Custom hacking services

ptsecurity.com

Contents

Many businesses actively and productively use corporate sites, online stores, and web services to accomplish tasks. Customers register on these websites by leaving their personal data, make purchases by entering credit card information, and use cloud services to store information or use the resources provided to send their sensitive information. It is obvious that not only competitors, but also cybercriminals, would like to have access to such precious data, so it is no surprise when clients' personal data is leaked from yet another big company into the hands of criminals. Often, these events are associated with a successful attack on a company's web applications, as a result of which attackers gain access to the user database or steal other information. For example, in September 2020, hackers broke into more than 2,800 Magento-based online stores where they injected a malicious script that to scrape customers' personal information and payment card data.

As a result of hacking, both users and companies themselves may be affected. The web application security analysis conducted by Positive Technologies shows that criminals can conduct attacks on clients in 92% of web applications; in 68% of cases, there is a danger of a data leak; and in 16% of cases, attackers can gain control over the application and the server OS.

In this article, we will talk about why criminals hack websites, and what consequences there may be for the owners and users of hacked resources.

About the research

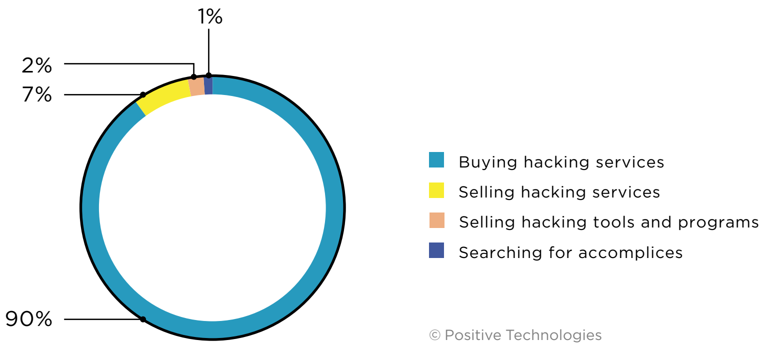
We have selected the ten most active forums on the dark web, which offer services for hacking websites, buying and selling databases, and accessing web resources. In total, more than 8 million users are registered on these forums, more than 7 million topics have been created, and more than 80 million messages have been published.

Note that this article does not consider ads that are posted in messages on such forums and related to services for organizing DDoS attacks on web resources, since in this case, the motives, goals, and tools of the attackers and those who hire them differ radically and go beyond the scope of this research.

Why criminals hack websites

In 90% of cases, users of darknet hacking forums search for a hacker who can provide them with access to a particular resource or who can download a user database. Seven percent of the messages include offers to hack websites. The rest of the messages are aimed at promoting hacking tools and programs and finding like-minded people to share hacking experience.

By offers, we mean ads published by service owners and hacker groups. They cannot act as indicators of supply and demand, as they are often posted only once. The demand for the services mentioned above can be estimated approximately only by individual inquiries from users who, for various reasons, did not make use of the information about the offers.

