POSITIVE TECHNOLOGIES

The criminal cyberservices market

2018

Contents

Introduction

The news today is full of stories about financial damage caused by hacker attacks against organizations, or about hundreds of thousands of user accounts being leaked from some website. Yet there's never any information about how much it costs to prepare and launch such attacks. But since the point of any work, including cybercrime, is to make a profit, hackers will simply switch to other, more lucrative pursuits if the costs of an attack are comparable or exceed the potential revenue.

In our recent study of current cyberthreats, we noted an increase in the number of major cyberincidents: Q1 2018 saw 32 percent more detections than in Q1 2017.[1] What's more, most malware attacks involved the use of programs for data theft and hidden cryptocurrency mining. Meanwhile, information keeps appearing online about the code for various Trojans being made open-source. The availability of ready-made malware is, in our view, the reason behind the significant rise in the number of attacks. The aim of this study is to investigate the cost of such software and the complexity of acquiring it, as well as analyze the market supply and demand.

We analyzed in detail the market for cybercriminal services and tried to assess whether cybercriminals need a wide range of specialized knowledge, or whether everything can be outsourced to the shadow market: hackers of websites and servers, malware developers and distributors, botnet owners, and other practitioners. During the analysis, we repeatedly encountered situations where the login credentials for systems and web shells for remote management of large companies' servers were up for sale. We immediately passed on the relevant information to the compromised organizations, warning about the need to take protective measures and carry out an investigation.

For the objects of our study, we selected the 25 most popular shadow trading platforms, whose names we do not disclose, with a total number of registered users in excess of three million. We analyzed more than 10,000 ads in total, without taking into account obvious scams, which inundate the gray market like any other.

We calculated the minimum and average cost of various tools and services sold on such sites, and estimated the supply–demand ratio and the adequacy of the services provided for conducting a full-scale cyberattack.

1 ptsecurity.com/ww-en/analytics/293716/

Executive summary

Instead of in-house products and services, most modern cyberattacks deploy ones purchased and leased from third parties. This not only lowers the cybercrime entry threshold and simplifies carrying out attacks, but also makes it difficult or impossible to accurately attribute targeted attacks.

The diagram below presents some common types of attacks, as well as their minimum cost in US dollars, assuming that the attack masterminds purchase all necessary means and tools with money. For example, the cost of a targeted attack against an organization, depending on its complexity, can start from $4,500, including hiring an expert hacker, leasing infrastructure, and purchasing the relevant tools. Hacking a site and gaining full control over a web application costs only $150, yet we found ads for the targeted hacking of sites with prices climbing to $1,000.

The study showed that cryptominers, hacking utilities, botnet malware, RATs, and ransomware Trojans are widely available in the shadow cyberservices market, while the highest demand is typically for malware development and distribution. The market offers more than 50 different categories of goods and services, which together can be used to organize any attack.

Hacking accounts of US government officials[2] **5** years prison term	Hacking email from **$40**	Hacking website from **$150**	Conducting DDoS attack[3] **1** year prison term
Targeted attack from **$4,500**			DDoS attack from **$50** a day
Infecting with ransomware Trojan (1,000 nodes) from **$750**			Stealing from ATM from **$1,500**
Managing shadow service for anonymous scan of malware using various antiviruses[4] **35** years prison term	Infecting with Trojan for mining (1,000 nodes) from **$300**	Stealing payment data from **$270**	Developing and distributing RAT[5] **10** years prison term

2 goo.gl/v8SwKZ
3 goo.gl/Pw5mST
4 goo.gl/c4j8tj
5 goo.gl/gyhvDi

1. Cybercrime as a business

According to FireCompas, only 4 percent of Internet pages are indexed by search engines.[6] Private forums and databases (medical, research, financial), and other resources invisible to search engines are collectively known as the deep web, or the deep Internet. Besides resources with confidential and other legal data, the deep web contains specialized platforms and forums of an unlawful nature, collectively known as the dark web. And since such resources often trade in illegal products and services, altogether they also called the shadow market. Our study focused on hacker forums.

Below is a schematic representation of the position occupied by the shadow market in the planning and implementation of cyberattacks.

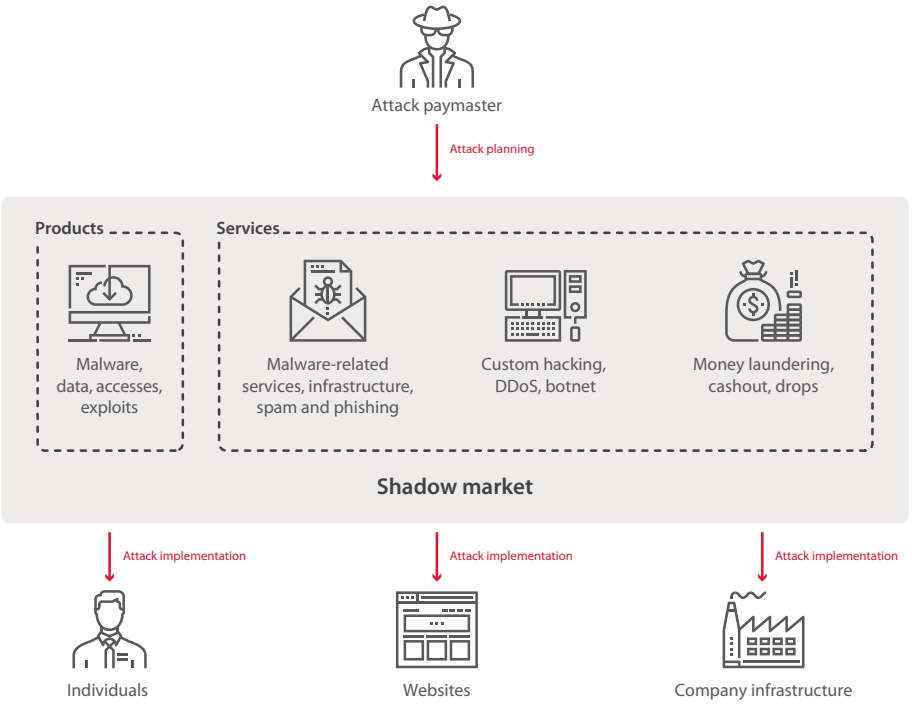


Figure 1. The shadow market and its place in the cybercriminal world

2. Sale of products

The vast majority of shadow market products fall into the following categories:

- Malware (ransomware, miners, etc.)
- Exploits (for both known and zero-day vulnerabilities)
- Data (personal, accounting, payment, etc.)
- Access (web shells, passwords for sites or servers)

The products in each category will be considered further in more detail. The demand and supply for a given product in the shadow market, and the price that it sells for, will be revealed.

6 firecompass.com/blog/darkweb-deepweb-darknet-browsers/

2.1. Malware

Today, malware is a key element in almost every cyberattack, since it handles tasks related to automation, speed of execution, and attack invisibility. Depending on its purpose, malware is divided into several types:

- Cryptominers
- Data-stealing Trojans (stealers)
- Hacking tools
- Malware for DDoS
- Ransomware
- RATs
- Trojan loaders, droppers
- Botnet malware
- ATM malware

The diagram below shows the prevalence of dark web ads for particular malware. It should be noted that during the research we encountered seller ads either for ready-made Trojans or malware developers, but no buyer ads for a specific ready-made Trojan. This suggests that the demand is almost completely covered by the wide range of malware offers, and when a specific solution is required, cybercriminals implement it independently or hire programmers. We explore the topic of hiring programmers separately (see Section 3.1.1).

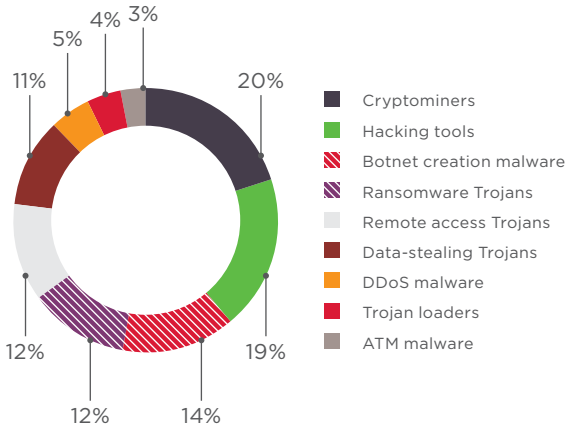


Figure 2. Shares of seller ads for various types of malware

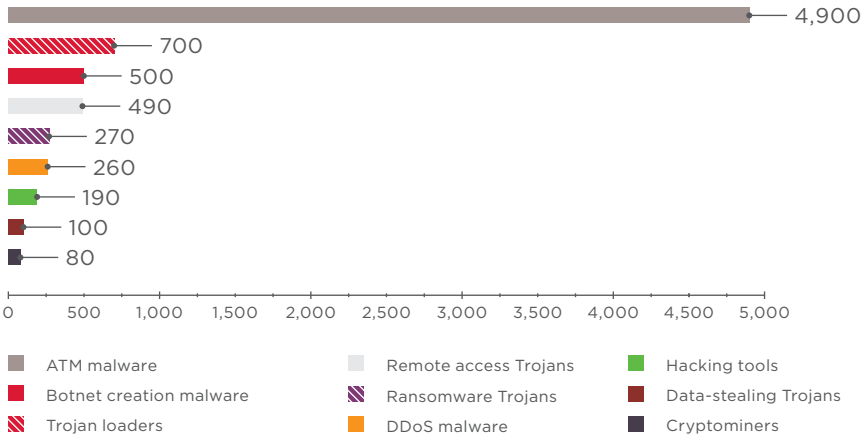


Figure 3. Average cost of malware, $

In 2017, the rapid rise in the value of cryptocurrencies caused an explosion in the use of hidden mining software. It accounts for 19 percent of malware currently up for sale. In Q1 2018, the share of cyberattacks using this type of malware stood at 23 percent.[7] The growing interest in cryptocurrencies also led to the wider dissemination of data-stealing malware (stealers, spyware) aimed primarily at taking funds from cryptocurrency accounts. With 11 percent of the total volume of malware offers, stealers are in first place by number of cyberincidents logged in Q1 2018 (30% of all such incidents).

Nineteen percent of offers up for sale were hacking tools, in which category we include software designed for website attacks, mass mailings, address and password generators, and packers and encryptors of executable files.

The average prices for tools from each category are given in the diagram above. The most expensive malware was for ATMs. This is not surprising, since cybercriminals can use it to gain substantial profit.

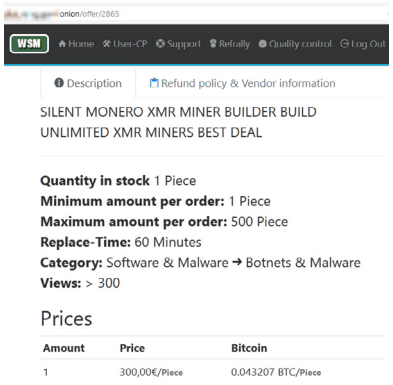


Figure 4. Sale of a Trojan for mining Monero cryptocurrency

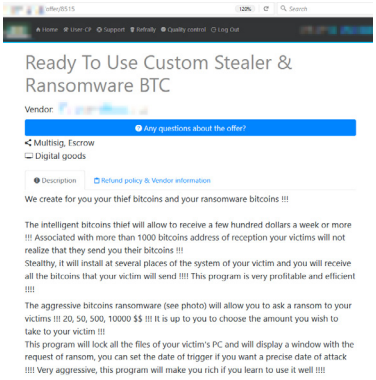


Figure 5. Sale of a Trojan for stealing cryptocurrency from a user wallet

2.1.1. Data-stealing Trojans

Stealers do the following:

- Steal passwords from the clipboard.
- Intercept keystrokes and save the title of the window in which the keys were pressed.
- Bypass or disable antivirus software.
- Send files to the attacker's email.

