iMPERVA®

Hacker Intelligence Initiative, Monthly Trend Report #13

Monitoring Hacker Forums

ADC Monthly Web Attacks Analysis, October 2012

1. Overview

Imperva analyzed one of the largest-known hacker forums with roughly 250,000 members, as well as other smaller forums. Using search capabilities, we analyzed conversations by topic using specific keywords. We found:

› **SQL injection is now tied with DDoS as the most discussed topic**. *Both topics got 19% of discussion volume. Last year, SQL injection was second with 19%, and DDoS came in first place with 22%. Ironically, of the $25 billion spent on software security, and we believe this means less than 5 percent of security budgets is allocated to products that cannot even recognize SQL injection attacks – let alone stop them. We believe this imbalance encourages hackers to continue to learn and deploy this attack method.*

› **Social networks today pose a major interest for hackers**. *They are becoming a prominent source of information, pictures, and potential monetary gain. Facebook was the most discussed social media platform, commanding 39% of discussions with Twitter a close second at 37%.*

› **E-whoring is becoming one of the most common methods for beginner cyber criminals to gain easy money.** *We saw more than 13,000 threads in a dedicated forum. E-whoring is a practice of selling pornographic content, while pretending to be the person, usually a female, photographed.*

> *Many security professionals do not spend time exploring hacker forums to understand the tools and techniques hackers use to attack.*

2. Methodology

Imperva 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 conversations 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. 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, invitation-only forum.

During our research we have encountered many other hacker forums with very similar content and professional opportunities. Some forums have very few members; some address specific communities or nationalities.

The more "professional" forums are in English but they attract an international group. Due to obvious anonymity requirements, hackers don't identify themselves or their nationality. Yet it is safe to assume that forums host a very internationally diverse group. The English grammar, or lack thereof, of many posts, leaves little doubt that the author is not a native English speaker.

On the other hand, we have also encountered nation-specific hacker forums: for example, Pak Hackerz, Indonesian Hacker Newbie Community, Italian Hackers, El Hacker, Comunidad Underground Hispana and more.

We have focused our efforts on the largest forum, and the quantitative analyses were mainly conducted on its data, similarly to the analyses performed in our previous hacker forums report.[1] However, our conclusions and examples are drawn from 18 forums scanned during our research.

---

[1] http://www.imperva.com/docs/HII_Monitoring_Hacker_Forums.pdf

3. Content Analysis

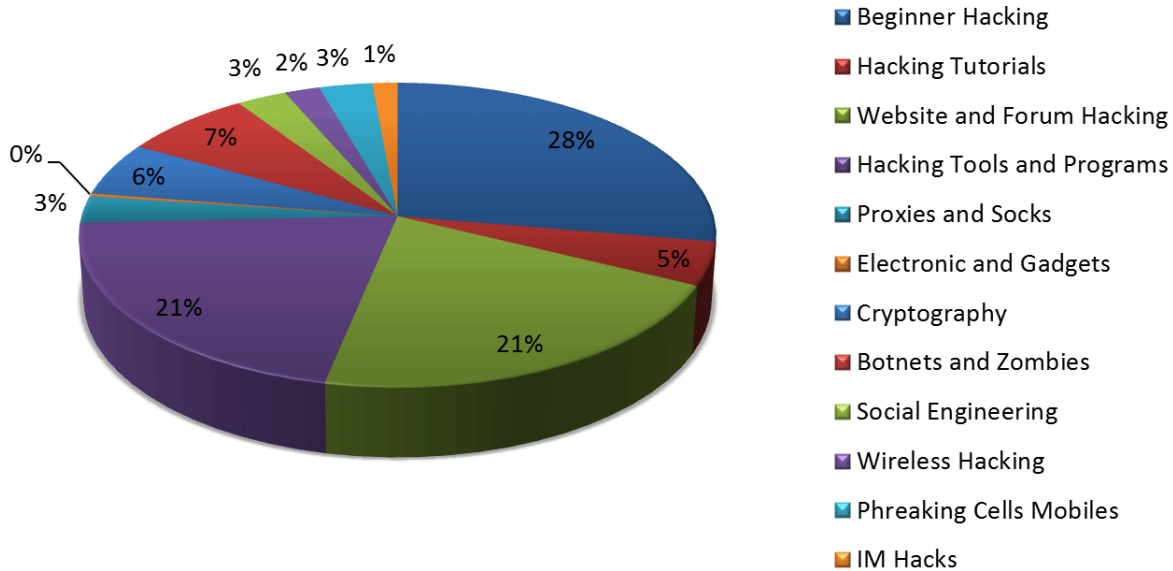Hacker forums serve several functions:

Training

Figure 1: Percentage of threads in each forum during September 2011-September 2012. Sample size was 439,587 total threads.

Our analysis shows that training comprises the most frequented topic, meaning forums mainly help aspiring hackers learn the trade, technically and nontechnically. In the monitored forum, 28% of the conversations are related to training and learning. "Beginner Hacking" sub-forum is the place where aspiring hackers can ask questions, learn about tools and methods, and publish their first successes in the cyber world. Another 5% of discussions include tutorials for various hacking methods. Posting a good tutorial can gain its author reputation in the community, and can lead to job offers, collaborations, and invitations to deeper, invitation-only forums. Taken together, about a third of the conversations are dedicated to hacker training and education, which make them the main topic of the forum.