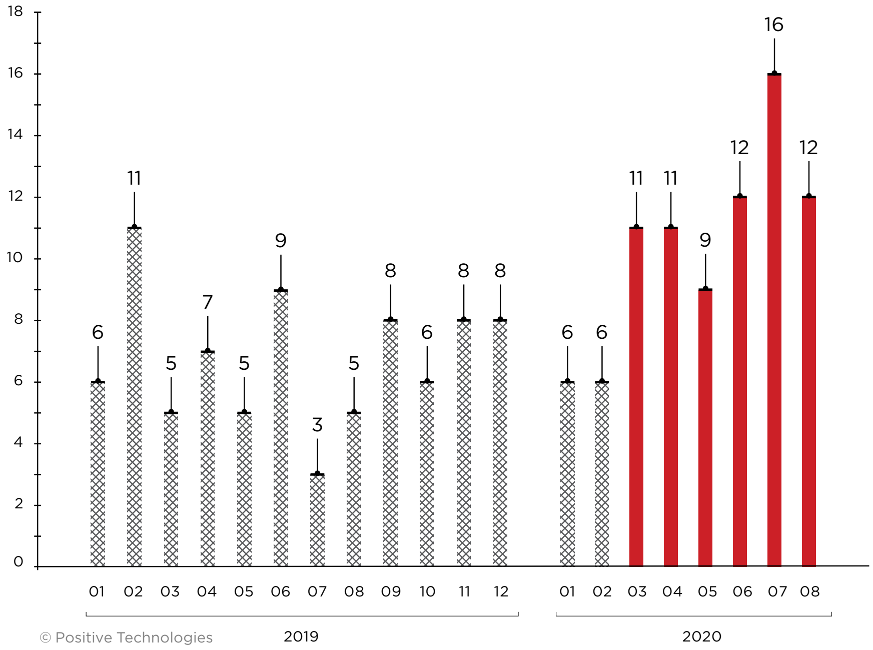


© Positive Technologies

Figure 1. Categories of inquiries related to hacking websites

Since March 2020, we have noticed a surge of interest in website hacking. This might have been caused by an increase in the number of companies available via the Internet, which was triggered by the COVID-19 pandemic. Organizations that previously worked offline were forced to go online in order to maintain their customers and profits, and cybercriminals, naturally, took advantage of this situation.

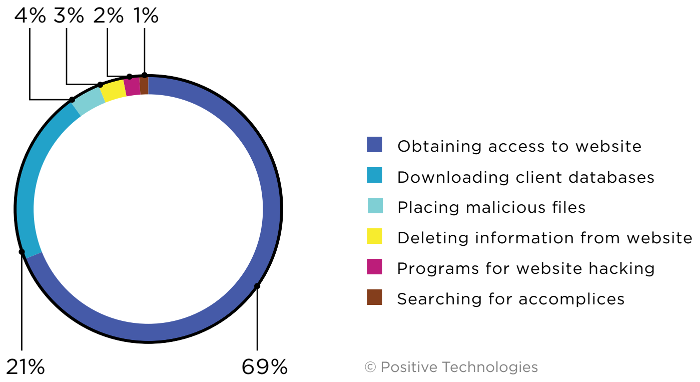
The following graph shows the number of new ads on dark web forums. Ads are posted not only by new members, but also by hackers with an established reputation. The latter do this as a form of self-promotion. It is difficult to determine which ads are duplicates and which have lost relevance, so we do not give the number of hackers or groups that actively provided hacking services at the beginning of 2019 or who are doing it today.



© Positive Technologies

Figure 2. Number of new ads related to hacking web resources on forums in 2019–2020

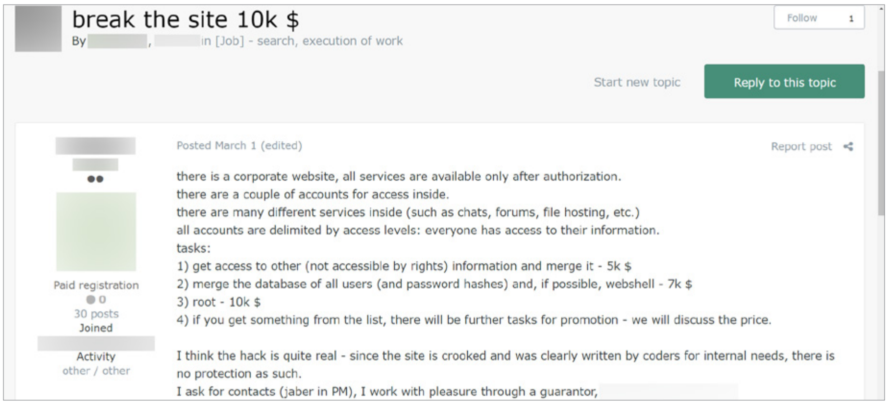
In about seven out of ten inquiries related to website hacking, the main goal is to gain access to a web resource. Not only can attackers steal sensitive information, but also sell access to web applications to so-called fences.