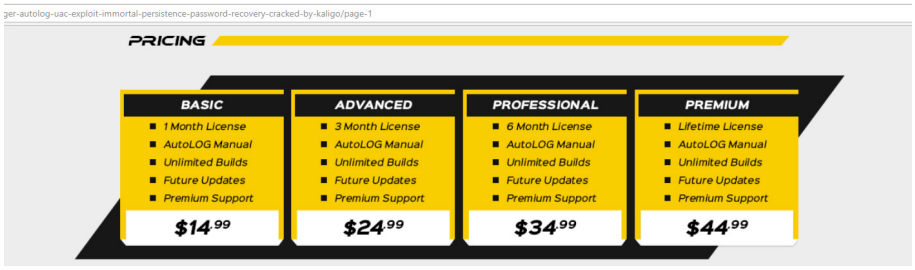


Figure 6. Sale of the Autolog keylogger

With a stealer costing around $10, stolen data can fetch anything from a few dollars to several hundred dollars for credentials for email accounts, social networks, and other resources containing personal information. And if the malware enables the theft of user data for payment systems or passwords for cryptocurrency wallets, the potential revenue is thousands of times greater than the cost of the attack.

7 ptsecurity.com/ww-en/analytics/293716/

2.1.2. RATs and botnet malware

When hackers are not simply after a certain set of data, but looking to establish a long-term latent presence in the system and execute commands remotely, they use what is known as a remote access Trojan (RAT). Typically, malware of this type allows the cybercriminal to:

- Track user actions.
- Run files and execute commands.
- Capture screenshots.
- Turn on the webcam and microphone.
- Scan the local network.
- Download files from the Internet.

RATs sell for an average of $490 on the shadow market, and are mainly used for targeted attacks and infecting individual nodes. The most well-known RATs are DarkComet, CyberGate, ProRAT, Turkojan, Back Orifice, Cerberus Rat, and Spy-Net. The most popular of these, DarkComet, was distributed for free until in 2012 it was discovered that the Syrian government was using it to spy on oppositionists, and China to keep an eye on pro-Tibetan non-governmental organizations.[8] Access to the DarkComet project was closed as a result, but it serves as the basis for numerous builds used by attackers today.

There exists an entire family of RATs developed on the basis of modified legal programs for remote management of computers, such as TeamViewer, Remote Manipulator System, and VNC. A monthly subscription to such malware costs around $1,000. Having lawful "roots" allows such malware to avoid detection by antivirus software, but unlike "donors" it operates in hidden mode. Such software is often found in the arsenal of hackers targeting banks. For instance, the MoneyTaker group used UltraVNC to attack Russian and US banks.[9] Meanwhile, the sophisticated banking Trojans Dridex, Neverquest, and Gozi use hVNC-based modules to control infected user workstations.[10]

If the cybercriminals expect to seize control of multiple devices, then besides malware with RAT functionality, they will need special software designed to coordinate the control of the infected devices, such as a command-and-control (C&C) center. A network of infected devices under single control is called a botnet.

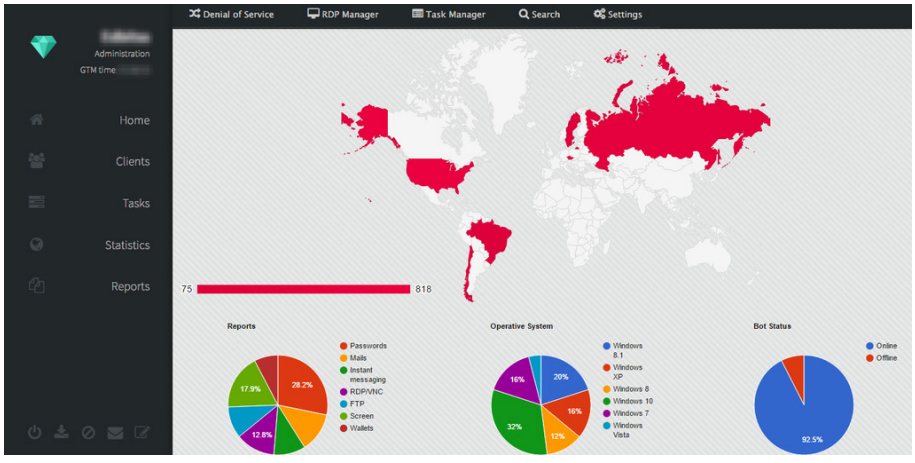


Figure 7. Interface of a botnet C&C center with statistics about infected nodes

8 blog.trendmicro.com/trendlabs-security-intelligence/darkcomet-surfaced-in-the-targeted-attacks-in-syrian-conflict/
9 group-ib.com/resources/threat-research/money-taker.html
10 securityintelligence.com/anatomy-of-an-hvnc-attack/

On the shadow market, prices for malware to create a botnet start at $200. A complete package that includes C&C server software, software for creating Trojans configured to work with a particular server (builder), and additional Trojan modules can cost $1,000–1,500. Such a botnet pays for itself in less than a month, if used solely to conduct DDoS attacks, for instance.

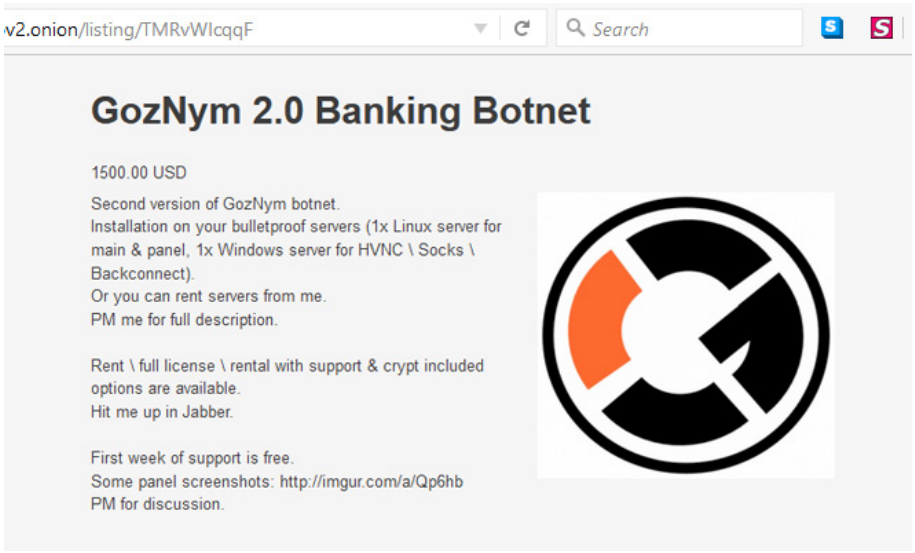


Figure 8. Sale of a banking botnet

2.1.3. ATM Trojans

Another kind of malware that criminals see as a short cut to riches are Trojans for ATMs. Our 2017 study "Attacks against ATMs using GreenDispenser: Organization and techniques"[11] examined logical attacks against ATMs in detail, and in early 2018 this topic again proved relevant during a string of ATM attacks in the US.[12]

Malware for ATMs is the most expensive class of ready-made malware, with prices starting from $1,500. Developing such programs requires not only good programming skills, but knowledge of the internal workings of ATMs made by various manufacturers. Sure, malware's market value also depends on the potential profit to be gained from using it: one ATM contains around 8,000 banknotes of different denominations, amounting to approximately 8 million rubles ($200,000 or £120,000). A single piece of malware can be used to attack many identical ATMs all at once, so if the criminal group coordinates its actions properly, it can expect a big payout.

In 2017, according to the European Association for Secure Transactions (EAST), there were 192 attacks against ATMs involving the use of malware, causing official damage estimated at €1.52 million.[13] In comparison with 2016, the number of incidents rose by 231 percent, and the total damage by 230 percent.

2.1.4. Ransomware Trojans

This type of malware is perhaps the most well-known today due to a series of attacks involving Trojan encryptors in 2017.

11 ptsecurity.com/upload/corporate/ww-en/analytics/ATM-Security-eng.pdf
12 krebsonsecurity.com/2018/01/first-jackpotting-attacks-hit-u-s-atms/
13 association-secure-transactions.eu/atm-malware-attacks-hit-europe/

According to an IBM study, up to 70 percent of US companies polled have paid a ransom to recover data.[14] Although this statistic is difficult to calculate for Russian companies, our experience of investigating incidents shows that some victims also prefer to pay up.

As such, it is obvious that the costs involved are recouped several times over after one successful mass attack.

The biggest ransomware attacks in 2017 were the WannaCry, NotPeyta, BadRabbit, Locky, and Cerber epidemics, while the total damage caused by ransomware attacks exceeds $1.5 billion.

The average cost of acquiring such malware is $270.

The ransom, payable only in cryptocurrency, is set by the distributors of the ransomware and is generally in the order of $200–500.

For example, the ransom to recover WannaCry- and NotPetya-encrypted data was set at $300.

Today, the most advanced method of malware propagation, particularly for encryptors, is the as-a-service sales model.

The buyer pays only for a set number of launches, operating period, or number of files created.

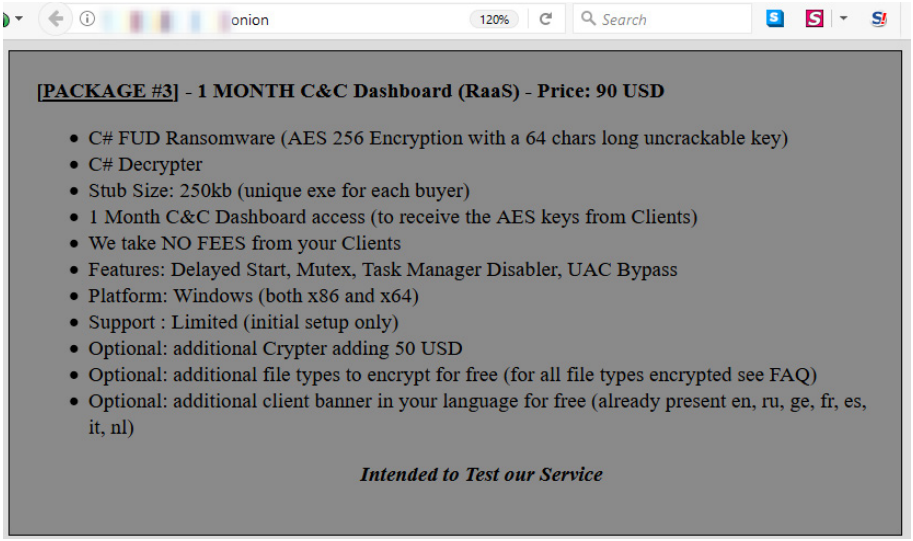


Figure 9. Ad for the lease of a ransomware Trojan

To increase their revenue, the developers of encryptors have recently begun distributing them through so-called partner programs.

The seller sends a personalized encryptor file and a link to a personal account with statistics about infected sites and payments made.

The buyer's task is to spread the Trojan.

When a victim pays a ransom using this instance of the Trojan, the seller transfers the payment to the distributor (minus its fee).

Usually the seller keeps 15–50 percent, meaning that the distributor gets 50–85 percent.

This is the propagation scheme for Gandcrab, Tantalus, Aleta, Princess, Rapid, Scarab, Sphinx, Lovecraft, Onyonlock, and other encryptors.

14 www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03135USEN

Having been widely disseminated over the past year, Gandcrab in April–May 2018 alone raked in $700,000 for its cybercriminal handlers, with more than 315,000 nodes infected.

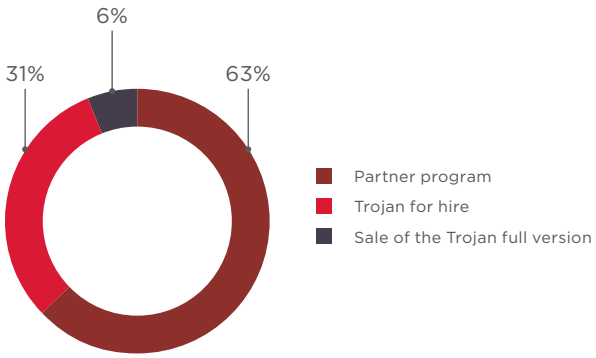


Figure 10. Offers for the sale of encryptors

As can be seen from the diagram, at the time of this research, partner programs enjoyed overwhelming popularity in this segment of the malware market.

