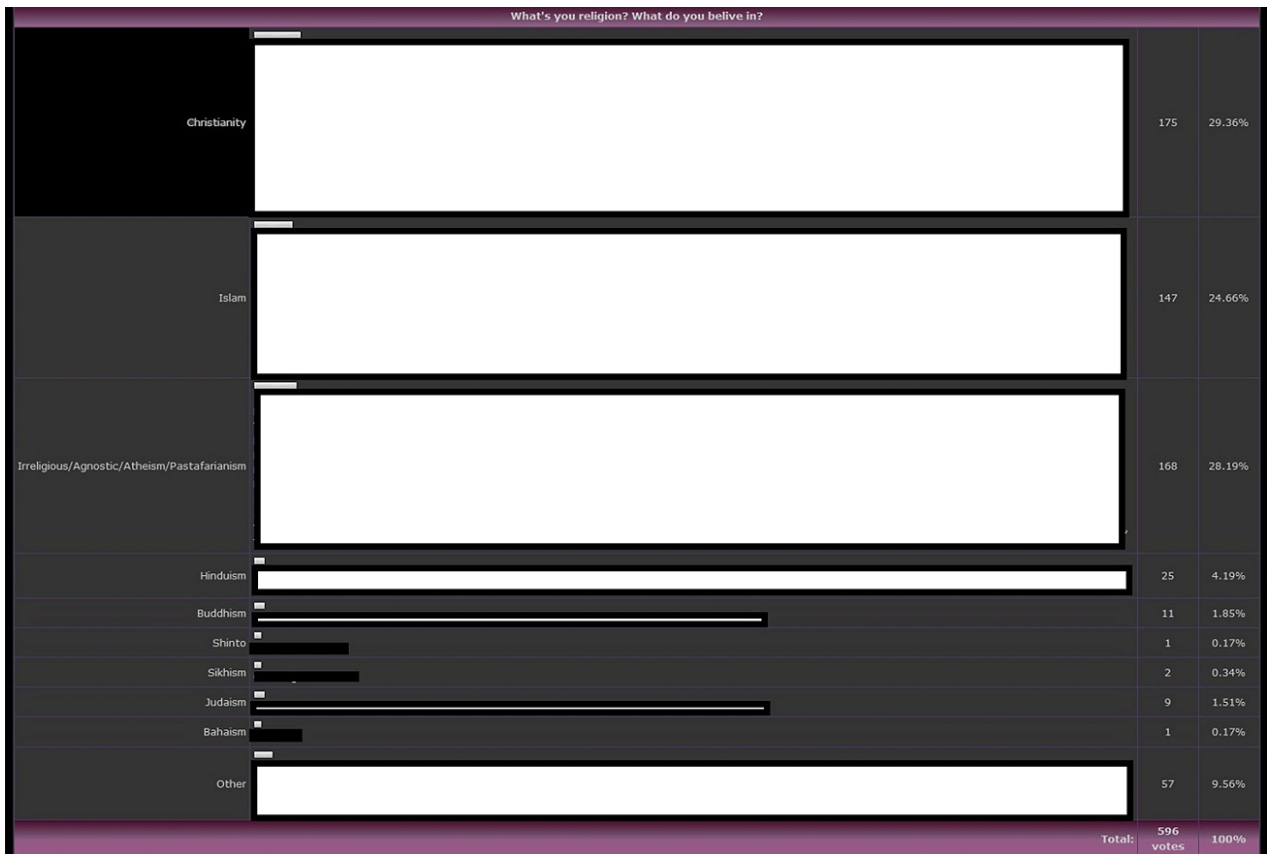
As a Wiccan Priest I meditate all the time. I also perform Inner Journey's and Soul Retrievals while meditating. These rituals bring me closer to my inner being and help me to become one with the Goddess & God.

.....skillful to rouse Leviathan.

01-29-2011, 03:27 AM Post: #7

I have tried it, it is a really good stress remover.

Here, hackers take an informal poll regarding religious views (we have obfuscated some derogatory comments about various religions):



Conclusion

In June 2011, the UK's Guardian [explained](#) how hackers are acting as FBI informants. The article cited the importance of forums when it came to apprehend cyber criminals:

...popular illegal forums used by cyber criminals as marketplaces for stolen identities and credit card numbers have been run by hacker turncoats acting as FBI moles. In others, undercover FBI agents posing as "carders" – hackers specializing in ID theft – have themselves taken over the management of crime forums, using the intelligence gathered to put dozens of people behind bars.

The article went on to suggest that nearly 25% of hackers act as FBI informants. Although this figure seems too high in our opinion, it highlights the value of studying hackers for security professionals to focus on actual threats and devise new defenses based actual attacks. Specifically, studying hackers gives:

- › **Clues on what hackers are attacking.** This helps security teams prioritize the overwhelming number of vulnerabilities they need to remediate.
- › **Technical insight into hacker activity.** Hackers, by definition, are early adopters and innovators which is often detailed in forums.
- › **Business trends of hacker activity.** By monitoring the sale of data and how hackers make money, security teams can monitor what type of data is most attractive on the black market.
- › **Future directions of hacker activity.** Forums today have much more discussions regarding mobile computing. Not coincidentally, mobile malware has risen just as dramatically. This episode, to paraphrase hockey great Wayne Gretsky, assists security teams to not keep their eye on the puck, but rather, know where it's going.

Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative goes inside the cyber-underground and provides analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of Imperva's Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, Web application security and cyber-crime business models with the goal of improving security controls and risk management processes.