© Positive Technologies

Figure 3. Distribution of inquiries by topic

Inquiries aimed at obtaining user or client databases from a targeted resource account for 21% of all ads. Competitors and spammers who collect lists of addresses for targeted phishing attacks aimed at a specific audience are primarily interested in acquiring this type of information.



break the site 10k $

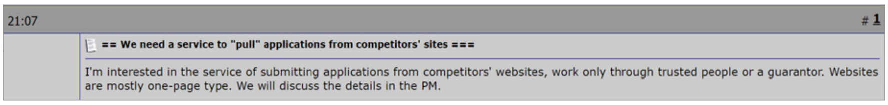
By [redacted], [redacted] in [Job] - search, execution of work

Posted March 1 (edited)

there is a corporate website, all services are available only after authorization.
there are a couple of accounts for access inside.
there are many different services inside (such as chats, forums, file hosting, etc.)
all accounts are delimited by access levels: everyone has access to their information.
tasks:
1) get access to other (not accessible by rights) information and merge it - 5k $
2) merge the database of all users (and password hashes) and, if possible, webshell - 7k $
3) root - 10k $
4) if you get something from the list, there will be further tasks for promotion - we will discuss the price.

I think the hack is quite real - since the site is crooked and was clearly written by coders for internal needs, there is no protection as such.
I ask for contacts (jaber in PM), I work with pleasure through a guarantor, [redacted]

Figure 4. Custom website hacking

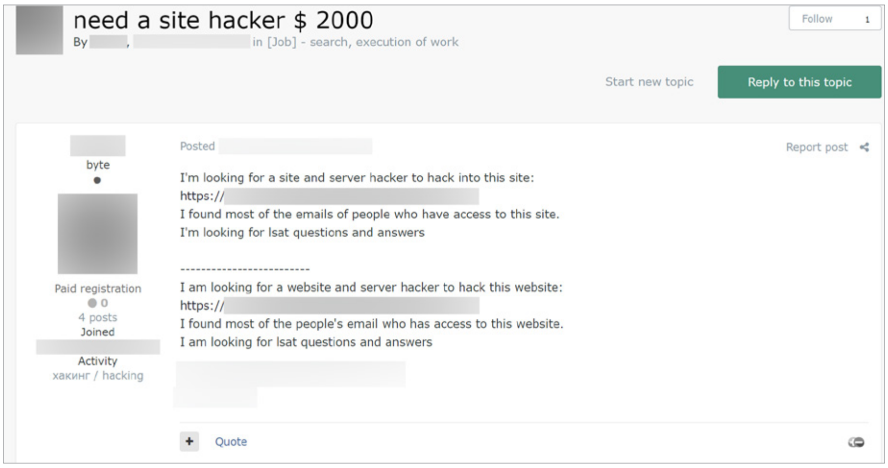


== We need a service to "pull" applications from competitors' sites ===

I'm interested in the service of submitting applications from competitors' websites, work only through trusted people or a guarantor. Websites are mostly one-page type. We will discuss the details in the PM.

Figure 5. Collecting information from competitors' websites

In 4% of inquiries, the main goal of attackers is not to hack the website, but to inject malicious programs into it, for example, for conducting watering hole attacks or placing web skimmers. In August 2020, during one of its campaigns aimed at scientists from the universities of Haifa and Tel Aviv, the APT group Charming Kitten hacked the Deutsche Welle website in order to place a malicious link on it. After clicking this link, the victim was asked to pass authorization, and the credentials they entered were sent to the attackers.



need a site hacker $ 2000

By [redacted], [redacted] in [Job] - search, execution of work

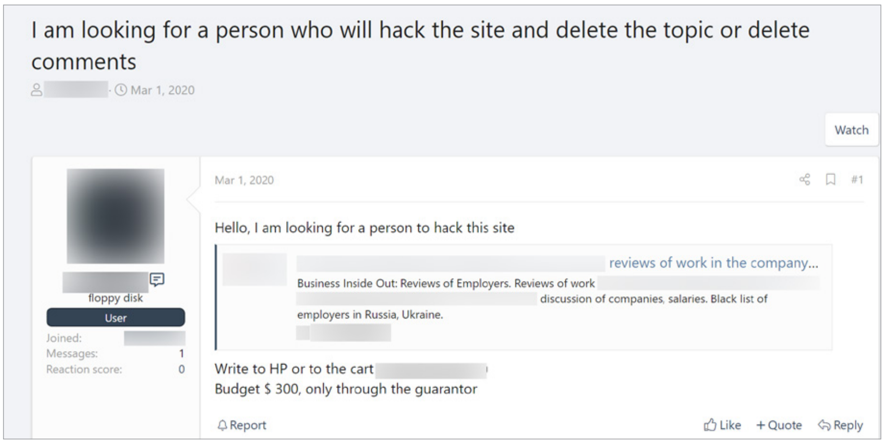
Posted [redacted]