This is entirely understandable, since attackers do not have to worry about the technical aspects of the malware and its infrastructure, or about having the requisite programming and hacking skills.

For as little as $90 per month to access the service, they receive a ready-to-distribute Trojan configured for their wallet, which pays for itself after the first ransom payment.

2.2. Exploits

$2,540
average cost of an exploit for web and Windows applications

An exploit is a program or program code that uses software vulnerabilities to attack a computer system.

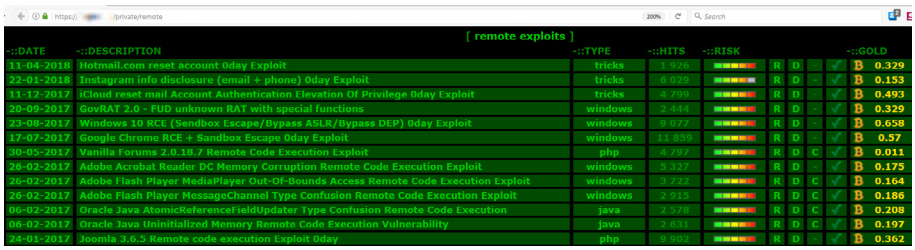
Information about software vulnerabilities and exploits for them fetch a high price on the shadow market.

On one site, for instance, the average price for exploits put up for sale in 2017–2018 was $2,540.

Thirty-eight percent of these exploits were intended for vulnerabilities in the Windows family of operating systems or software running under Windows.

Nearly a fifth of them (19%) were designed for cross-platform technologies, such as Java and Adobe Flash, which can be employed in attacks against users of not only Windows, but also Linux, Android, and macOS.

The macOS family of operating systems accounted for 5 percent of all exploits for vulnerabilities on offer, and the cost ranged from $2,200 to $5,300.


[remote exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD
11-04-2018	Hotmail.com reset account 0day Exploit	tricks	3 926		R	D	-	✓	B 0.329
22-01-2018	Instagram info disclosure (email + phone) 0day Exploit	tricks	6 029		R	D	-	✓	B 0.153
11-12-2017	iCloud reset mail Account Authentication Elevation Of Privilege 0day Exploit	tricks	4 799		R	D	-	✓	B 0.493
20-09-2017	GovRAT 2.0 - FUD unknown RAT with special functions	windows	2 444		R	D	-	✓	B 0.329
23-08-2017	Windows 10 RCE (Sendbox Escape/Bypass ASLR/Bypass DEP) 0day Exploit	windows	9 077		R	D	-	✓	B 0.658
17-07-2017	Google Chrome RCE + Sandbox Escape 0day Exploit	windows	11 859		R	D	-	✓	B 0.57
30-05-2017	Vanilla Forums 2.0.18.7 Remote Code Execution Exploit	php	4 797		R	D	C	✓	B 0.011
26-02-2017	Adobe Acrobat Reader DC Memory Corruption Remote Code Execution Exploit	windows	5 327		R	D	-	✓	B 0.175
26-02-2017	Adobe Flash Player MediaPlayer Out-Of-Bounds Access Remote Code Execution Exploit	windows	3 722		R	D	C	✓	B 0.164
26-02-2017	Adobe Flash Player MessageChannel Type Confusion Remote Code Execution Exploit	windows	2 915		R	D	C	✓	B 0.186
06-02-2017	Oracle Java AtomicReferenceFieldUpdater Type Confusion Remote Code Execution	java	2 578		R	D	C	✓	B 0.208
06-02-2017	Oracle Java Uninitialized Memory Remote Code Execution Vulnerability	java	2 631		R	D	C	✓	B 0.197
24-01-2017	Joomla 3.6.5 Remote code execution Exploit 0day	php	9 902		R	D	-	✓	B 0.362

Figure 11. Exploit trading site

38%
exploits on sale for Windows and applications running under this OS

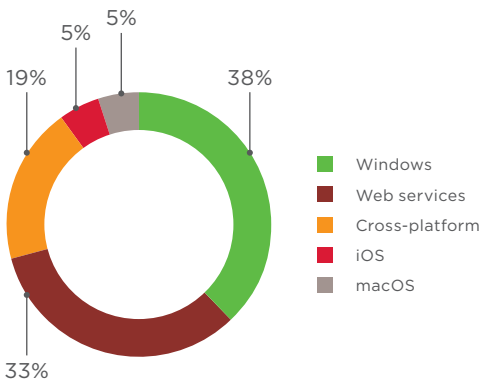


Figure 12. Exploit categories

Figure 13. Sale of files with exploits

The most valuable exploits in the shadow market are for zero-day vulnerabilities (that is, vulnerabilities for which the vendor has not yet released a patch).

But it's extremely common for users not to install patches even when released, so cybercriminals can often use exploits for known vulnerabilities.

According to our data, the minimum interval between the details of a vulnerability being published and the first attempts to exploit it in 2017 was just three hours.[15] Last year's most striking ransomware attack was WannaCry, which resulted in more than 500,000 infected devices,[16] despite the fact that a patch was made available on the Microsoft website two months before the attack.

2.3. Data

Data ends up on the shadow market in a variety of ways: for example, from cybercriminals who extract personal information and users' credentials for various services, or from criminal groups that get hold of client databases during targeted attacks on companies.

15 ptsecurity.com/upload/corporate/ww-en/analytics/Web-application-attacks-2018-eng.pdf
16 ptsecurity.com/upload/corporate/ww-en/analytics/Corporate-vulnerabilities-2018-eng.pdf

Data bought and sold on the shadow market can be divided into the following categories:

- Logins and passwords for various Internet services (social networks, online banks)
- credit card information
- Personal data of individuals, including scanned copies of identity documents (passports, driving permits)
- Financial statements of companies, scanned copies of incorporating documents, and other confidential documentation

The most common ads on the dark web are for the sale of user credentials for various services.

This is not surprising given the frequency of media reports about passwords and other information for various online services being leaked from databases.

Most of these leaks are not publicized.

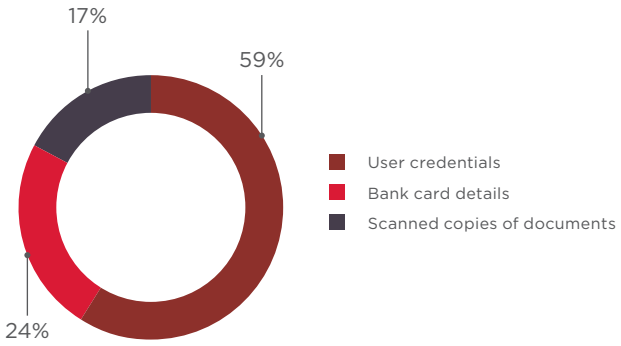


Figure 14. Types of data sold

2.3.1. User credentials

User logins and passwords for payment systems, online banks, and cryptocurrency exchanges are of most interest and value to intruders.

Passwords for popular online stores such as Ebay and Amazon are also in demand, since users' personal accounts often have bank cards linked to them, enabling criminals to make purchases with other people's funds or use these trading platforms to cash out money from stolen bank cards by buying goods in someone else's name for subsequent resale.

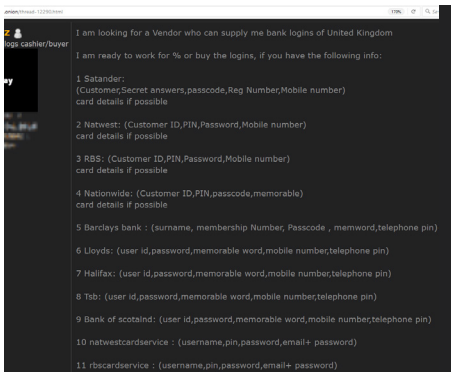


Figure 15. Buyer ad for online bank credentials

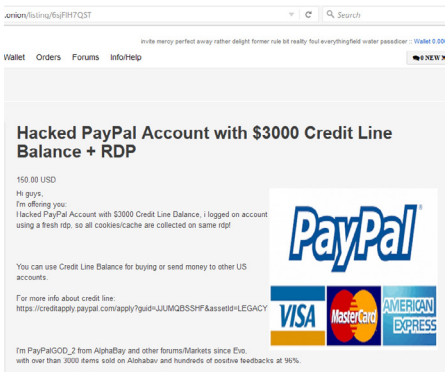


Figure 16. PayPal user credentials

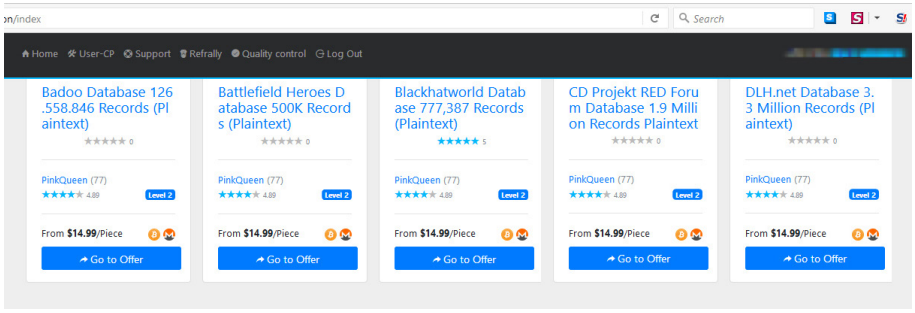


Figure 17. Sale of user credentials for various services

Most credentials sell for up to $10.

Note that stolen accounts for social networks and other online services are sold in batches numbering several thousand to several million.

Prices for such sets range from tens to hundreds of dollars.

Credentials for access to online banking personal accounts are sold per piece; at an average price of $22, accounts have balances ranging from a few tens of dollars to tens of thousands.

$22
average cost of data of online banking users

$5,840
average amount in a hacked payment system user account

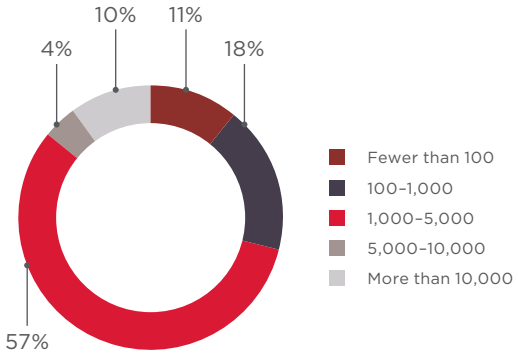


Figure 18. Amount of funds in hacked accounts, $

2.3.2. Credit card information

Another category of data that is sold on the shadow market is credit card information. They are used to receive money in the following ways:

- Buying and selling goods on the Internet
- Cashing out funds through payment systems
- Making duplicate bank cards to be used for withdrawing cash from ATMs

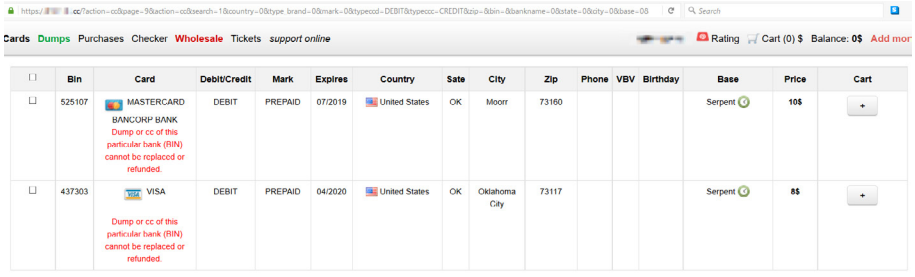


Figure 19. Credit card information

$9
cost of details for one bank card

In the first two cases, the attacker may need a confirmation code sent by the issuing bank to the owner in a text message.