Technical Discussions

Forums also evolve to fit changes of interest in technologies and trends. When there's a growing interest in a certain topic, a new sub-forum is opened to encourage more specific discussions. For example, a new forum titled "Decompiling, Reverse Engineering, Disassembly, and Debugging" was opened last December (not included in Figure 1 due to low number of threads). This may reflect growing professionalism and interest in higher level coding.
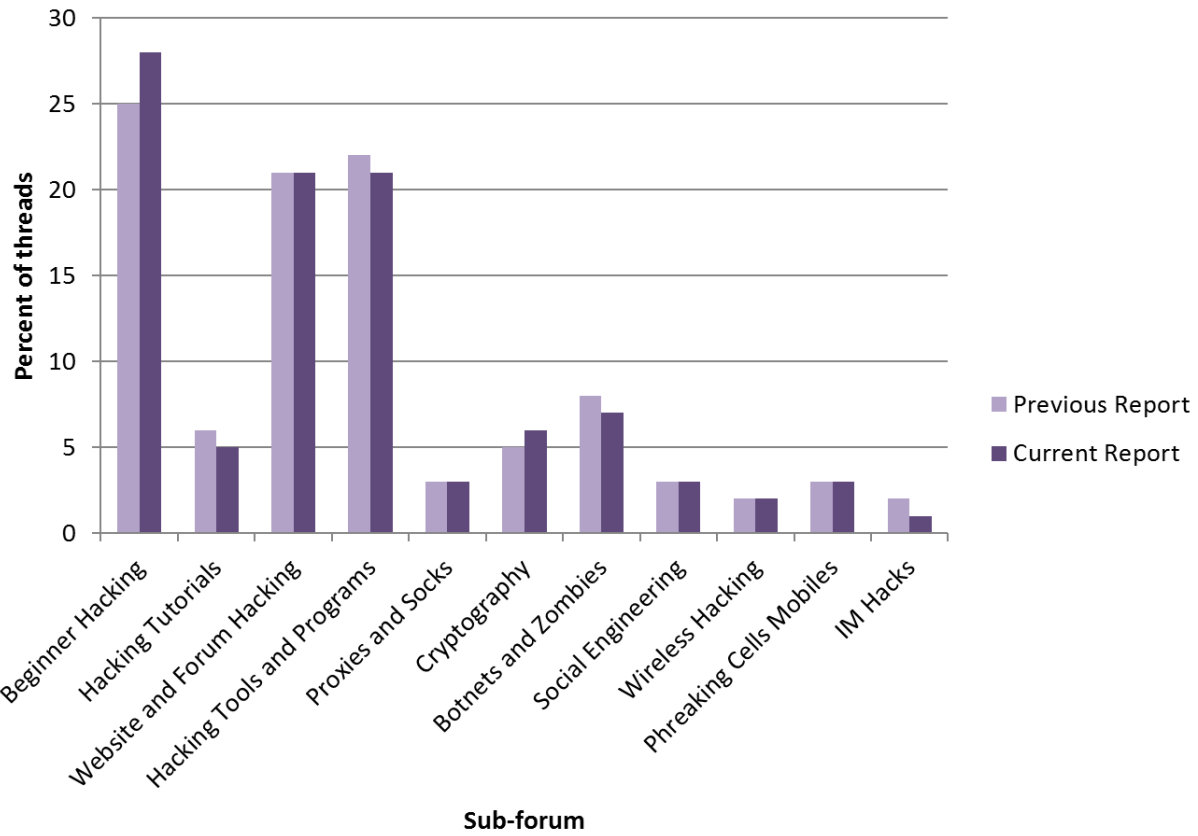
Figure 2: Changes in conversations per sub-forum.

We further analyzed the most frequently discussed topics by keyword. DDoS and SQL injection were the most popular topics.
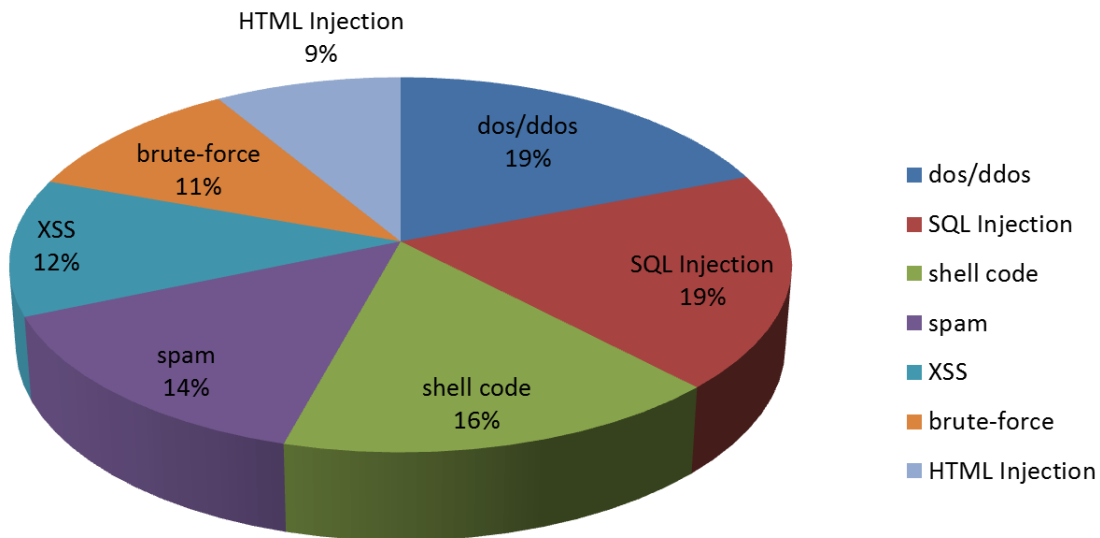
Figure 3: Percentage of threads with keyword, September 2011-September 2012.
Sample size was 439,587 total threads.

