Monthly Threat Intelligence Report

December 2011

Demyo Inc. is one hundred percent American owned and one hundred percent IT security oriented company with headquarters in Miami, Florida, USA.

Demyo Inc. delivers comprehensive threat intelligence, penetration testing, vulnerability assessment, incident response, and compliance audit services.

Find out more at:

www.demyo.com

info@demyo.com

Tel. +1 201 665 6666

Tel. +1 786 203 3948

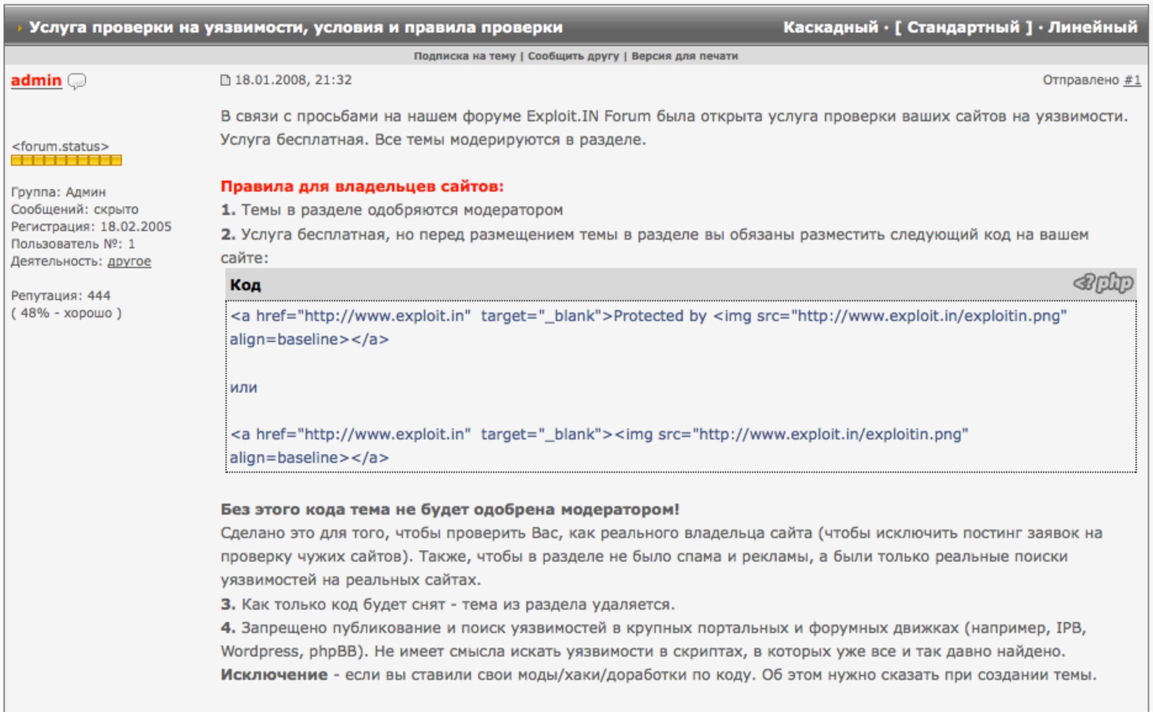
Miami, Florida, USA

Scope

Monthly Threat Intelligence report provides information on techniques and / or ways to attack company's assets and infrastructure. This report aims to be general in nature and is not tailored to any particular company. Please contact us for a threat intelligence service tailor for your company.

1. Hackers can check your webpage for errors

Russian hackers can check your webpage for flaws in exchange of backlink. Here is a post on one of the Russian underground forums explaining how it works:



В связи с просьбами на нашем форуме Exploit.IN Forum была открыта услуга проверки ваших сайтов на уязвимости. Услуга бесплатная. Все темы модерируются в разделе.

Правила для владельцев сайтов:

1. Темы в разделе одобряются модератором

2. Услуга бесплатная, но перед размещением темы в разделе вы обязаны разместить следующий код на вашем сайте:

Код

```
<a href="http://www.exploit.in"  target="_blank">Protected by <img src="http://www.exploit.in/exploitin.png"
align=baseline></a>

или

<a href="http://www.exploit.in"  target="_blank"><img src="http://www.exploit.in/exploitin.png"
align=baseline></a>
```

Без этого кода тема не будет одобрена модератором!