This problem can be overcome by purchasing details of calls and text messages for the relevant mobile phone number on the shadow market.

A text message containing a one-time payment code can be obtained for $250.

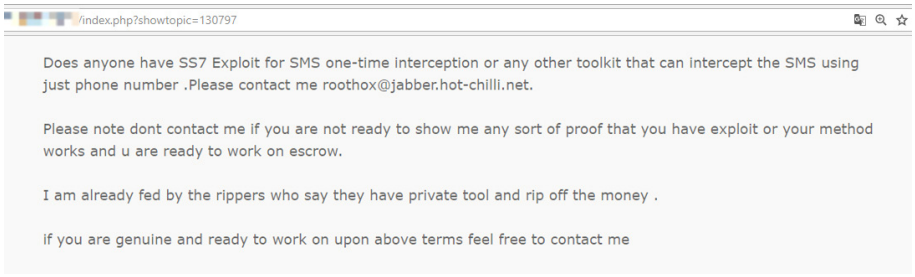


Figure 20. Buyer ad for services to intercept text messages through the SS7 network

Details for one bank card linked to an account containing between several hundred and several thousand dollars sell on average for $9.

2.3.3. Scanned copies of personal and confidential documents

Another category of data that can be bought or sold on the shadow market is scanned copies of various documents, including:

- Identity documents containing personal data: passports, driving licenses, ITINs
- Financial documents, including credit history reports
- Scanned copies of internal documents of commercial companies

$2
average cost of a scanned copy of a passport

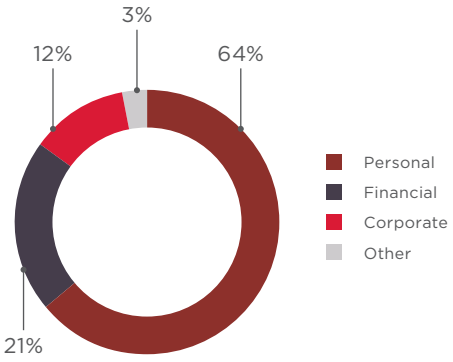


Figure 21. Types of confidential documents up for sale

Personal data is used by attackers to register with various online services.

For example, PayPal verification requires completing two out of three steps: linking and confirming bank account, verifying credit or debit card information and/or providing social security number. In this case, an SSN and credit card details will suffice, all available on the shadow market.

This wallet will not be linked to the attacker's identify, allowing them to make transactions with other shadow market players in someone else's name.

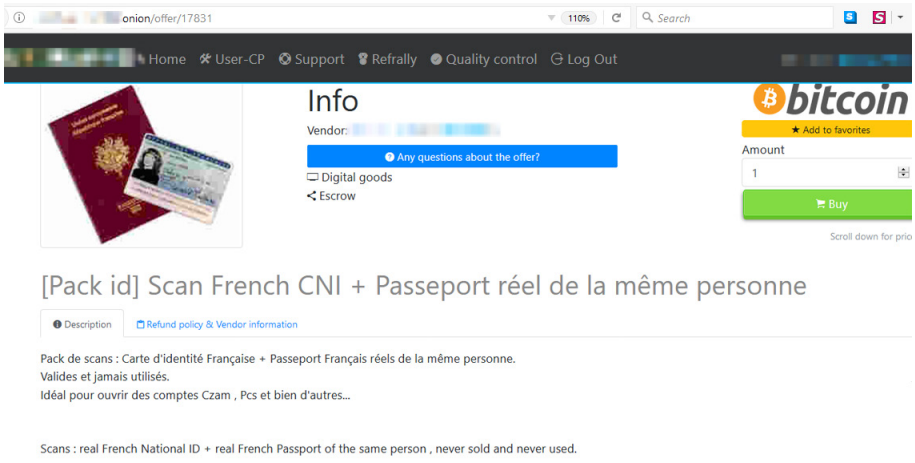


Figure 22. Sale of scanned copies of passports

2.4. Accesses

On the dark web, "accesses" are information that can be used to gain unauthorized access to a site or server with a view to downloading files or executing commands. Accesses can be used for various purposes.

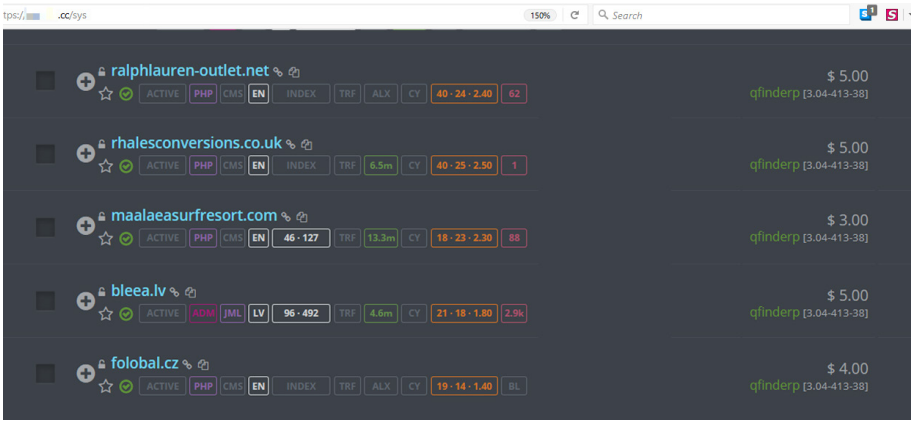


Figure 23. Marketplace selling accesses for hacked sites

For example, after gaining control over a news site, hackers can distribute malware from its pages and infect visitors.

Cybercriminals can use an access to an online store to steal clients' credit card information.

Government sites often experience DoS attacks or defacing (changing the contents of the home page).

Accesses for servers and workstations are most often used to distribute Trojan encryptors and as entry points to corporate information systems in targeted attacks.

The results of external penetration testing by Positive Technologies show that although in 2017 the network perimeter security of corporate information systems remained at the level of 2016, the complexity of attacks declined significantly.

Whereas in 2016 the attack complexity was rated as trivial in 27 percent of cases, in 2017 the figure was 56 percent.[17]

17 ptsecurity.com/upload/corporate/ww-en/analytics/Corporate-vulnerabilities-2018-eng.pdf

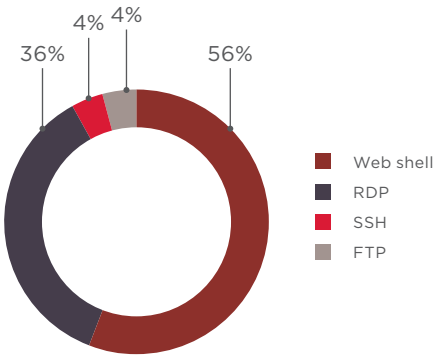


Figure 24. Types of accesses requested

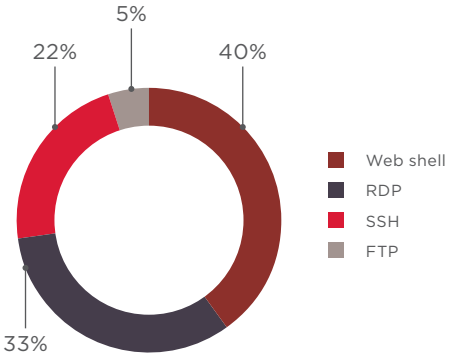


Figure 25. Types of accesses offered

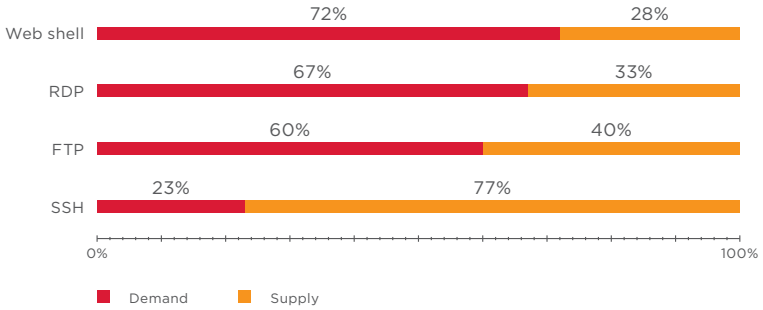


Figure 26. Supply–demand ratio in trading accesses

The most popular type of access is for a hacked site in the form of a web shell or content management system (CMS) administrator credentials.

A web shell is a malicious script uploaded through a vulnerability in a web application giving the attacker access to the server operating system via a page in the browser, often providing database access as well.

In most cases, the privileges of the cybercriminal in possession of such a web shell do not exceed the privileges of the web application itself, and therefore only the site can be attacked.

To gain full control over the server, intruders have to increase their privileges themselves through exploiting software vulnerabilities.

Since many sites are developed using the same technologies, the detection of a critical vulnerability in just one CMS, for example, can facilitate an attack on multiple sites simultaneously.

In this case, an access to one site allowing files to be uploaded to the server can sell for $0.15.

If the hacked resource is connected with finance, cryptocurrencies, an ICO, or is an online store, the price for such access can range from a few hundred to several thousand dollars.

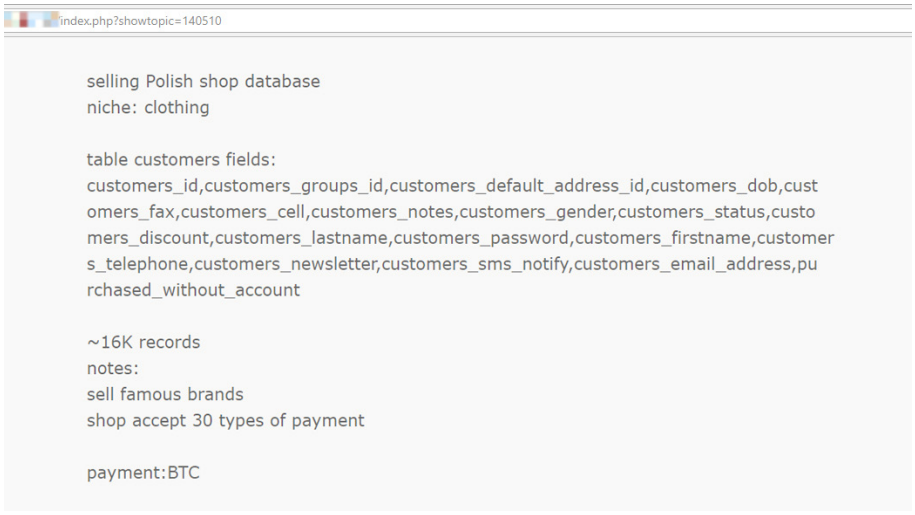


Figure 27. Sale of an online store database

An access to a server is usually the server address and user credentials for login using the RDP or SSH protocols. The small demand for SSH accesses is because this protocol is most often used to connect to servers running under Linux, while attackers tend to favor Windows-based machines. Prices for access credentials for one site can range from a few dollars to several hundred. For instance, an RDP access for an ATM can cost $500.

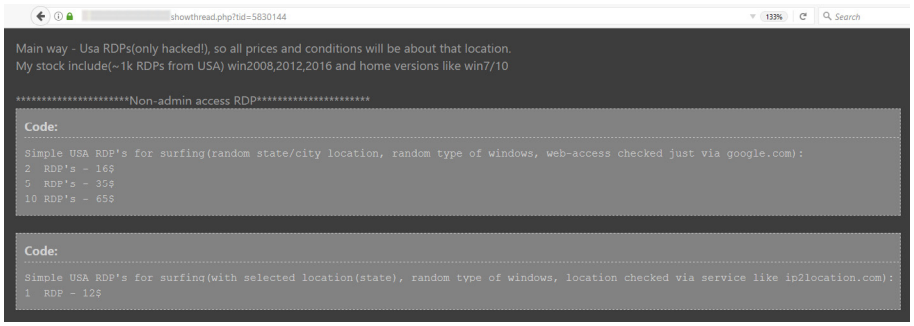


Figure 28. Sale of RDP access credentials for remote sites

3. Services

To prepare attacks, cybercriminals often engage third parties.