When comparing the results to the analyses we conducted last year (see Figure 4); the common topics seem to remain stable.
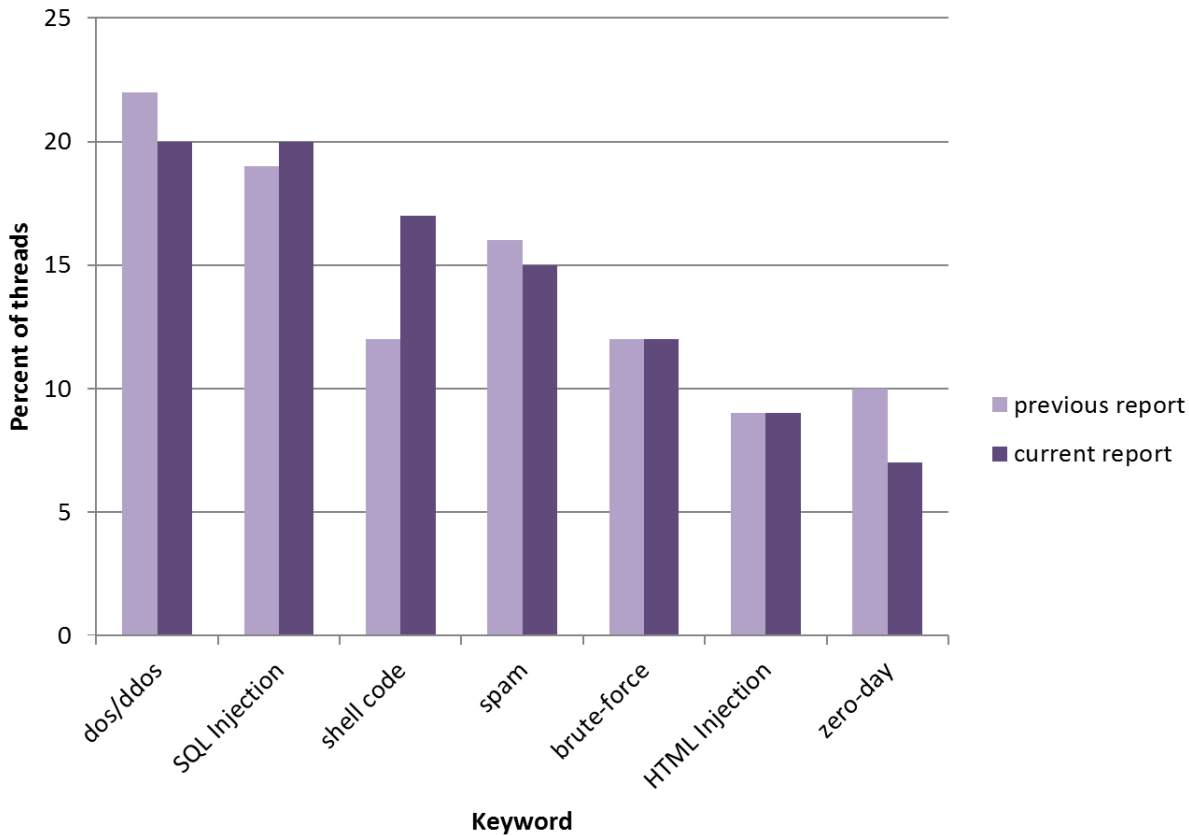

Figure 4: Top 7 attacks discussed.

Commerce

The abundance of job offers and advertising content suggests that one of the main services forums provide is a place to do business. The pages are filled not only with job offers, but with advertisement for paid services, Buy/Sell, ads and trading goods. Goods in the cyber world can be anything from Facebook "Likes," hacking tools, and Ebooks, to botnets and pornographic material. Some simple tools are shared for free, just to increase the status of the developer.

Transactions are usually made in ways that allow anonymity, like Bitcoins, Liberty Reserve, or even PayPal.
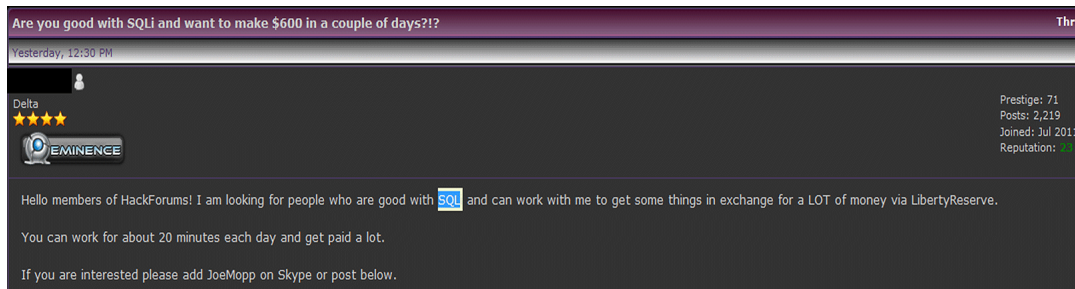
In the world of social networks, popularity has become a crucial commodity, and so trading social resources is becoming a common practice. People are willing to pay for google +1's, Facebook likes, Twitter followers, YouTube likes, and views.

