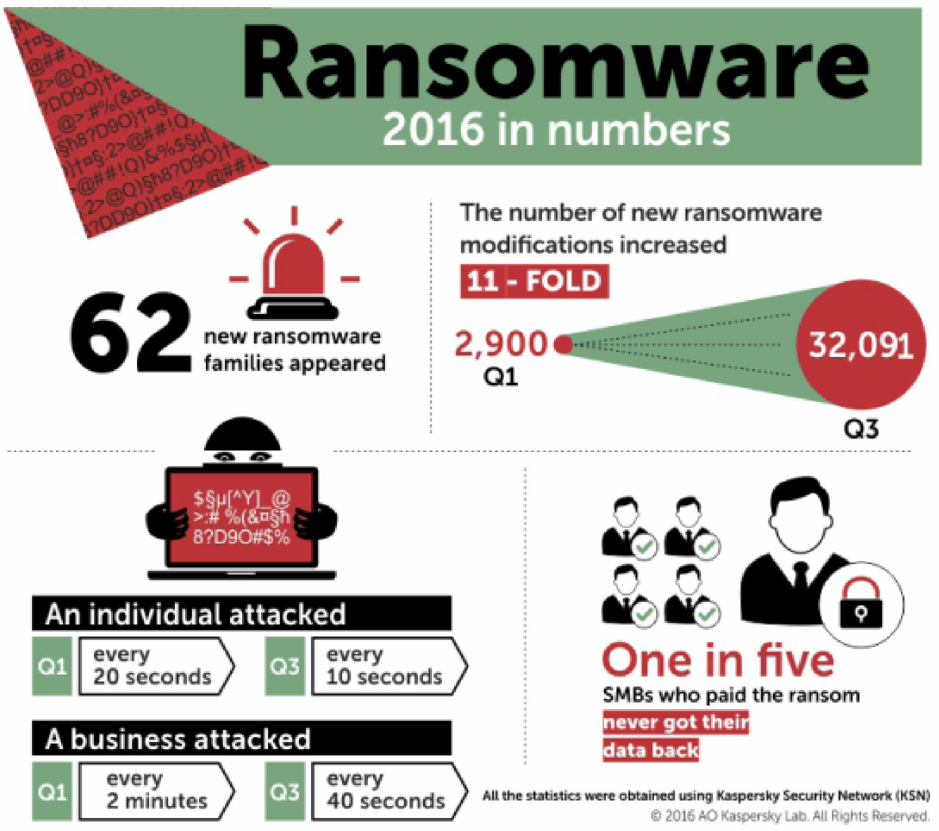
A look into the Russian-speaking ransomware ecosystem

CRYPTO MALWARE STATISTICS RANSOMWARE RUSSIAN-SPEAKING CYBERCRIME

By Anton Ivanov on February 14, 2017. 12:41 am

PUBLICATIONS

It is no secret that encryption ransomware is one of the key malware problems today, for both consumers and corporate users. While analyzing the attack statistics for 2016, we discovered that by the end of the year a regular user was attacked with encryption ransomware on average every 10 seconds, with an organization somewhere in the world hit around every 40 seconds.



Kaspersky Lab statistics on the ransomware threat in 2016

In total we've registered attacks using encryption ransomware against 1,445,434 users worldwide. Between them, these people were attacked by 54 thousand modifications of 60+ families of crypto ransomware.

So why is this happening now if encryption ransomware, as a type of malware, has existed since the mid-2000s? There are three main reasons:

- It's easy to buy a ransomware build or builder on the underground market
- It's easy to buy a distribution service
- Crypto ransomware, as a business, has a very clear monetization model through cryptocurrencies

In other words, this is a fine tuned, user friendly and constantly developing ecosystem. In the last few years we, at Kaspersky Lab, have been monitoring the development of this ecosystem. This is what we've learned.

1. In most cases crypto ransomware has a Russian origin

One of the findings of our research is that 47 of the 60+ crypto ransomware families we've discovered in the last 12 months are related to Russian-speaking groups or individuals. This conclusion is based on our observation of underground forums, command and control infrastructure, and other artefacts which can be found on the web. It is hard to draw strong conclusions on why so many of the ransomware families out there have a Russian origin, but it is safe to say that this is because there are a lot of well-educated and skilled code writers in Russia and its neighboring countries.

Another possible reason is that the Russian cybercriminal underground has the richest background when it comes to ransomware schemes. Prior to the current crypto ransomware wave, there was another ransomware-themed malware epidemic. Between approximately 2009 and 2011, thousands of users in Russia and its neighboring countries experienced attacks which used so-called Windows- or browser-lockers. This type of ransomware blocks the user's access to their browser or OS and then demands a ransom in exchange for unlocking access. The epidemic withered for a number of reasons: law enforcement agencies responded adequately and caught several criminals involved in the business; mobile operators made the process of withdrawing money through premium SMS services harder; and the security industry invested a lot of resources into developing free unlocking services and technologies.