Сделано это для того, чтобы проверить Вас, как реального владельца сайта (чтобы исключить постинг заявок на проверку чужих сайтов). Также, чтобы в разделе не было спама и рекламы, а были только реальные поиски уязвимостей на реальных сайтах.

3. Как только код будет снят - тема из раздела удаляется.

4. Запрещено публикование и поиск уязвимостей в крупных портальных и форумных движках (например, IPB, Wordpress, phpBB). Не имеет смысла искать уязвимости в скриптах, в которых уже все и так давно найдено.

Исключение - если вы ставили свои моды/хаки/доработки по коду. Об этом нужно сказать при создании темы.

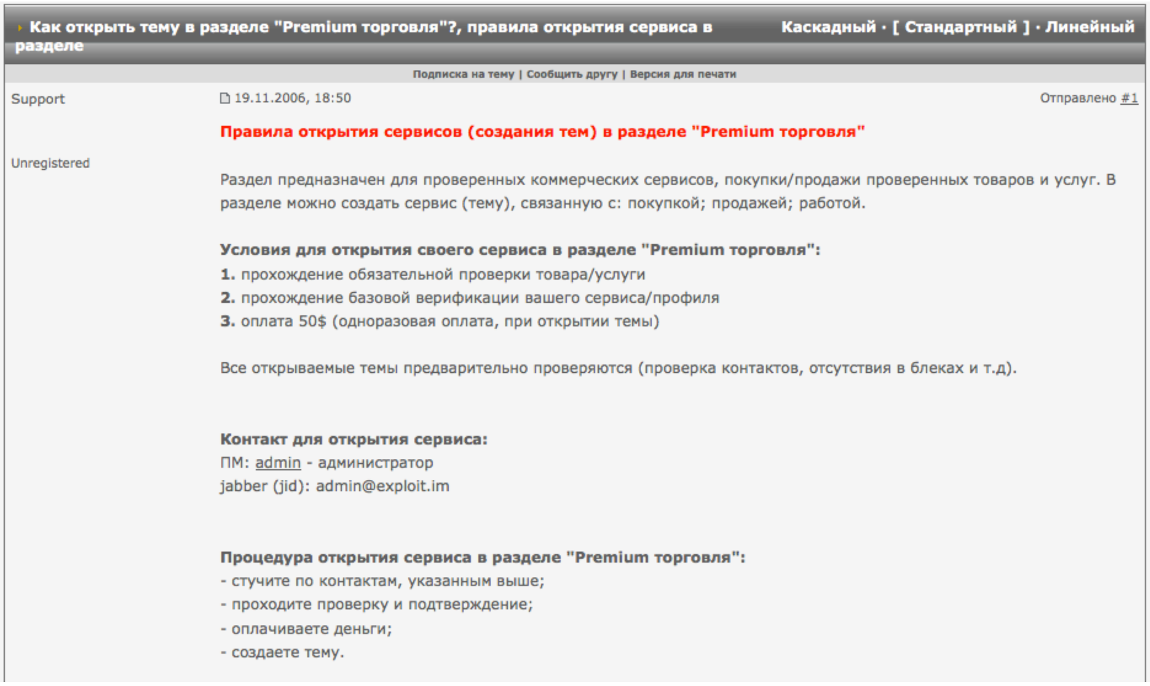
Some rules:

1. All posts in this thread have to be approved by moderators.
2. Service is free, however before posting you must copy – paste the following code into your website.
3. As soon as you remove the code above from your website all posts and advices will be removed from our forum.
4. It is forbidden to test any open source content management systems (for example Wordpress, phpBB, IPB), with exception of your plugins for that system or if you modified source code yourself.

Question comes up – is it safe to do? For some small hobby projects that should be fine. For big ones – no, as you are asking for trouble yourself. However, every web page is audited by hackers on the daily basis, you just don't get the report.

2. A premium posting area in Russian black market sales section

There is a new "premium" sales section in one of the underground hacking forums. This area is intended to be special, however no DDOS and carding services are allowed. All posts are from trusted posters. Posts should be oriented to services and one-time sales of goods are not permitted.