What's more, the hired hands may not be aware of the true purpose of the assignment: they are given a specialized task and the promise of a financial reward for completing it.

Besides the services of such freelancers, attackers are interested in the provision of infrastructure and resources for conducting attacks (dedicated servers, VPNs, botnets, etc.).

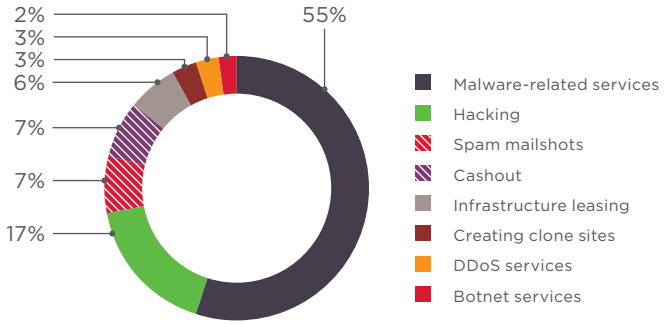


Figure 29. Demand for services

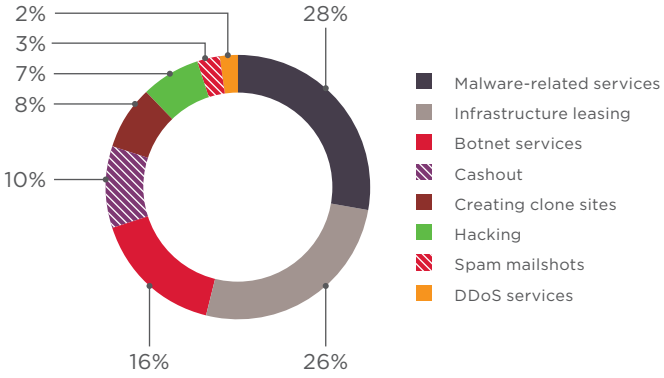


Figure 30. Supply of services

The most in-demand services on the dark web are for creating and distributing malware (55%), as well as for hacking email accounts, websites, and remote servers (17%).

More often than not, offers are also linked to malware (28%).

At the same time, a significant number of offers are for hosting and VPN services (26%), services for driving up views, likes, posts using botnet resources (16%), and cashout services (10%).

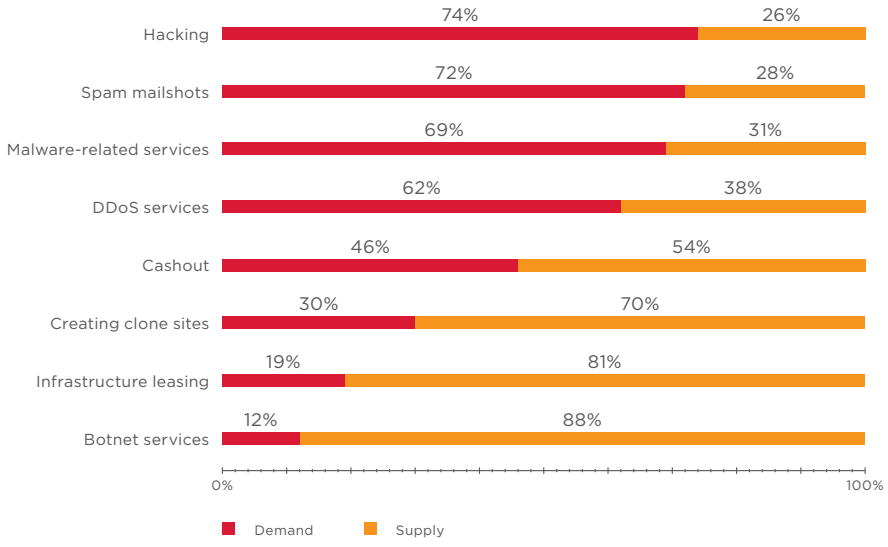


Figure 31. Supply–demand ratio for shadow market services

3.1. Malware-related services

When there are no ready-made solutions on the malware market, and a specific Trojan needs to be developed, the cybercriminal can either do it independently or place an ad for a programmer.

As can be seen from the diagram below, the demand for malware development is three times higher than current supply, which means that cybercriminals modify their attack methods on a daily basis, searching for new ways to bypass security measures and make their schemes more profitable.

Moreover, programmers who once specialized in bespoke malware are starting to sell ready-made solutions, because it is a more lucrative business.

Malware obfuscation—the process of transforming executable code for the purpose of hindering analysis while retaining its functionality—is usually included in the cost of development, and so is rarely ordered separately, but this service still appears among the offers.

Similarly, the dark web provides services for distributing newly created malware.

Demand for malware distribution significantly exceeds supply.

If the criminals do not have their own botnet, and do not want to do mailshots, they must find the corresponding services on the market.

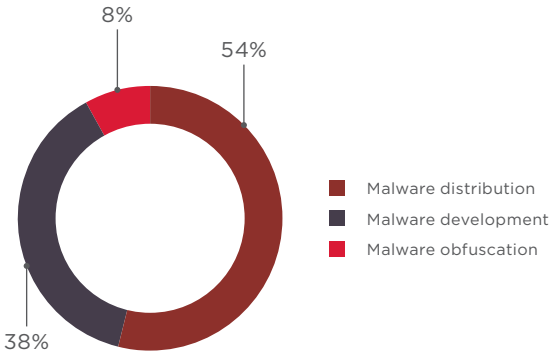


Figure 32. Demand for malware-related services

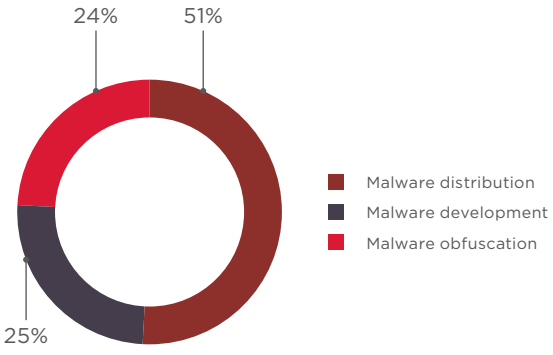


Figure 33. Supply of malware-related services

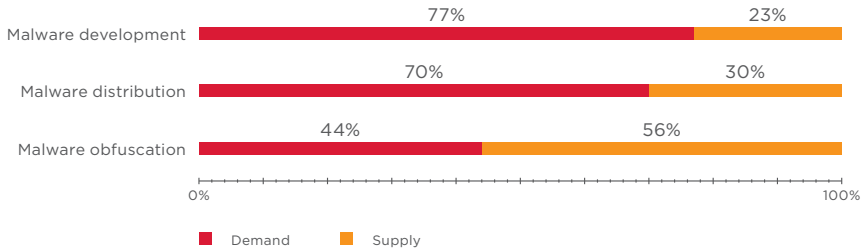


Figure 34. Supply–demand ratio for malware-related services

3.1.1. Malware development

Malware development services on dark web sites start on average from $500.

It often happens that not only development, but reverse engineering is required (for example, to create a new malware program on the basis of existing ones whose code is not available from public or private sources).

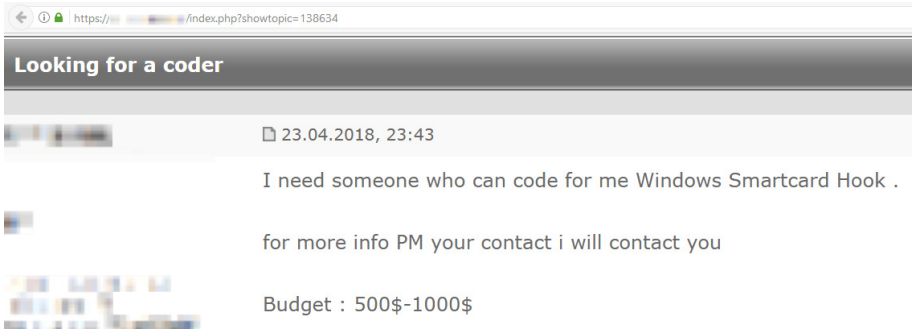


Figure 35. Searching for a private malware developer

On specialized sites, reverse engineering jobs start at $1,000 per project.

3.1.2. Malware obfuscation

Various service categories have emerged around malware development on the dark web, such as zipping, obfuscation, encryption of executable files, and file scanning by all possible antivirus solutions.

The task of such services and solutions is to ensure that the resulting executable file is not detectable by the most common antiviruses, and ideally remains under the radar of all of them for as long as possible.

The first file wiping, obfuscation, or encryption is usually included in the cost of the malware.

Additional wiping costs 5–10 percent of the base cost of the malware.

If the developer does not do obfuscation, the buyer can always use third-party services, which cost an average of $20.

There are services that charge several cents to check a file using several dozen antiviruses.

For those who need to check more files on a regular basis, a monthly subscription of $25 is available.

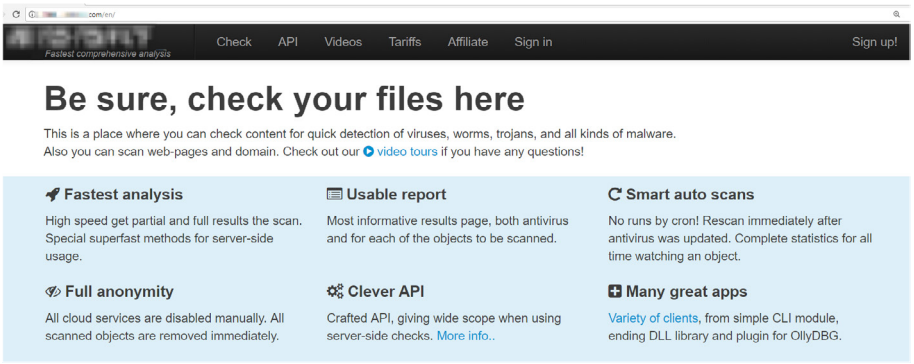


Figure 36. Anonymous scan of a file using several dozen antiviruses

3.1.3. Malware distribution

To carry out a cyberattack, simply having the malware itself is not enough; it has to be delivered to victim computers.

Cybercriminals can distribute malware:

- As phishing email attachments
- Through a file download link in phishing emails, SMS, instant messengers, or social networks
- As malicious files supposedly containing updates or utilities that are posted on hacked or attacker-controlled websites
- Through a botnet

To attract users to an infected resource, attackers use traffic selling services.

The service, which costs about $15 on average, involves redirecting users to the attackers' website from a hacked site with high "footfall" or via the contextual advertising system of popular search engines.

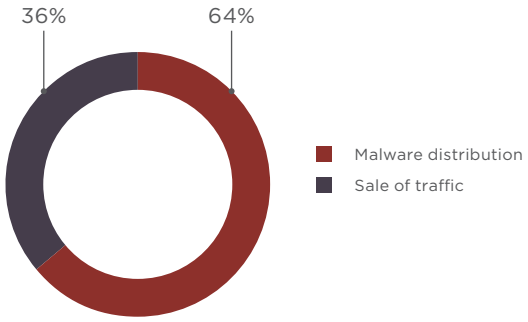


Figure 37. Demand for distribution services

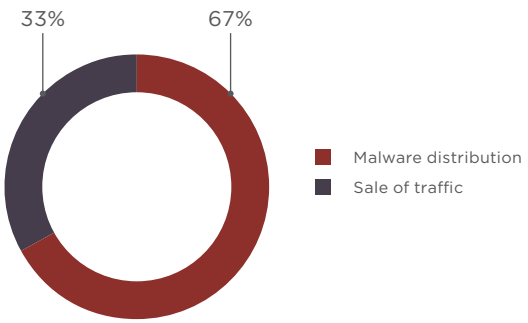


Figure 38. Supply of distribution services

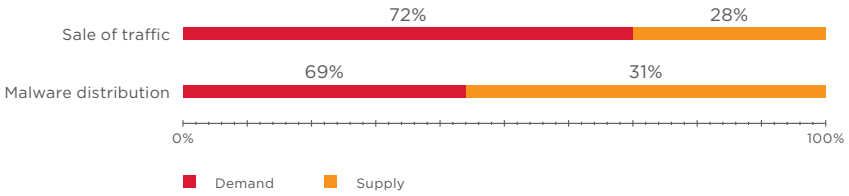


Figure 39. Supply–demand ratio for malware distribution services

Botnet owners offer services to load third-party files onto controlled devices and then run them.