I'm looking for a site and server hacker to hack into this site:
https://[redacted]
I found most of the emails of people who have access to this site.
I'm looking for lsat questions and answers

I am looking for a website and server hacker to hack this website:
https://[redacted]
I found most of the people's email who has access to this website.
I am looking for lsat questions and answers

Figure 6. Search for a website hacker

Three percent of ads are aimed at finding a person who can hack a website and delete certain data specified by the customer. This service may be in demand among those who want to remove negative reviews about a company posted on resources that are not controlled by that company, as one example.



I am looking for a person who will hack the site and delete the topic or delete comments

[redacted] · Mar 1, 2020

Mar 1, 2020

Hello, I am looking for a person to hack this site

[redacted] reviews of work in the company...
Business Inside Out: Reviews of Employers. Reviews of work [redacted] discussion of companies, salaries. Black list of employers in Russia, Ukraine.
[redacted]

Write to HP or to the cart [redacted]
Budget $ 300, only through the guarantor

Figure 7. Ad for a hacker

Offers for the sale of ready-made programs and hacking scripts were found in 2% of total analyzed inquiries.

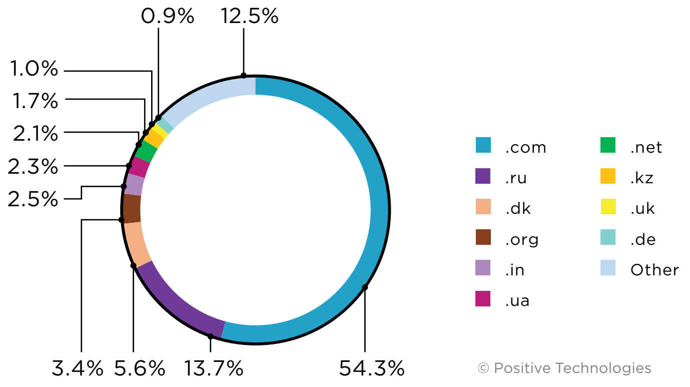
Some hack, and some buy

We already explained that fences buying access to websites have appeared on the dark web. Now that this phenomenon has taken root, it turns out instances of it can be broken into categories. In some cases, users buy web shells, some buy access to the administration interfaces of websites, and others buy ready-made exploits for injecting SQL code into specific resources.

What is a web shell

A web shell is a file uploaded to a server that an attacker can use to execute OS commands on that server through the web interface and gain access to other files.

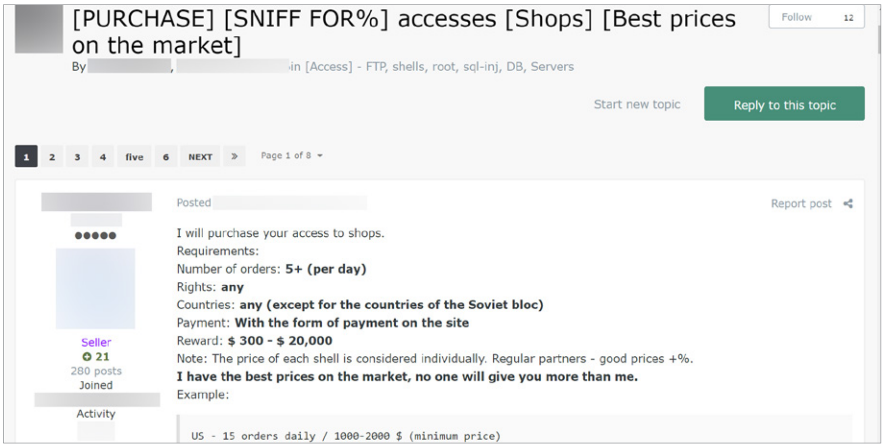
Web shells are inexpensive relative to, say, databases, which we will talk about later: their prices range from a few cents to 1,000 USD. This is mainly due to the fact that the privileges obtained by uploading the web shell to the file system are limited. Selling a web shell means sending the customer a link to the file path and, possibly, credentials for authorization. The most common web shells are on websites in the .com domain zone—they account for 54.3% of the offers for sale.