Как открыть тему в разделе "Premium торговля"?, правила открытия сервиса в разделе

Каскадный · [Стандартный] · Линейный
Подписка на тему | Сообщить другу | Версия для печати

Support

Unregistered

19.11.2006, 18:50

Отправлено #1

Правила открытия сервисов (создания тем) в разделе "Premium торговля"

Раздел предназначен для проверенных коммерческих сервисов, покупки/продажи проверенных товаров и услуг. В разделе можно создать сервис (тему), связанную с: покупкой; продажей; работой.

Условия для открытия своего сервиса в разделе "Premium торговля":
1. прохождение обязательной проверки товара/услуги
2. прохождение базовой верификации вашего сервиса/профиля
3. оплата 50$ (одноразовая оплата, при открытии темы)

Все открываемые темы предварительно проверяются (проверка контактов, отсутствия в блеках и т.д).

Контакт для открытия сервиса:
ПМ: admin - администратор
jabber (jid): admin@exploit.im

Процедура открытия сервиса в разделе "Premium торговля":
- стучите по контактам, указанным выше;
- проходите проверку и подтверждение;
- оплачиваете деньги;
- создаете тему.

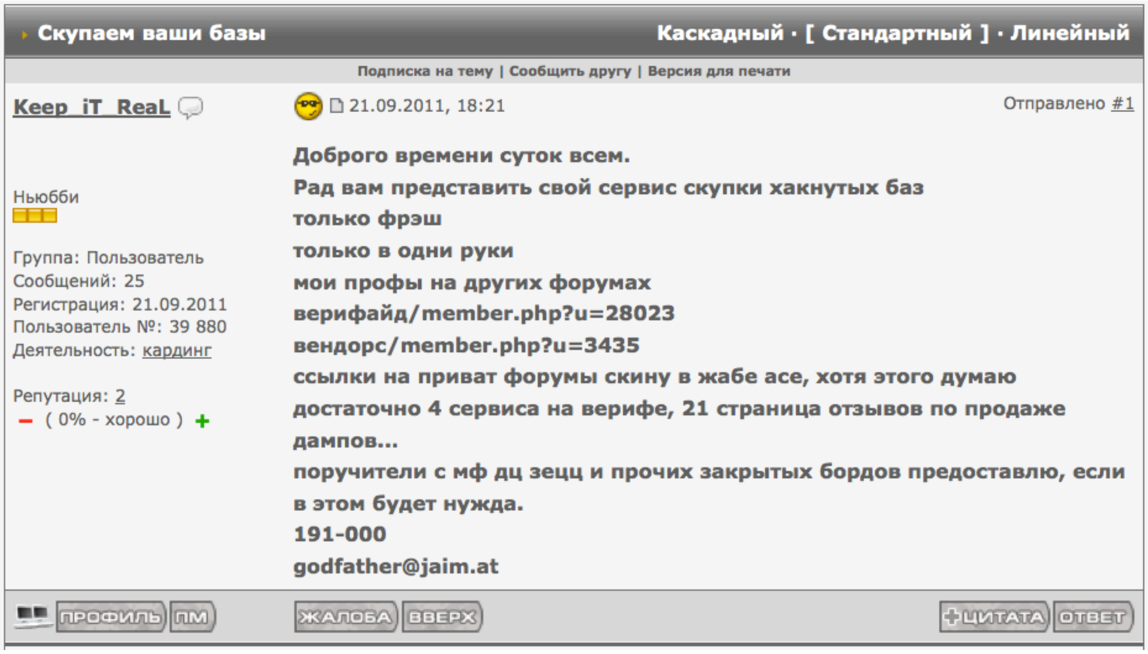
Rules are as follows:

1. We will check your product to make sure it is valid.
2. We will check your profile to make sure you are trustable seller.
3. You will have to pay $50 one time fee to open your thread.

This is yet another way how underground hackers make money. For the owner of the forum this is yet another revenue stream, for the seller it's a way to have his ad on the top of the list all the time. Should we explain why it is important to have your ad on the top of the list? A perfect example is craigslist, some people just keep on posting similar ad every hour or so, so it will get noticed.