Other things are for sale: The paranoid can find privacy services that offer secure internet connections. For example, one tunneling and encryption service offers different packages, ranging from 6/8$ a month for a shared/dedicated IP to 60$ for a full year of protected traffic. Accepted payment methods include Paypal, AlertPay, MoneyBookers, Liberty Reserve, Bitcoins, and Paysafecard.
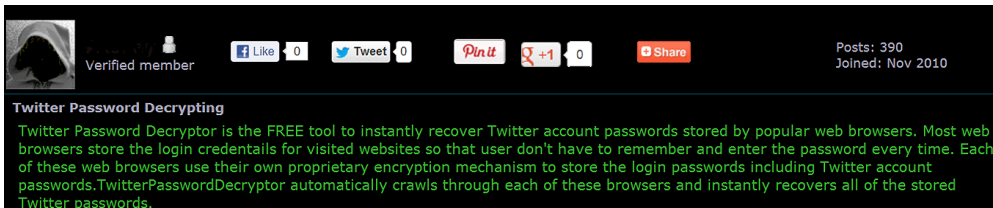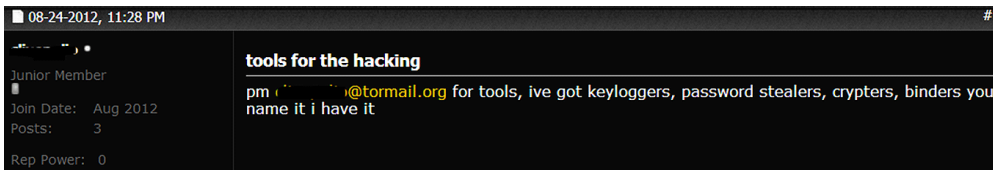
Social media

Social networks today pose a major interest for hackers. They are becoming a prominent source of information, pictures, and potential monetary gain. Hacking someone's Facebook account can provide the hacker with sensitive information, as well as cause a lot of personal damage.
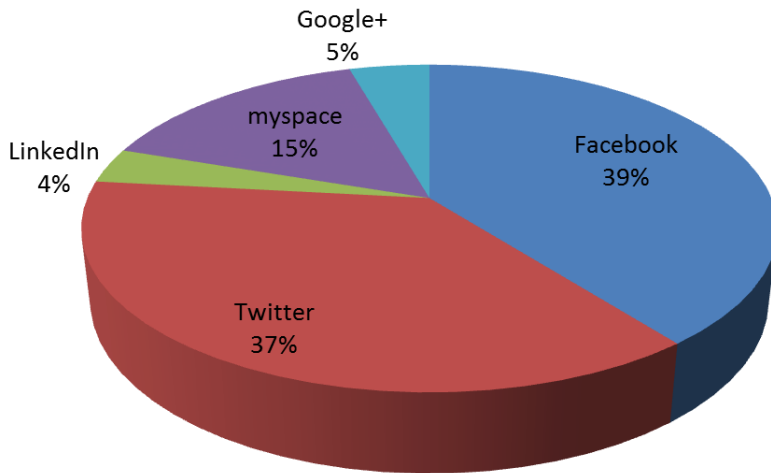

Figure 5: Social networks popularity. Percentage of threads with keyword September 2011-September 2012

Figure 5 illustrates the results of the content analysis we performed using different social media as keywords. It should be taken into account that the results of such a search include not only posts in which the content of the message, or its title, contained the keyword, but also posts in which the author himself used the social media for future contact. In the post below, for example, the author gives her Gmail account as a contact. When searching big amounts of data, it's impossible to separate the cases where the social media is the subject or target, or merely a means of communication. This, of course, happens more with email services than with social networks, and, for this reason, email services were omitted from our statistics. That said, our results clearly show that Facebook and Twitter are the most popular social media today in hacker discussions. Many threads include requests to hack someone's Facebook profile, usually to settle personal matters. Common examples are spying on one's girlfriend/ex, taking revenge, and just for lulz; sometimes these things get really complicated, as we see here:
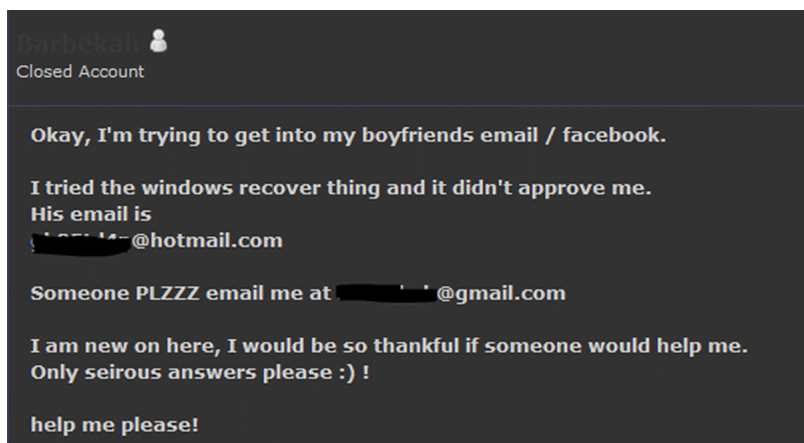

Figure 6: This hack request shows the use of email services both as a target for hacking and as a means of communication.