For $50, for example, the buyer can load a file onto 1,000 random nodes, while around $400 lets them choose the geographic location of these nodes.

Such services are used by groups that attack companies in a certain industry.

For example, if banks are the target, the attackers ask the botnet owner for a list of IP addresses and select nodes relating to financial organizations and their partners.

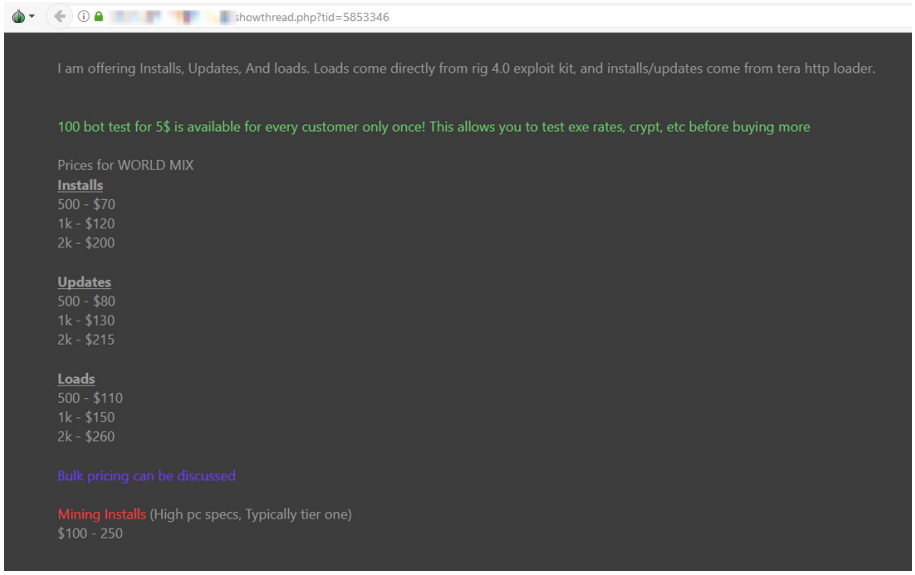


Figure 40. Botnet services for loading and installing malware on bots

A successful phishing attack often requires a website either to distribute malware or to steal user credentials and payment data.

The creation of a simple copy of a site costs $50–150 on the dark web, while an advanced version with authentication forms that verify input data and redirect the user after the attack to the original site (so as not to arouse suspicion) costs over $200.

Meanwhile, our study of employee cybersecurity awareness showed that 27 percent of successful attacks involve sending a phishing email with a link to a web resource requesting user credentials.[18]

The most relevant example of this attack method came in 2017, when ICOs were targeted through cloning official project sites together with mass phishing mailshots.

Users visited such resources and transferred cryptocurrency to the wallets specified by the criminals.

So instead of putting money in the project, potential investors put it in the pockets of thieves.

18 ptsecurity.com/upload/corporate/ww-en/analytics/Social-engineering-2018-eng.pdf

This was the case with the BeeToken ICO project in early 2018, in which cybercriminals managed to steal more than $1,000,000 worth of Etherium.[19]

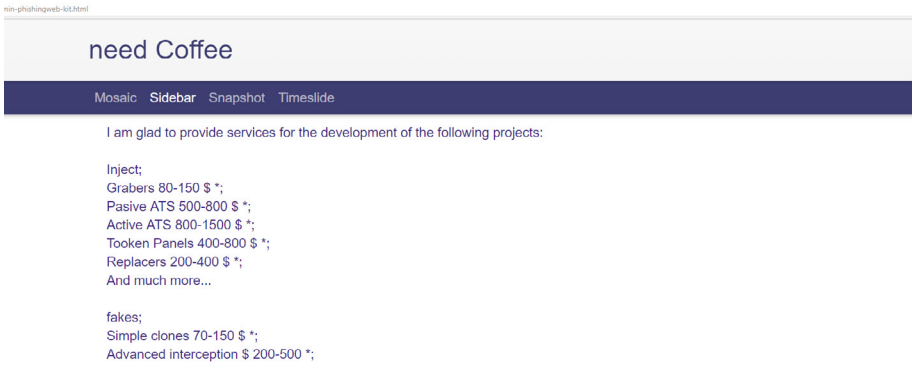


Figure 41. Cost of phishing site development services

3.2. Infrastructure

The Internet is brimming with providers of legal commercial VPN, domain registration, and hosting services.

Attackers can purchase the services of such providers relatively cheaply by registering with other people's passport data.

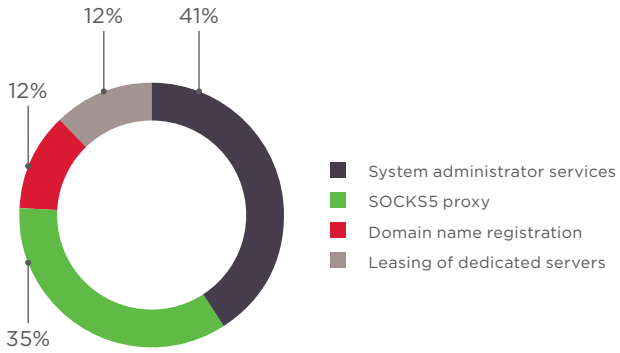


Figure 42. Types of infrastructure-related services requested

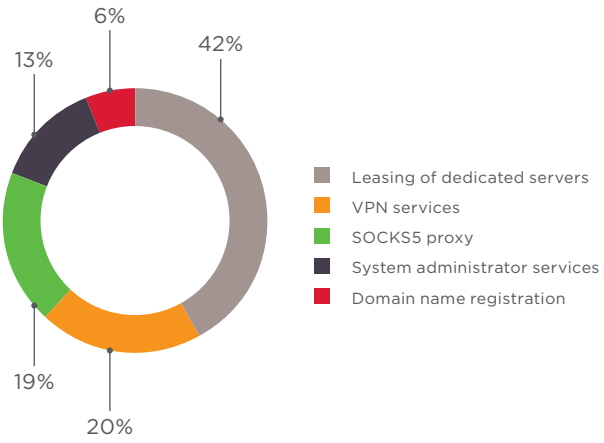


Figure 43. Types of infrastructure-related services offered

19 medium.com/@MikeBacina/buzz-off-ico-phishing-scams-44b8e5620211

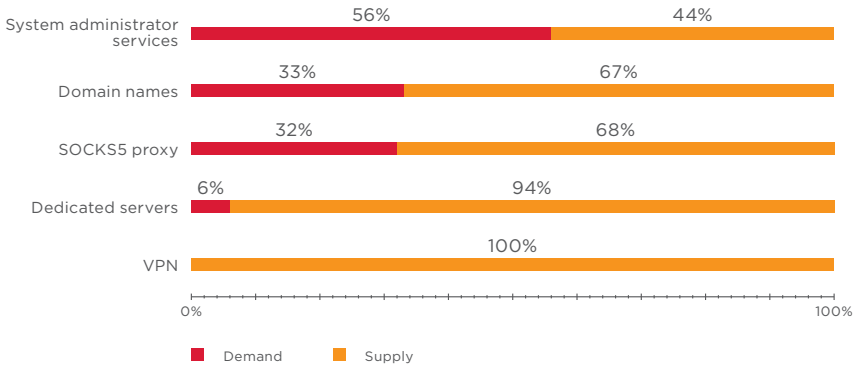


Figure 44. Supply–demand ratio for infrastructure-related services

Both legal and illegal VPN services are used in cyberattacks to provide anonymity for the perpetrators.

The main criterion by which cybercriminals choose a service is the lack of a user tracking system, that is, no records linking an IP address to a specific user.

The price for commercial VPN services starts at $5 per month, ignoring seasonal discounts and the like.

However, some users prefer more expensive—and thus generally more reliable—services, which can cost upwards of $15 per month.

Such services are legal and openly advertised online. That said, ads for them can also appear in dark web forums where cybercrooks might leave feedback about a certain VPN service, prompting other criminals to make the same choice.

The situation is similar with the lease of dedicated servers, which are used by attackers as C&C centers for malware, hosting sites, or intermediate nodes from which an attack is carried out.

Owners lease such servers on shadow market forums at prices starting from $80 per month.

In addition to hosting services to create a phishing site, the cybercriminals need a domain name, which can be obtained for $3–10 through a registrar.

The domain name registrar usually checks the passport data of the buyer.

However, as noted above, buying a scanned copy of a passport does not pose too much of a problem.

Some services accept payment for domain registration in cryptocurrency; cryptowallets can be created in a matter of minutes and do not contain information about the owner, again helping the criminals to remain anonymous.

It is no surprise that such services enjoy solid demand.

3.3. Spam and phishing

Today, there can be very few Internet users who have not encountered a phishing or spam email.

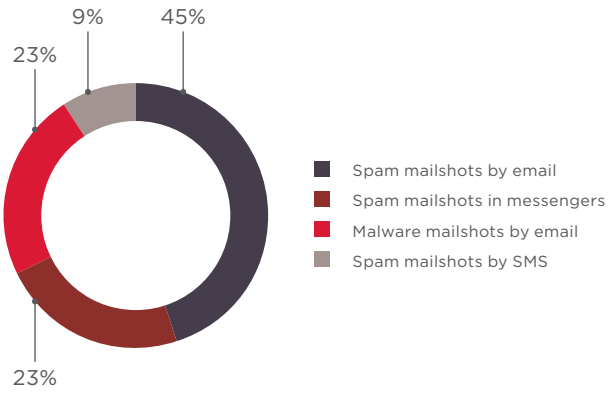


Figure 45. Demand for mailshot services

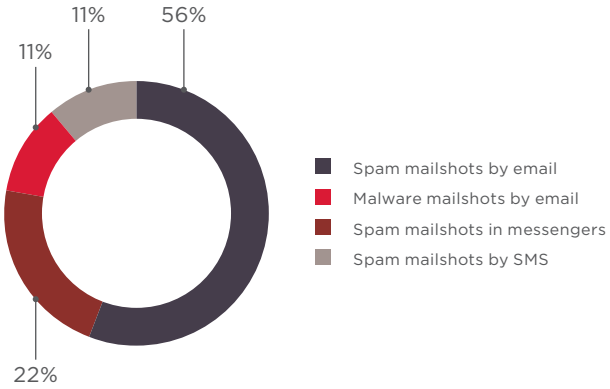


Figure 46. Supply of mailshot services

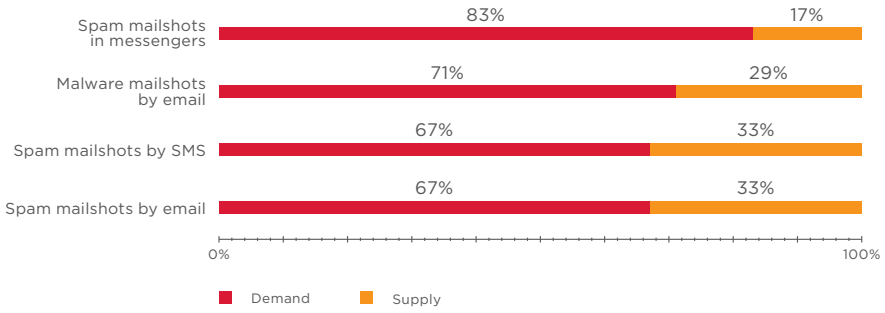


Figure 47. Supply–demand ratio for mailshot services

In order to expand the potential victim base, criminals often use mass mailing services advertised on specialized forums.