3. We buy your hacked databases

This person is buying freshly hacked databases of any kind; he has profiles on other websites and provides links to threads. This way he can show others he is a seller in good standing.


Скупаем ваши базы
Каскадный · [Стандартный] · Линейный
Подписка на тему | Сообщить другу | Версия для печати
ПРОФИЛЬ
ПМ
ЖАЛОБА
ВВЕРХ
ЦИТАТА
ОТВЕТ

Keep_iT_ReaL

Ньюбби

Группа: Пользователь
Сообщений: 25
Регистрация: 21.09.2011
Пользователь №: 39 880
Деятельность: кардинг

Репутация: 2
(0% - хорошо)

21.09.2011, 18:21 Отправлено #1

Доброго времени суток всем.
Рад вам представить свой сервис скупки хакнутых баз
только фрэш
только в одни руки
мои профы на других форумах
верифайд/member.php?u=28023
вендорс/member.php?u=3435
ссылки на приват форумы скину в жабе асе, хотя этого думаю достаточно 4 сервиса на верифе, 21 страница отзывов по продаже дампов...
поручители с мф дц зецц и прочих закрытых бордов предоставлю, если в этом будет нужда.
191-000
godfather@jaim.at

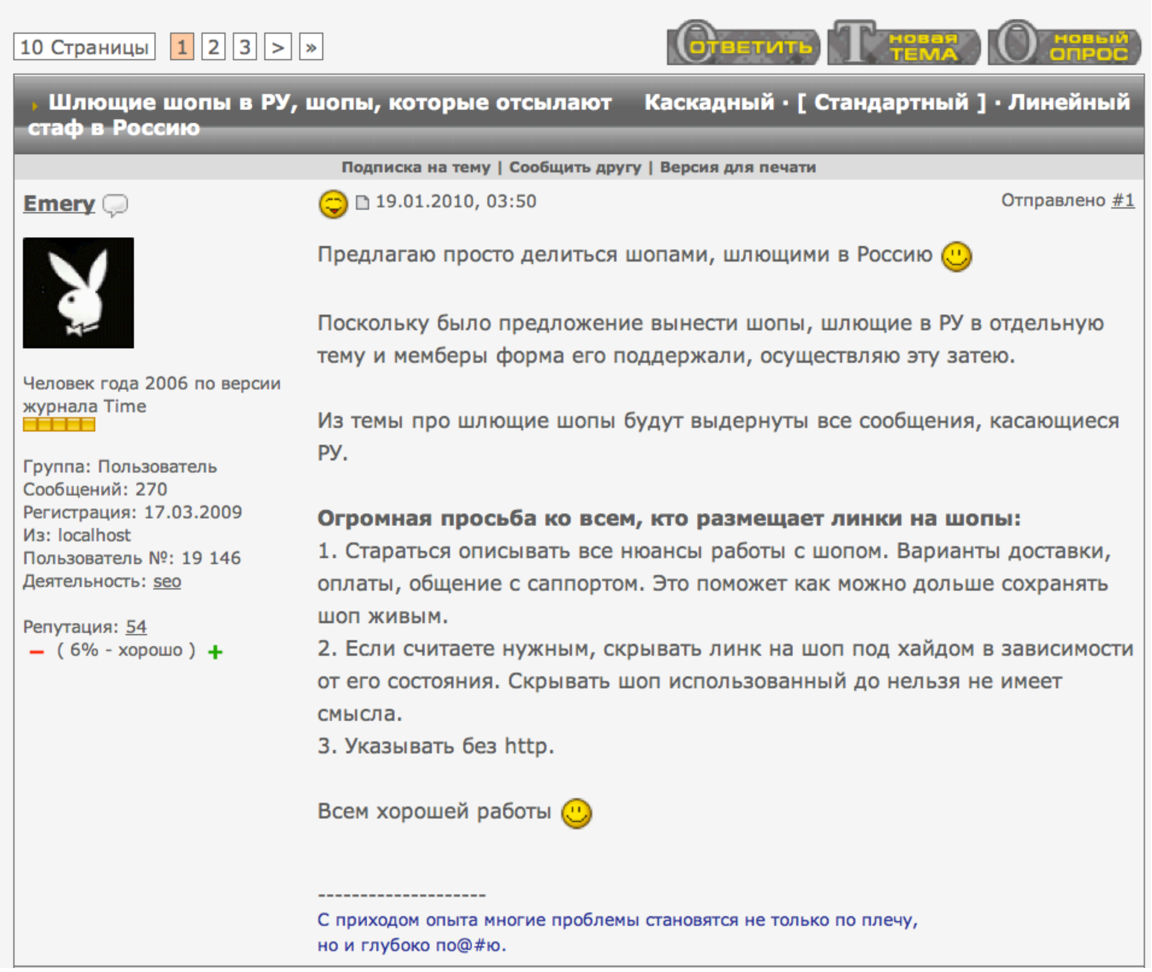
Some guidance is provided, what databases will be bought:

- Only freshly hacked databases.
- Sale should be only to one set of hands.
- Especially interested in USA and EU databases.

Hacking web servers was always profitable and / or it is a first step into environment. These days it is close to impossible to do business without IT and a web server is a necessity. Competition is fierce, quality developers are not cheap, and because of this web applications have insanely a lot of bugs and vulnerabilities.

4. Online shops that send goods to Russia

Not all web-based shops send goods overseas, especially to Russia and China. Some shops do that, and there is a possibility for hackers to use stolen credit cards numbers to acquire these goods.


10 Страницы
1
2
3
>
»
ОТВЕТИТЬ
НОВАЯ ТЕМА
НОВЫЙ ОПРОС
Каскадный · [Стандартный] · Линейный
Подписка на тему | Сообщить другу | Версия для печати

Шлющие шопы в РУ, шопы, которые отсылают стаф в Россию

Emery

Человек года 2006 по версии журнала Time

Группа: Пользователь
Сообщений: 270
Регистрация: 17.03.2009
Из: localhost
Пользователь №: 19 146
Деятельность: seo

Репутация: 54
− (6% - хорошо) +

19.01.2010, 03:50 Отправлено #1

Предлагаю просто делиться шопами, шлющими в Россию

Поскольку было предложение вынести шопы, шлющие в РУ в отдельную тему и мемберы форма его поддержали, осуществляю эту затею.

Из темы про шлющие шопы будут выдернуты все сообщения, касающиеся РУ.

Огромная просьба ко всем, кто размещает линки на шопы:
1. Стараться описывать все нюансы работы с шопом. Варианты доставки, оплаты, общение с саппортом. Это поможет как можно дольше сохранять шоп живым.
2. Если считаете нужным, скрывать линк на шоп под хайдом в зависимости от его состояния. Скрывать шоп использованный до нельзя не имеет смысла.
3. Указывать без http.

Всем хорошей работы

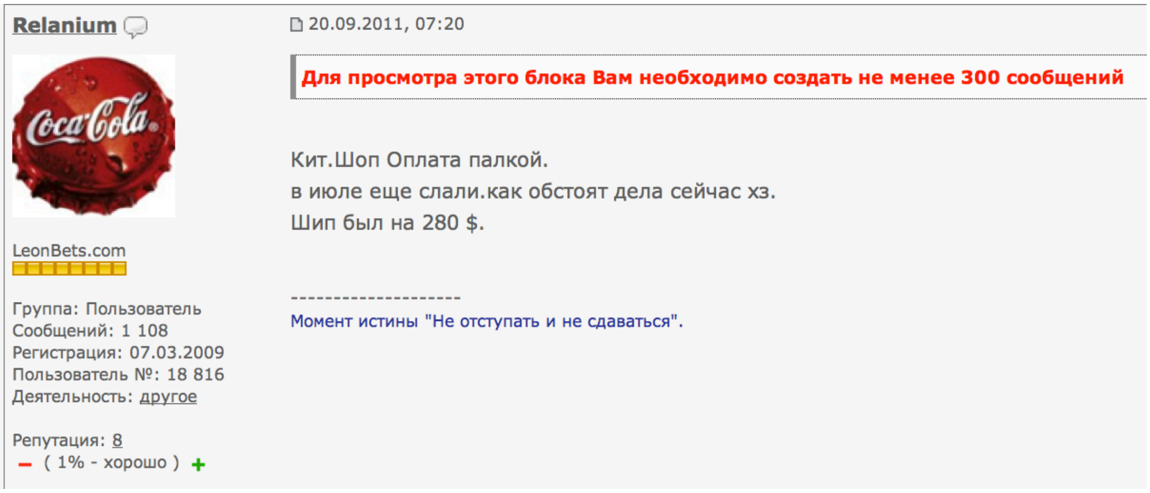
С приходом опыта многие проблемы становятся не только по плечу,
но и глубоко по@#ю.