© Positive Technologies

Figure 8. Distribution of top-level domains where websites with web shells are registered

Fences, first of all, have to keep track of what is appealing to the consumer market. It is difficult to deduce the industry specifics of types of sold or bought access, but we can safely say that access to online stores is in its own category. The demand for it is consistently high: this is due to the fact that when paying for goods, users enter their credit card details. Thus, attackers can inject malicious JavaScript code into the website to intercept the information entered by the user and use it for their personal gain. Another way to cash in on users is to obtain privileged access to an online store, then place orders using other people's payment cards, or not pay at all. Prices for access to online stores range between $50 and $2,000.



[PURCHASE] [SNIFF FOR%] accesses [Shops] [Best prices on the market]

By [redacted], [redacted] in [Access] - FTP, shells, root, sql-inj, DB, Servers

Posted [redacted]

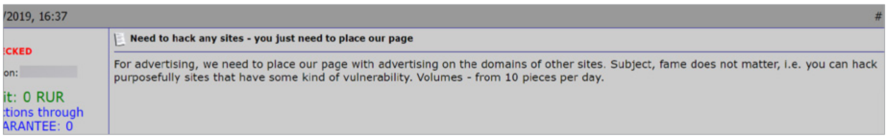
I will purchase your access to shops.
Requirements:
Number of orders: **5+ (per day)**
Rights: **any**
Countries: **any (except for the countries of the Soviet bloc)**
Payment: **With the form of payment on the site**
Reward: **$ 300 - $ 20,000**
Note: The price of each shell is considered individually. Regular partners - good prices +%.
I have the best prices on the market, no one will give you more than me.
Example:

```
US - 15 orders daily / 1000-2000 $ (minimum price)
```

Figure 9. Ad for purchasing access to online stores

If the web service is hosted on a server connected to the company's internal network, the main risk for the organization is that an attacker (or someone who buys access to the server through a web shell) can develop an attack and penetrate the company's infrastructure. The results of external pentests conducted by Positive Technologies experts in 2019 show that at 86% of companies there is at least one vector for penetration into the local network, which is associated with insufficient protection of web applications. At one out of every six tested companies, we found traces of prior attacks. For instance, we found web shells on the network perimeter, malicious links on official sites, or valid credentials in public data dumps.

Attackers use access to the administration web interfaces of popular CMSs in order to place web shells and malware on them and use them for illegal advertising. For example, in August and September 2020, a series of attacks were observed targeting the websites of WHO, UNESCO, government agencies, the National Institute of Health, and major educational institutions. On these resources, hackers posted phishing ads for tools used to hack accounts in well-known social networks and for cheating in online games. They had two goals: stealing payment card data and spreading malware. Some users were redirected to a payment page where they were asked to enter their card information, while others immediately downloaded malware to their devices.



/2019, 16:37

Need to hack any sites - you just need to place our page

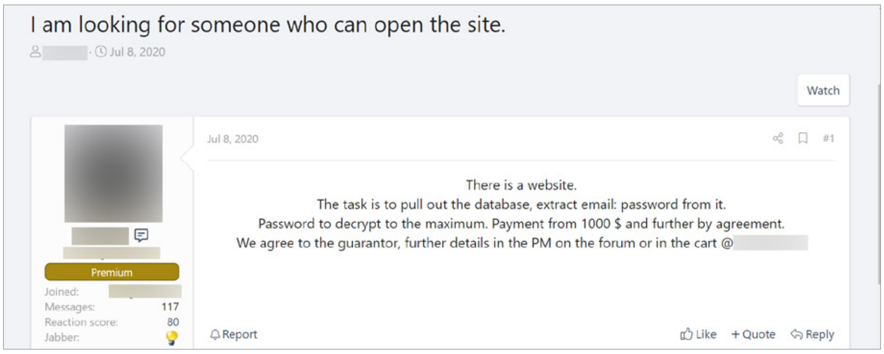
For advertising, we need to place our page with advertising on the domains of other sites. Subject, fame does not matter, i.e. you can hack purposefully sites that have some kind of vulnerability. Volumes - from 10 pieces per day.