It is possible today to send an email containing text and a file attachment to 1,000 random addresses all at once—for less than $1!

And of course there are services offering themed mailshots to whet the appetite of a certain user group.

The business model is sound, since just one ransom payment by the owner of an infected computer would cover the cost of the mailshot many times over.

index.php?showtopic=130979&hl=spam+service

Hello.

If you sick for looking spammers who are sending only 10k and after that they logout,
We have our service for sending milions of emails per day (**INBOX**) !

*__Note:__ We send only with links, we don't spam with attached file.

10k emails = $100
100k emails = $800
1 milion emails = $4000

Figure 48. Supply of mass mailshots

3.4. Custom hacking services

In the public mind, hackers are associated with attacks on servers belonging to state institutions and large companies.

In reality, the majority of dark web requests for hacking services are related to finding website vulnerabilities (36%) and retrieving email passwords (32%).

In fact, only 23 percent of dark web visitors are looking for someone able to carry out an attack on a remote server.

Among the services on offer, top place goes to hacking social network (33%) and email (33%) accounts.

On the one hand, this is because some people are desperate to gain access to someone else's messages, and on the other, this kind of hacking requires no technical skills on the part of the perpetrator.

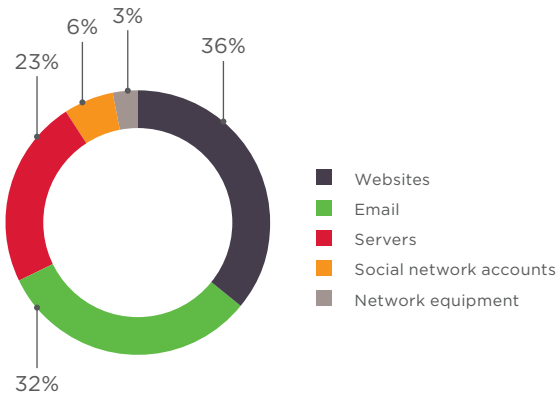


Figure 49. Demand for hacking services

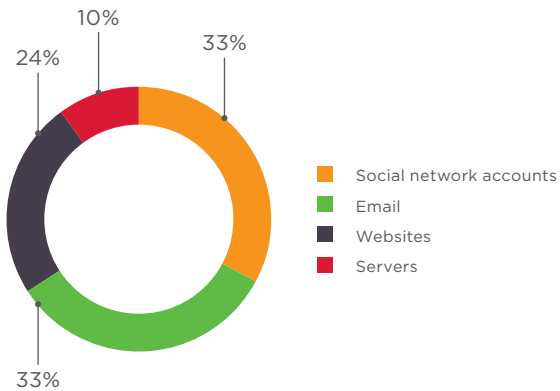


Figure 50. Supply of hacking services

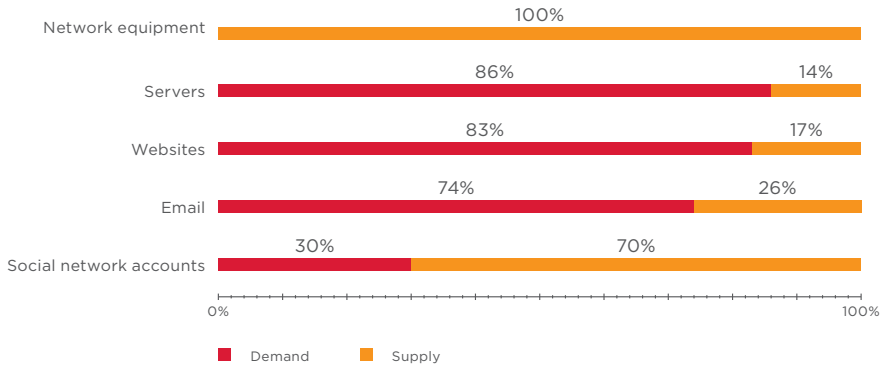


Figure 51. Supply–demand ratio for hacking services

3.4.1. Hacking email and social network accounts

On shadow websites, hacking services aimed at mailboxes and accounts in popular social networks cost from $40.

There are many reasons why hackers and their clients might need access to someone's mailbox or social network account.

Some want to read the private correspondence of celebrities, others to access the confidential information of business competitors, still others just want to control friends or relatives.

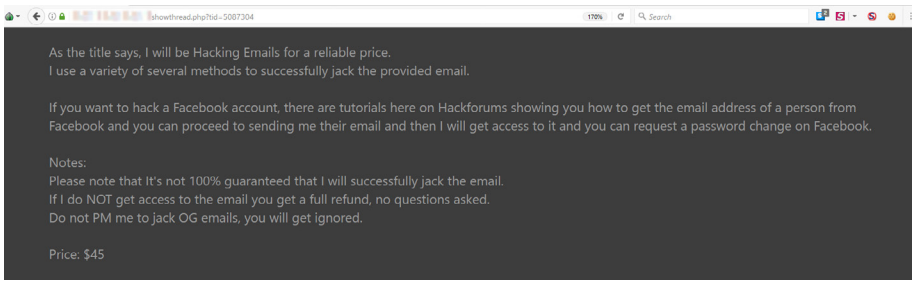


Figure 52. Mailbox hacking

Access to email automatically gives control over all the victim's personal accounts for which this email address was specified during registration, including social networks, forums, online stores, e-wallets, and many other services.

The attacker needs only send a password recovery request to these sites and then change the password to their.

It is much easier and more effective to hack just one email account than trying to steal the credentials of one person across many different platforms; hence this hacking service remains in demand.

3.4.2. Hacking sites, servers, and network equipment

There are various reasons for wanting to gain control over a website: to access a database of users, post malicious content, test one's hacking skills, make a personal or political statement (for example, defacing).

To carry out an attack, cybercriminals need to gain control over the site or exploit vulnerabilities in the web application.

Given the extremely low protection of most online resources, this is not such a complex task.

Website hacking services are provided both by lone-wolf hackers and groups.

In the dark web, the price for hacking one web resource starts at $150.

The highest price on the trading platforms we investigated did not exceed $1,000.

In 2017, site hackers focused their attention on cryptocurrency projects: exchanges and companies holding ICOs.

Simply by changing the wallet number on the target ICO project site, attackers redirected millions of dollars of cryptocurrency investments into their own wallets.

Hacking web resources is not only the most common ICO attack method, but also the most successful: in the course of our ICO robustness analysis, web application vulnerabilities were discovered in 32 percent of projects.

Furthermore, vulnerable sites can be used by attackers to host malware for later campaigns, making the owners of such sites unwitting links in the attack chain.

A similar technique was used by the Cobalt group, whose methods are described in one of our reports.[20]

It's also worth mentioning hacktivists, who carry out politically motivated hacking and defacing of government websites.

The work of expert server hackers using password-cracking malware is valued at $150–250 per week.

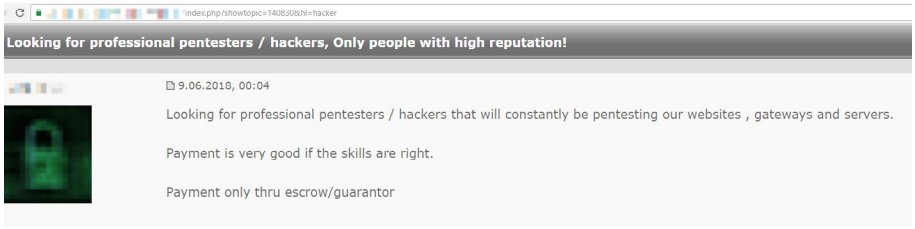


Figure 53. Recruiting a hacking team

Accesses obtained in this manner are sold on shadow trading platforms or monetized by the attackers themselves, for example using cryptominers or encryptors.

Access to network equipment is gained in a similar fashion: users often forget to change the default password, allowing attackers to crack it in their sleep.

More often than not, hacked devices are infected with special malware and connected to a botnet, which is then deployed in DDoS attacks.

Professional cybercriminal groups often seek out specialists with in-depth technical skills in the field of searching for vulnerabilities and hacking network resources.

The platforms we studied featured ads offering people with this skill set a wage of $3,000.

What's more, the groups themselves provide hacking services, including attacks on web servers and infrastructure, charging upwards of $500 per attack.

20 ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf

3.5. Drops, cashout, and insiders

The ultimate aim behind almost every cyberattack is personal enrichment.

This is evidenced by our research statistics, which show that 70 percent of cyberattacks in 2017 were committed for financial gain.[21] However, the dirty profits of cybercriminal activity cannot immediately be transferred to a bank card.

Therefore, cybercriminals have to avail themselves of various shadow market financial services.

Funds transfer through payment systems is the most popular service (52%) and the most widely offered (35%).

Cybercriminals often use it to embezzle money from bank cards linked to payment system accounts.

The average commission charged by these services is 20 percent of the transfer amount.

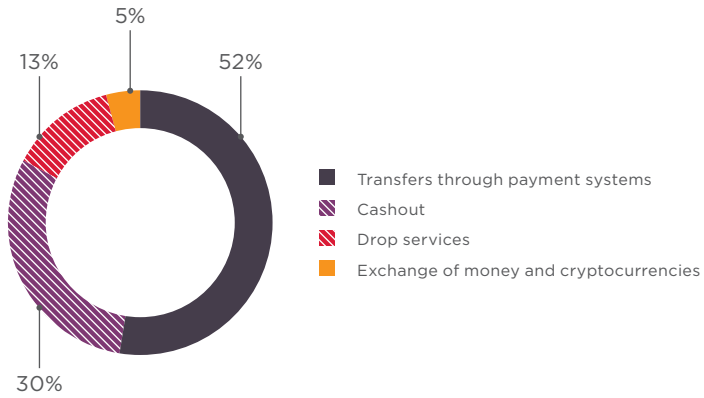


Figure 54. Demand for financial services

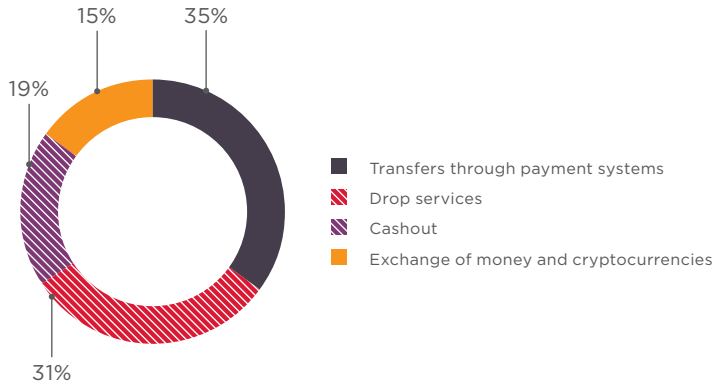


Figure 55. Supply of financial services

21 ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity-threatscape-2017-eng.pdf

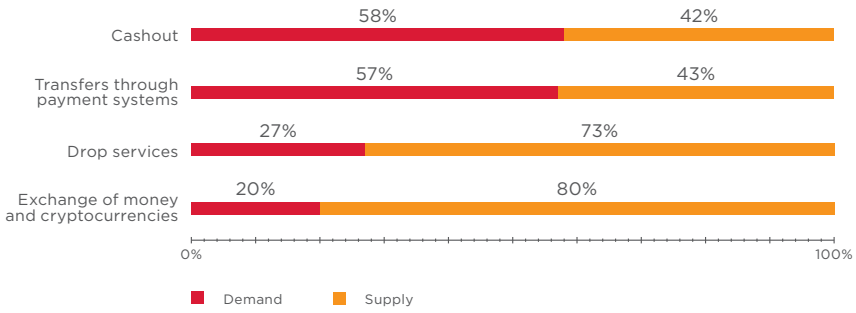


Figure 56. Supply–demand ratio for financial services

To implement various cashout schemes or other fraudulent activities, cybercriminals need accomplices inside financial institutions.