Requirements and rules for this thread:

1. Please do your best to describe all nuances we need to know in order to place order successfully. This will help to exploit shop for as long as possible.

2. If you find it necessary, please post links to shop under hide (hide is a feature in many forums that hides information based on the number of posts you have in particular forum. So, if you don't have enough meaningful posts in this forum you can't see it)

   Example, text in red says, "you can't read it as you don't have 300 posts":



Relanium

LeonBets.com

Группа: Пользователь
Сообщений: 1 108
Регистрация: 07.03.2009
Пользователь №: 18 816
Деятельность: другое

Репутация: 8
− (1% - хорошо) +

20.09.2011, 07:20

Для просмотра этого блока Вам необходимо создать не менее 300 сообщений

Кит.Шоп Оплата палкой.
в июле еще слали.как обстоят дела сейчас хз.
Шип был на 280 $.

Момент истины "Не отступать и не сдаваться".

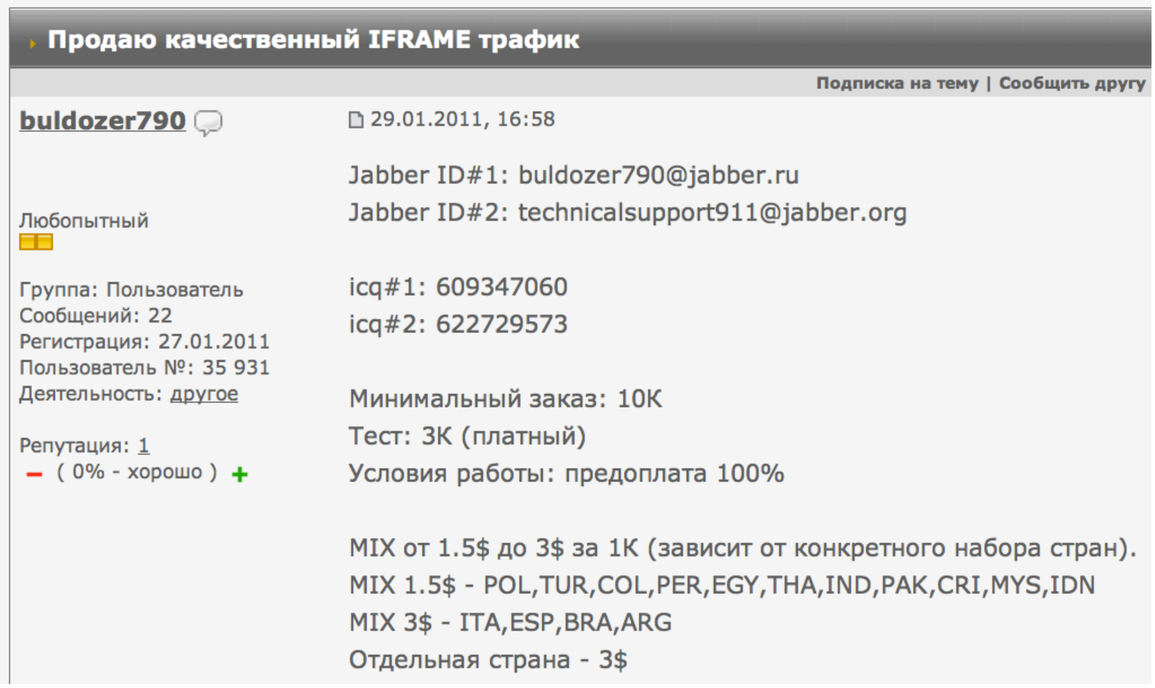
3. Don’t give a direct link to website, a typical method is to replace http with hxxp, example:

   Hxxp:exampleshop.com

   It takes quite some time to find shops willing to ship goods to Russia or China. Many online shops learned their lessons hard way; others are yet to learn it….