Figure 10. Search for a hacker to place ads

It is worth noting that a website's involvement in illegal advertising campaigns may negatively affect its position in the search results of popular search engines.

User databases

Dumps, or databases from hacked websites, can be bought by competitors or criminals who plan targeted phishing attacks.



I am looking for someone who can open the site.

[redacted] · Jul 8, 2020

[redacted]

[redacted]

Premium

Joined: [redacted]

Messages: 117

Reaction score: 80

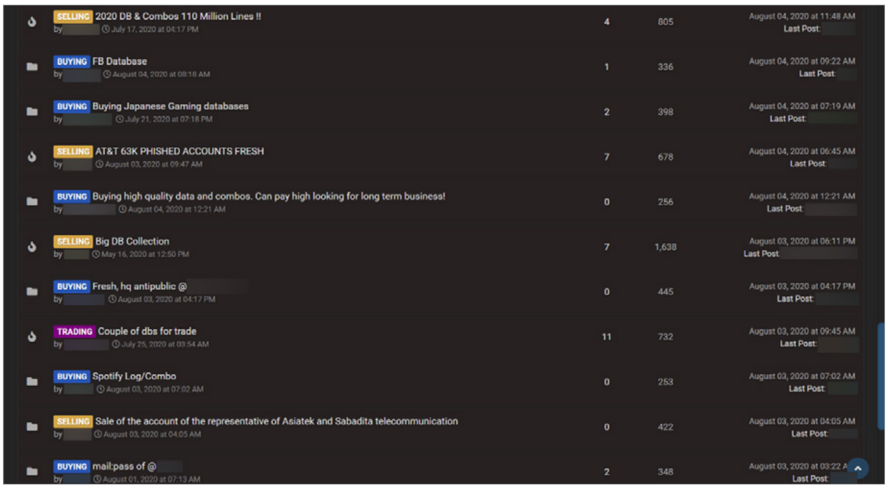
Jabber:

Jul 8, 2020 #1

There is a website.
The task is to pull out the database, extract email: password from it.
Password to decrypt to the maximum. Payment from 1000 $ and further by agreement.
We agree to the guarantor, further details in the PM on the forum or in the cart @[redacted]

Figure 11. Ad for a website hacker

Custom databases cost between $100 and $20,000 or between $5 and $50 per 1,000 entries.