For example, a mobile phone store employee may be needed to identify the owner of a wallet in a payment system.

A bank employee could provide access to a client database containing information about depositors and borrowers.

There have been cases of bank employees issuing cards for clients' accounts without their knowledge and consent.[22]

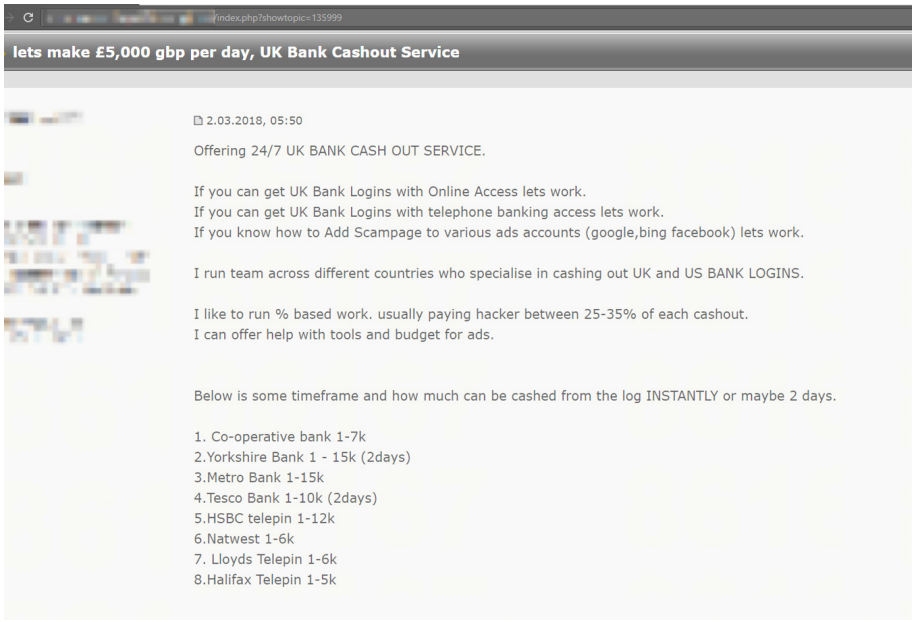


Figure 57. Cashout services

In situations where further actions require ID verification, or there is a high risk of exposure, cybercriminals employ the services of "drops."

Drops are stooges who do "dirty" jobs like withdrawing money from ATMs using duplicate cards, registering a legal entity in their own name, receiving and forwarding mail items, and other activities.

22 bankinfosecurity.com/ex-bank-employee-charged-fraud-id-theft-a-2474

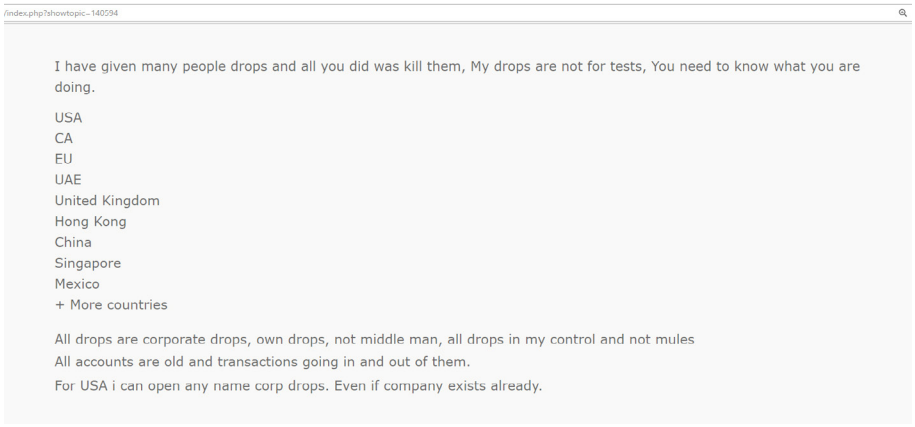


Figure 58. A drop handler with drops

To maintain anonymity, cybercriminals do not withdraw monetary funds directly to their cryptocurrency wallets or bank accounts.

For example, if an attacker wants to transfer a cryptocurrency from one wallet to another so that the transaction is untraceable, they can use the services of so-called Bitcoin mixers.

Cryptocurrency funds are transferred from the first wallet to the mixer wallet, after which the address of the second wallet is specified and the funds are moved on.

This means that the cryptocurrency arrives at the destination wallet from an unknown, unpredictable address.

The owners of such services exploit the operational intricacies of cryptocurrency exchanges and bookmaker services to muddle the transactions.

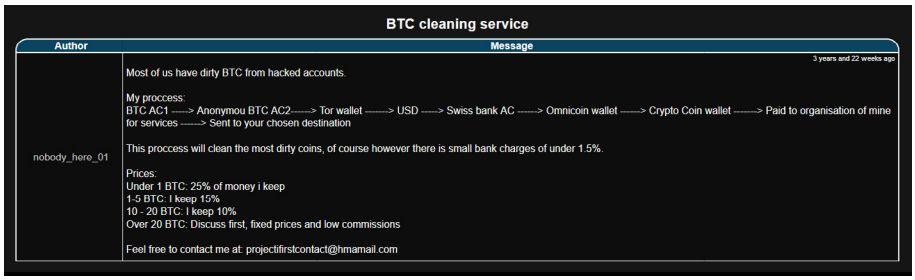


Figure 59. Money laundering

There are entire shadow market forums devoted to the topic of transferring, laundering, and cashing out money from bank accounts.

There exist numerous schemes linked to casinos, bookmakers, and shell companies that were not covered in this study.

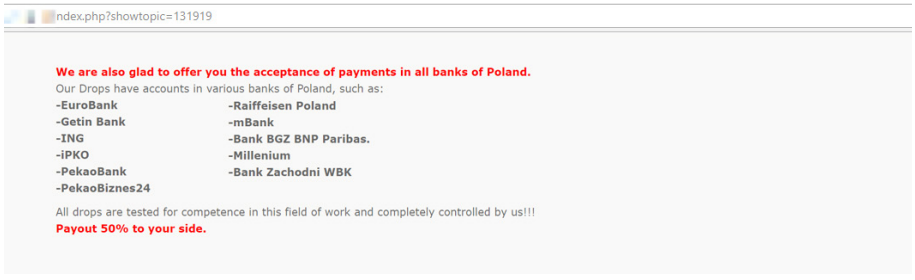


Figure 60. Supply of cashout services using drops

3.6. Botnets

Generally speaking, a botnet is a group of devices that are infected with a special Trojan and can perform certain instructions issued by a single C&C center.

The most harmless botnets are ones that drive up likes and views—something that ordinary users, professional bloggers, and online companies all value.

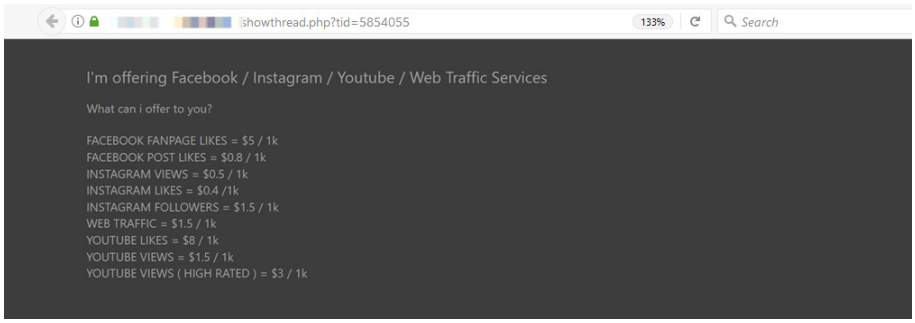


Figure 61. Driving up video views on a popular platform

The price of a bot-generated like on a popular video platform, for instance, starts at ₽0.1, while one vote in a popular movie rating service costs from ₽6.

Botnets also can be used for cryptocurrency mining.

The rewards might not be vast, but still greater than the zero generated by an idle botnet.

Assuming that one bot can mine Monero cryptocurrency at a rate of 40 hashes per second (equivalent to an income of $2 per month at the time of this study), then a botnet of 1,000 computers will increase the attacker's revenue by $2,000 per month.

On the whole, the botnet scenarios are limited only by the capabilities of the malware controlling the infected nodes and the attackers' imagination.

3.7. DDoS

When it comes to deploying botnets, the topic of DDoS attacks warrants a separate mention.

The dark web features a wide range of automated services and offers from hacker teams for conducting DDoS attacks of any complexity.

A 270 Gbit/s DDoS attack against a site costs about $50 per 24 hours.

DDoS attacks are one of the most common unfair business practices.

Neustar estimates the damage caused by every hour of attack for a third of US companies at $250,000.[23]

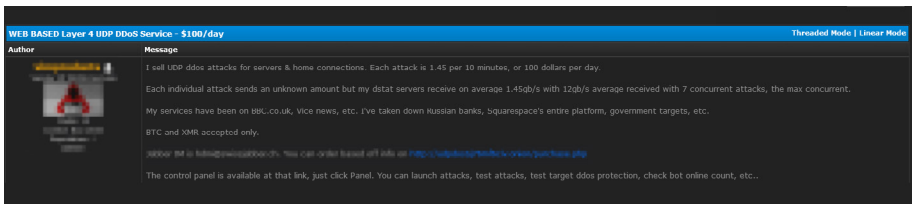


Figure 62. DDoS service

23 hello.neustar.biz/201710-Security-Solutions-Siteprotect-DDoS-2H2017-Report-LP.html

Conclusion

In Q1 2018, the number of unique incidents increased by 32 percent against the same period in 2017, with 63 percent of all incidents involving malware. This study has shown that demand for malware development services currently exceeds supply by a factor of three, and for distribution services by a factor of two. This points to growing demand for new tools on the part of cybercriminals, and such utilities are becoming increasingly available as a result of partner programs, malware leasing, and as-a-service distribution models.

This trend is not only causing a rise in the number of cyberincidents, but seriously hindering investigative efforts to properly attribute attacks. Clear attribution is possible only in the case of independently developed exclusive exploits and malware, or when such exclusive services are outsourced.

As a result, it can happen that cybercriminals are wrongly associated with a particular group because they buy the same services and malware on the shadow market. The same applies to determining the location or country of the attacker. The fact that malware contains comments in a certain language or phishing messages are riddled with errors is only evidence that such malware was written by a native speaker of the language and then sold to an unknown entity, or that such phishing messages were written by an illiterate student making a living by offering the most basic cyberservices on online forums.

All this could turn threat intelligence into a devilishly complex, perhaps even meaningless, process, since 100 percent–attribution will be impossible. If so, threat intelligence in its current form will cease to exist, and the focus will shift from indicators of compromise to dark web analysis with a view to identifying, based on the available indicators, not the attacking group, but the developer or seller of the malware. Based on information about who bought what and from whom, assumptions can then be drawn about the cybercriminal group. These methods have already proved themselves in practice and are actively applied.

At the same time, it is important to understand and analyze in greater depth the techniques and tactics used to organize an attack. Often, an attacker's skill set is revealed not by the tools they employ, but the errors they commit at the post-exploitation stage, or by their behavior in the compromised infrastructure. Unfortunately, for various reasons, many companies are not ready to deal with hacking or investigate major incidents, which involves searching for all relevant artifacts, tracing the attack chain, and analyzing the intruders' actions inside the infrastructure. But if a top-class team is hired to do the job, and their recommendations are implemented, the security and robustness of the organization are increased by an order of magnitude, and future hackers will be seriously deterred by the extra complexity and costs they face.

ptsecurity.com
info@ptsecurity.com