Can someone hack my wife's BF gmail for me?
« on: September 30, 2012, 01:20:27 AM »

Quote

n00b

Karma: +0/-0

ONLINE

Online

Posts: 13

hi,
Can someone hack one gmail account for me.
if you can hack it without changing the password better, otherwise he may change the password back by the time i can check their chats.
if it is not possible please give me the password by early mornign so that i will get some time.

If someone is willing I am even ready to pay.

Alpha

Prestige: 0
Posts: 11
Joined: Jul 2012
Reputation: 0

Hi there! I need help. Can anyone help me hack my stupid suitors facebook account? Here's what happened. He courted me when my boyfriend and i broke up. and when my boyfriend and i got back together i told that suitor to stop. He said he wouldn't want to stop. only to find out that he's been bragging about me being his girlfriend, already, to his friends. What an asshole! And right now I am 5 months pregnant and I am having a lot of problems with my relationship with my boyfriend since that freakin' guy told my bf that we had sex. now my baby is so unfortunate to be involved in this mess that guys caused me. the reason that I want to hack his account is to know what esle is he telling my bf via facebook. coz everytime i open my bf's fb account inbox i empty yet we always end up arguing about that shit that guy has been telling. this just have to be stopped since recently i was rushed to the hospital for a threatened abortion due to stress. Pls help me. Thank you

Hacking an account doesn't have to be done by technically exploiting a vulnerability in the application, and this does not necessarily require coding experience. Easier ways involve social engineering methods, in which the attacker manipulates the victim into giving away his credentials, thus providing the attacker with all he needs to break into the account.

08-26-2012, 03:13 PM   Post: #2

Gamma
★★★★

Prestige: 9
Posts: 261
Joined: Aug 2012
Reputation: -2

Security Questions, then manipulate the person who you are hacking the answer, (make another account, do some BSing, say you are from Facebook and need to know the answer).

Also, if the question is about food then the answer is 50% of the time "pizza" or "ice cream".

Hacking an account also requires bypassing, or sometimes exploiting, security mechanisms like security questions, geolocation detection, and password recovery.

Re: Need help accessing facebook
« Reply #2 on: September 04, 2012, 01:26:12 pm »

Quote

Administrator
Hero Member
■■■■■
Posts: 530
Rep: 25
Gender: ♂

Honestly outside is sniffing their network traffic, installing a keylogger, or distracting them and hopping on their computer, you could either crack their password, guess their password reset question, or find a vulnerability in facebook that allows you to access accounts while bypassing legitimate authentication.

That being said, don't hope on finding the last of that list because I doubt facebook is that stupid.

Report to moderator   Logged

As we mentioned earlier, popularity in social media is becoming a valuable resource today. Many forum discussions contain requests to buy Facebook friends and Likes, Twitter followers and other types of social currency. There are, of course, many who are willing to provide the, service, for variable prices.

Beginners are willing to provide the service for free, in return for positive feedback ("vouches"). This serves both as a learning platform and a way to build hacking reputation.

Special emphasis is given in many ads to the origin and quality of likes/followers. Apparently sites have obtained a certain ability to identify and ban users who use automated scripts to increase their popularity. This is reflected in the discussions in the forum regarding such services, and service offers state specifically that the likes would be provided (or appear to be) by real human users and not bots.

Likes and followers can be used to gain rank, win competitions, and many other causes that can often be translated to monetary profit. Such competitions are usually local; therefore the origin of voters (likes, fans, followers) must fit the specific case to look reliable. Recently, it was claimed that out of 200,000 likes to the Facebook page of Israel's Prime Minister, Benjamin Netanyahu, only 17% are in fact Israeli profiles.[2] About 52% were of American citizens, and, more surprisingly, 3% were Indonesian. This publication raised a lot of public criticism, demonstrating the importance of suitable geolocation and characteristics of the profiles, and not only their amount, when it comes to popularity wars. This is also reflected in related discussions in forums:
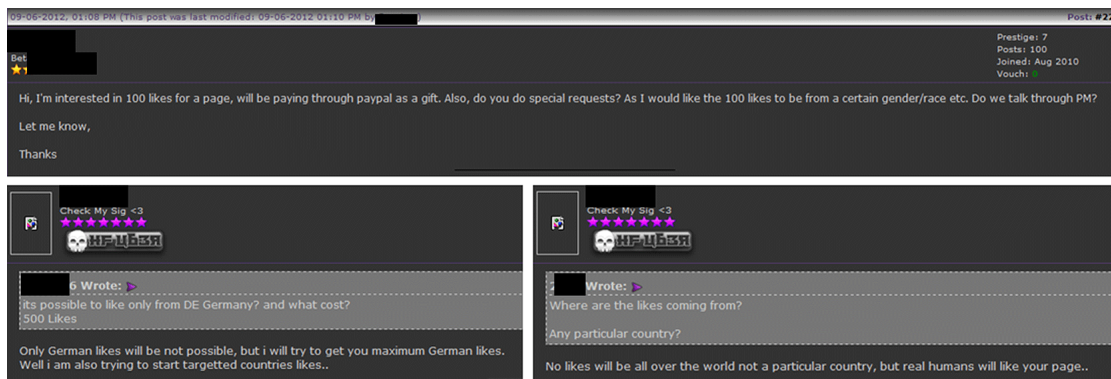
There are always limitations:
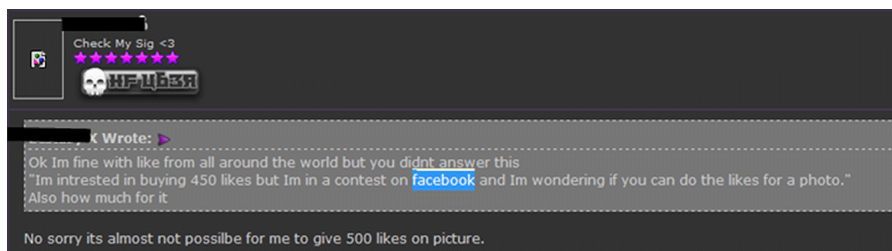
And the prices are usually negotiable:

[2] http://www.holesinthenet.co.il/archives/42585#comment-41425
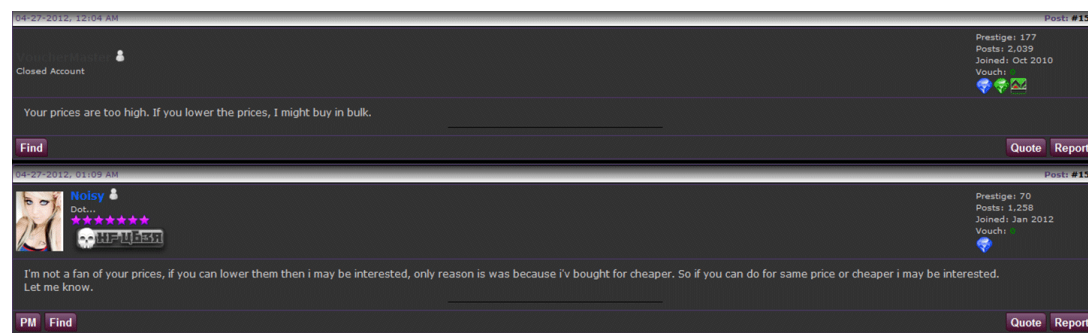
Trading Facebook friends is also possible:

```
I have 2 facebook Accounts having 5000 friends in each account, I will suggest all friends to your account upto 5000 to 10000 friends in just 10-15 minutes.

Add me on skype = Clones.ali

Prices are below..

5000 Friends suggestion = $5
10000 friends suggestion = $9

=> Friends are all over the world.

=> All friends are real i have added them by myself.
```
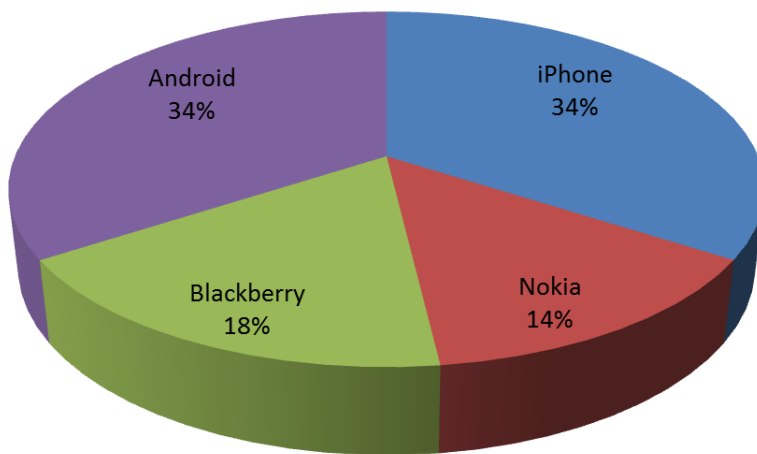
Being popular was never so easy.

Mobile Platforms

Figure 7: Popularity of different mobile platforms. Percentage of threads with keyword September 2011-September 2012.

A closer look into conversations about mobile platforms reveals that the majority of discussions deal with different methods to unlock mobile devices, namely jailbreaking Apple iOS devices and rooting Android devices. Jailbreaking is the process of removing limitations imposed by the manufacturer in order to gain root access to the operating system. This enables the user to download additional applications, extensions, replace system settings and perform operations that are unavailable to the normal user. While not illegal, jailbreaking is considered by Apple a violation of copyrights and voids the warranty for the device.
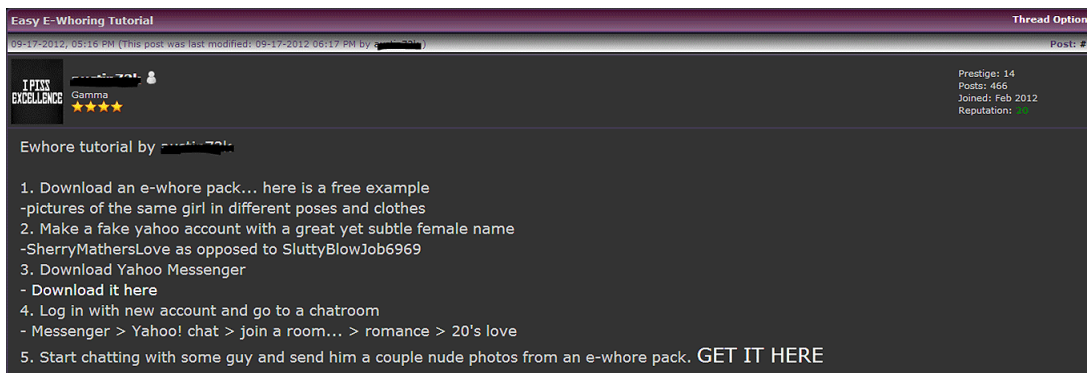
Other common topics are comparisons between different models and manufacturers ("iPhone 5 vs. Samsung Galaxy S III").