5. So your website is hacked? What’s next?

Typically extra code is inserted in your website in the form of iframe, this gentlemen below sells drive-by-attacks by thousands of “hits”. He has some compromised websites with his code on them and he is selling potential malware installations to you.



Продаю качественный IFRAME трафик

Подписка на тему | Сообщить другу

buldozer790

Любопытный

Группа: Пользователь
Сообщений: 22
Регистрация: 27.01.2011
Пользователь №: 35 931
Деятельность: другое

Репутация: 1
− (0% - хорошо) +

29.01.2011, 16:58

Jabber ID#1: buldozer790@jabber.ru
Jabber ID#2: technicalsupport911@jabber.org

icq#1: 609347060
icq#2: 622729573

Минимальный заказ: 10K
Тест: 3K (платный)
Условия работы: предоплата 100%

MIX от 1.5$ до 3$ за 1K (зависит от конкретного набора стран).
MIX 1.5$ - POL,TUR,COL,PER,EGY,THA,IND,PAK,CRI,MYS,IDN
MIX 3$ - ITA,ESP,BRA,ARG
Отдельная страна - 3$

Actual prices:

Hits from mixed countries will cost $1.5 to $3.0 per 1000 hits. He is able to select certain countries out of the stream and present your exploit code just to them. Sorting out any particular country will set you back $3 per 1000 hits. Prices are cheaper for countries such as Poland, Turkey, Egypt, and Thailand…. and more expensive for countries such as Italy, Spain, Brazil and Argentina.

Statistics shows about 90% of hacked web sites are compromised by known attacks. Regular arsenal is LFI, RFI, SQLi, XSS, brute force to login, session fixation, etc. Only about 10% of all successful attacks have some kind of 0day or other means.

Lets take a look at some key points and what is a typical scenario to make some hard $$$ out of it.

- Dedicated hosting vs. shared hosting. Shared hosting is used for small projects, for projects that don't have a lot of traffic. If the hacker can't compromise the target web site he will take a look what other websites are hosted on the same server and try to compromise "neighbor" website. If that is successful, a shell is dropped on the server and from the shell he will see all websites being hosted on the server.

- The goal is to compromise as high traffic website as possible. It is simply more money to have 1 million users coming to a compromised web site than 10 users on a daily basis. This way hackers can infect many more users by drive-by-attacks.

- Malicious code is placed on the website, typically via iframe. Why iframe? Because it is a one liner, can be invisible in the content of the website, and it takes code from another website and executes it in the context of user browser.

- Malicious code takes a look what kind of operating system you use.

- Malicious code takes a look what browser and particular version you use.

- Based on this information malicious code on the web site exploits your browser and tries to compromise your system.

How money is being made:

- Lets assume attacker have successfully exploited users web browser.

- First step is to install a dropper into your operating system. This is a modular approach, as dropper can install different malware every other month, or it can install different malware based on victim's geo location, etc.

- Most installations are completely transparent to victim, i.e. victim doesn't need to confirm anything, doesn't need to click OK. It just happens in the background.

- By malware installation victim becomes a part of the botnet.

- The guy who runs the botnet makes quite some money by sending spam from machines he controls, aka botnet.

- The bigger the botnet - the more money.

- Typical services provided by botnets:

* Distributed denial of service attacks (examples: VISA, PAYPAL, MASTERCARD, SONY, EBAY)

* SPAM (examples: SPAM you have in your inbox!)

* Using the compromised hosts as a launchpad for other attacks or scanning the rest of the Internet for vulnerabilities. (We have to remember there are roughly 4 billion or 4 000 000 000 IP addresses in the world, and it takes a lot of time to scan all of them. This task is much easier to do with botnet.

Conclusion

There are a lot of threats and a lot of different ways to compromise networks, servers, infrastructure. Defense plan will vary from company to company based on the nature of the business, however most IT security best practices apply to most companies:

- Develop and use employee awareness and training program.
- Have audit and penetration testing on your systems on regular basis.
- Keep software updated and patched.
- Assess your physical security.
- Stay ahead of hackers by doing research and threat intelligence.