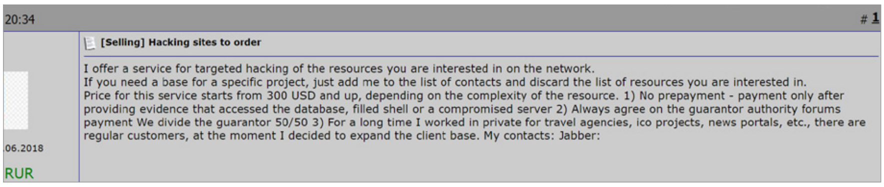
SELLING 2020 DB & Combos 110 Million Lines !! by [redacted] July 17, 2020 at 04:17 PM	4	805	August 04, 2020 at 11:48 AM Last Post: [redacted]
BUYING FB Database by [redacted] August 04, 2020 at 08:18 AM	1	336	August 04, 2020 at 09:22 AM Last Post: [redacted]
BUYING Buying Japanese Gaming databases by [redacted] July 21, 2020 at 07:18 PM	2	398	August 04, 2020 at 07:19 AM Last Post: [redacted]
SELLING AT&T 63K PHISHED ACCOUNTS FRESH by [redacted] August 03, 2020 at 09:47 AM	7	678	August 04, 2020 at 06:45 AM Last Post: [redacted]
BUYING Buying high quality data and combos. Can pay high looking for long term business! by [redacted] August 04, 2020 at 12:21 AM	0	256	August 04, 2020 at 12:21 AM Last Post: [redacted]
SELLING Big DB Collection by [redacted] May 16, 2020 at 12:50 PM	7	1,638	August 03, 2020 at 06:11 PM Last Post: [redacted]
BUYING Fresh, hq antipublic @[redacted] by [redacted] August 03, 2020 at 04:17 PM	0	445	August 03, 2020 at 04:17 PM Last Post: [redacted]
TRADING Couple of dbs for trade by [redacted] July 25, 2020 at 03:54 AM	11	732	August 03, 2020 at 09:45 AM Last Post: [redacted]
BUYING Spotify Log/Combo by [redacted] August 03, 2020 at 07:02 AM	0	253	August 03, 2020 at 07:02 AM Last Post: [redacted]
SELLING Sale of the account of the representative of Asiatek and Sabadita telecommunication by [redacted] August 03, 2020 at 04:05 AM	0	422	August 03, 2020 at 04:05 AM Last Post: [redacted]
BUYING mail:pass of @[redacted] by [redacted] August 01, 2020 at 07:13 AM	2	348	August 03, 2020 at 03:22 A Last Post: [redacted]

Figure 12. Ads for the sale of accounts obtained through phishing

User entries may, for example, contain the following information: username, email address, full name, phone number, address of residence, social security number, and date of birth. This information can be used to conduct social engineering attacks.

Is it difficult to hack a website?

Our web application security analysis revealed that, on average, each web application has 4 high-severity and 12 medium-severity vulnerabilities. Even if we do not take into account the large number of vulnerabilities, criminals can use social engineering techniques to conduct attacks, such as targeted phishing campaigns, on a resource administrator in order to obtain their credentials (username and password). These data allow attackers to access the company's website.



20:34

1

06.2018

RUR

[Selling] Hacking sites to order

I offer a service for targeted hacking of the resources you are interested in on the network.
If you need a base for a specific project, just add me to the list of contacts and discard the list of resources you are interested in.
Price for this service starts from 300 USD and up, depending on the complexity of the resource. 1) No prepayment - payment only after providing evidence that accessed the database, filled shell or a compromised server 2) Always agree on the guarantor authority forums payment We divide the guarantor 50/50 3) For a long time I worked in private for travel agencies, ico projects, news portals, etc., there are regular customers, at the moment I decided to expand the client base. My contacts: Jabber:

Figure 13. Ad for custom website hacking

Based on our research data, we can conclude that most web resources are not sufficiently protected from intruders. The number of ads on the dark web offering services for hacking web resources should also be taken into account. If required, criminals can easily hire an experienced hacker or buy a ready-made hacking tool from a fence or another source.

Conclusions

Web application hacking services are in high demand. Ads for custom website hacking are not characteristic of any single specific industry; however, most customers purchasing such services are interested in online stores. This is primarily due to the fact that users of these resources enter their personal data and credit card information there. We believe that there is a definite trend towards a further increase in demand, as more and more companies go online as a result of the COVID-19 pandemic.

Hacking a company's web applications can lead to global consequences: from data leaks and sanctions for violation of legislation (for example, GDPR) to penetrating the company's local network and using its resources in subsequent attacks—as a platform for spreading malware or for storing tools that will be downloaded during the attack. When building a security system, we recommend following the principles of a risk-oriented approach, based on an understanding of the magnitude of negative consequences that are acceptable for your company. It will be easier and cheaper to proactively protect the most vulnerable part of your company's network than to pay huge fines and have your company's reputation smeared.

To protect your company, you should adhere to the principles of secure development and use automated source code analysis tools to search for errors and vulnerabilities, since the 2019 web application security analysis revealed that 82% of all vulnerabilities are found in web application code. It is essential to regularly analyze your web application security and to use a web application firewall for proactive protection against attacks.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 18 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.