4. E-whoring

With more than 13,000 threads in the dedicated forum we monitor, e-whoring is surely becoming one of the most common methods for beginner cyber criminals to gain easy money.

E-whoring is a practice of selling pornographic content, while pretending to be the person, usually girl, photographed. It is considered a form of social engineering, when the victim is misled to believe he is interacting with a girl who is sending him nude photos and video clips of herself. The attacker first has to get his hands on some "E-Whoring packages," like some photos or videos with pornographic material. Then he lurks for potential customers in adult chat rooms, or he initiates Skype conversations. The attacker pretends to be the girl in the pictures, sending some pictures to tease the client and then saying that for a payment of such and such dollars, would send some more pictures or even turn on the webcam. This whole time, he is actually playing the ready-made videos he obtained in advance. This way, money is transferred directly from the victim to the attacker, usually via Paypal or other transaction services, as described previously.

Beginner e-whores use forums to learn the trade, while the more experienced share their knowledge and advice.

Making money through e-whoring does not require great technological sophistication, but rather, success depends on social engineering skills. The challenge is to get the victims, often referred to as "slaves" in this context, to believe they are talking to an actual girl. The two excerpts below demonstrate how an e-whore should talk to be convincing and believable.

E-whores also use forums to exchange e-whore packages; that is, videos and pictures of girls. Some are given for free, and the more high, quality ones are for sale.
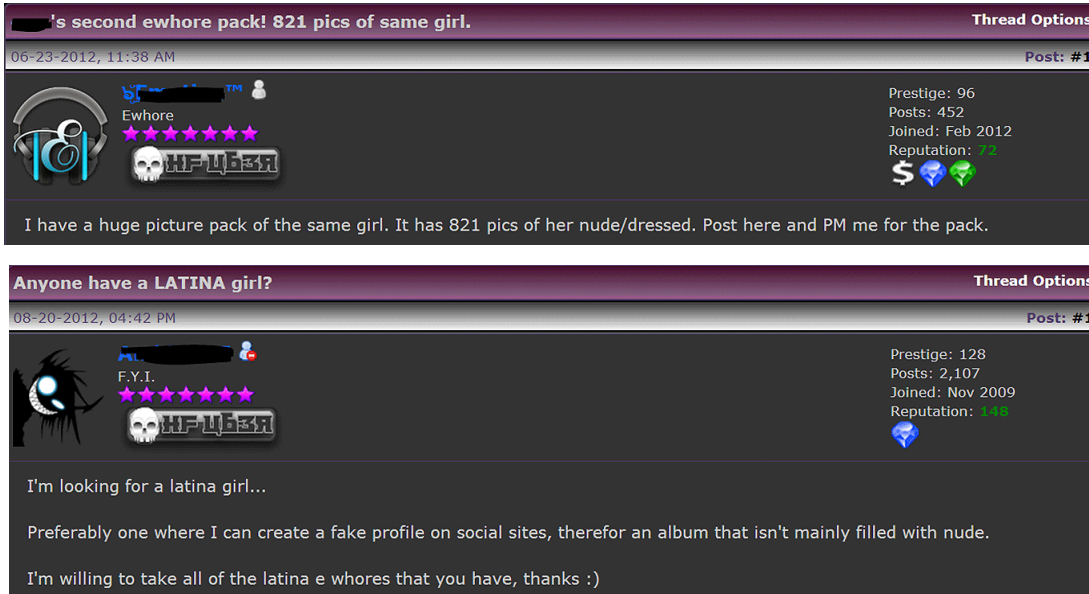
Why do victims fall for this? Why pay for nude pictures with all the freely available porn on the web? The point of e-whoring is that it mimics a "real" interaction. The victim is paying for the illusion of a brief relationship.
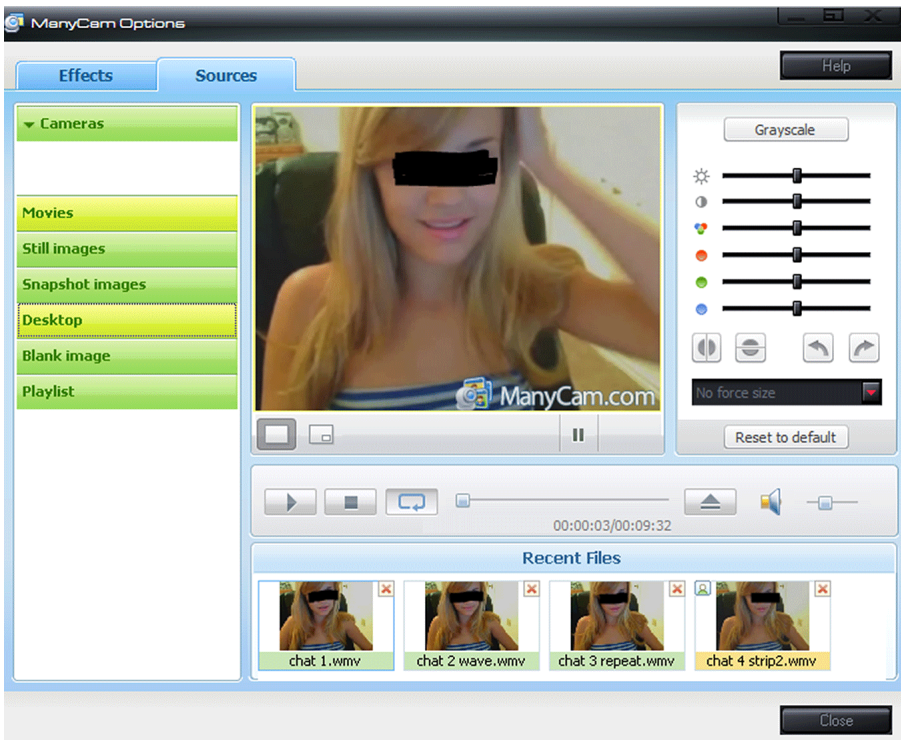

Figure 8: Examples of interfaces used for e-whoring. Ready-made video files are played to make the victim believe they are actually watching live webcam.

5. A Bit of Hacking Sociology

The forum we regularly monitor is not a very hardcore forum and, as we said earlier, is highly dedicated to hacking education and tutorials. It is a place for "newbies" (also: n00bz) to learn not only technical methods but the society's codes of behavior, brag about their first steps in the hacking world, make connections, and build their reputation. After a hacker makes himself a name, he can be noticed by the senior hackers or the admins of the forum. This can earn him an invitation to deeper, more serious forums or IRC channels, where the "real" hacking takes place. Each forum can lead to a deeper, more experienced and closed society. It seems that the open forums, though often disregarded as a place for "skids," are a necessary stage in the way to the insides of the hacking community.

Sharing and participation are very important factors in the hacking community, and members are expected to be active and contribute from their knowledge and experience. In one forum, a minimum amount of posts is a prerequisite to gain access to certain areas of the forum. For example, only members that posted a minimum of 40 posts are allowed to enter the E-Whoring section, and 10 more posts are required to gain access to the Hacking Tools and Programs section. The idea is "To protect the members who are contributing to the community, from ''leechers'' or people who doesn't want to contribute and get everything for free." (Sic).

Forums are also a place for gaming, technical advice, programming, exchanging freeware, and networking. Apart from the various hacking and technical sections, there are sub forums dedicated to conversations about religion, philosophy, music, anime, science, and politics.

Members use various means of communication. Sometimes the forum is used only as a billboard, while the actual negotiations and orders are done elsewhere. When posting a service, for example, authors leave an email address or a Skype name for future contact. However, this way of communication is less common. In most forums we had observed, members usually communicate via private messaging services provided by the forum. Hack requests and job offers often end with "for details PM me," "PM me if you are interested," etc. This way is convenient, as it does not expose any further identifying information about the hacker, while using email addresses or Skype gives away some of the anonymity.

Figure 9: examples for different contact information used in hacker forums: email addresses, private messaging, and Skype.

Although hacking forums are mainly in English, it is evident that many members are not native English speakers. The language used is usually slang, with nicknames, technical jargon, etc., and yet the grammar, or lack thereof, leaves no mistakes regarding the English proficiency of the authors. However, there are many hacking forums devoted to a specific nationality. We came across forums for speakers of Spanish, Arabic, Russian, Chinese, and more. Each of these communities has its own character, and sometimes forums reflect the politics and social dynamics of the real world.

Figure 10: A post in an Indian hacking community.

6. Summary and Conclusions

Our report highlights key technical and nontechnical trends in hacking. Many security professionals do not spend time exploring hacker forums to understand the tools and techniques hackers use to attack. This year's analysis shows:

› **Security teams continue to ignore SQL injection attacks at their own risk**. SQL injection continues to be the preeminent method of attack. Ironically, this year's Gartner's *Worldwide Spending on Security by Technology Segment, Country and Region, 2010-2016* shows that of the $25 billion spent on software security, we believe less than 5 percent of security budgets is allocated to products that cannot even recognize SQL injection attacks – let alone stop them. We believe this imbalance encourages hackers to continue to learn and deploy this attack method.

› **Consumers and enterprises that use social media need to better recognize the security risks posed by these platforms**. While privacy concerns often get most of the headlines, security should be just as much of a concern. Hackers have developed a profitable industry using services and tools to hijack accounts, dupe users, and spread malware.

› **Women should keep their clothes on when cameras are in the vicinity and men would better off getting to know the girl next door**. Pornography continues to drive cybercrime with the growth of e-whoring that exploits both unsuspecting males and females. Hopefully, building awareness of e-whoring will mitigate its growth.

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.