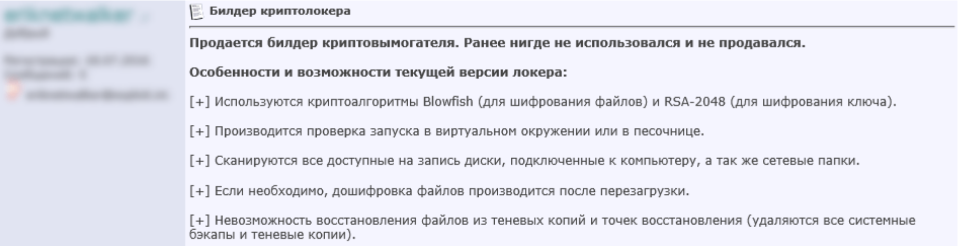
But it seems that experienced ransomware criminals haven't disappeared, they've just been waiting for a new monetization model, which has now emerged in the form of crypto currencies. This time though, the ransomware problem is not specifically Russian, but global.

2. There are three types of involvement in the ransomware "business"

The Russian underground crypto ransomware market currently offers criminals three different ways of entering the illegal business.

- Create new ransomware for sale
- Become a partner in a ransomware affiliate program
- Become the owner of an affiliate program

The first type of involvement requires advanced code writing skills, including a deep knowledge of cryptography. The actors which we have observed in this category are like gun traders: they usually don't participate in actual attacks, but only sell code.



[redacted]

Билдер криптолокера

Продается билдер криптовымогателя. Ранее нигде не использовался и не продавался.

Особенности и возможности текущей версии локера:

[+] Используются криптоалгоритмы Blowfish (для шифрования файлов) и RSA-2048 (для шифрования ключа).

[+] Производится проверка запуска в виртуальном окружении или в песочнице.

[+] Сканируются все доступные на запись диски, подключенные к компьютеру, а так же сетевые папки.

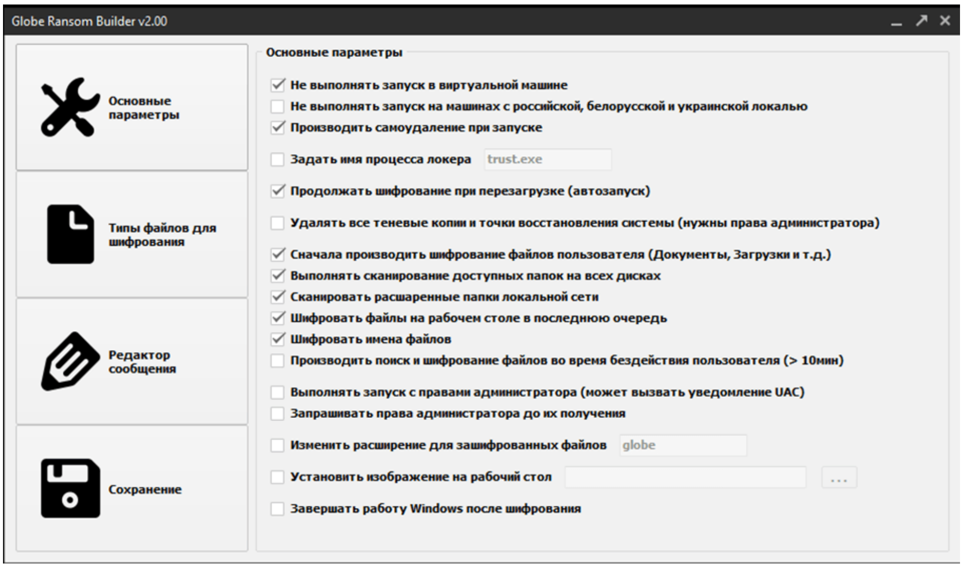
[+] Если необходимо, дошифровка файлов производится после перезагрузки.

[+] Невозможность восстановления файлов из теневых копий и точек восстановления (удаляются все системные бэкапы и теневые копии).

An example of an advertisement selling unique crypto malware, posted by its creator. The author promises encryption with Blowfish and RSA-2048 algorithms, anti-emulation techniques, advanced scanning capabilities, and functions allowing for the removal of backups and shadow copies of the information stored on the victim's PC.

Sometimes, authors of the malware sell their "products" with all the source code for a fixed price (usually several thousand dollars) and sometimes they sell their builder – the tool which allows criminals with no programming background to build the crypto ransomware with a specific list of functions.

The following illustration provides hints as to what capabilities a builder gives to a criminal. For example, it allows criminals to create ransomware which will start encrypting files only after 10 minutes of user inactivity; which will change the extensions of encrypted files to one of the criminals' choice; and which will request administrator privileges until it receives it. It also allows criminals to change desktop wallpapers to arbitrary ones, and to implement some other features that in the end can be combined into a very dangerous piece of software.



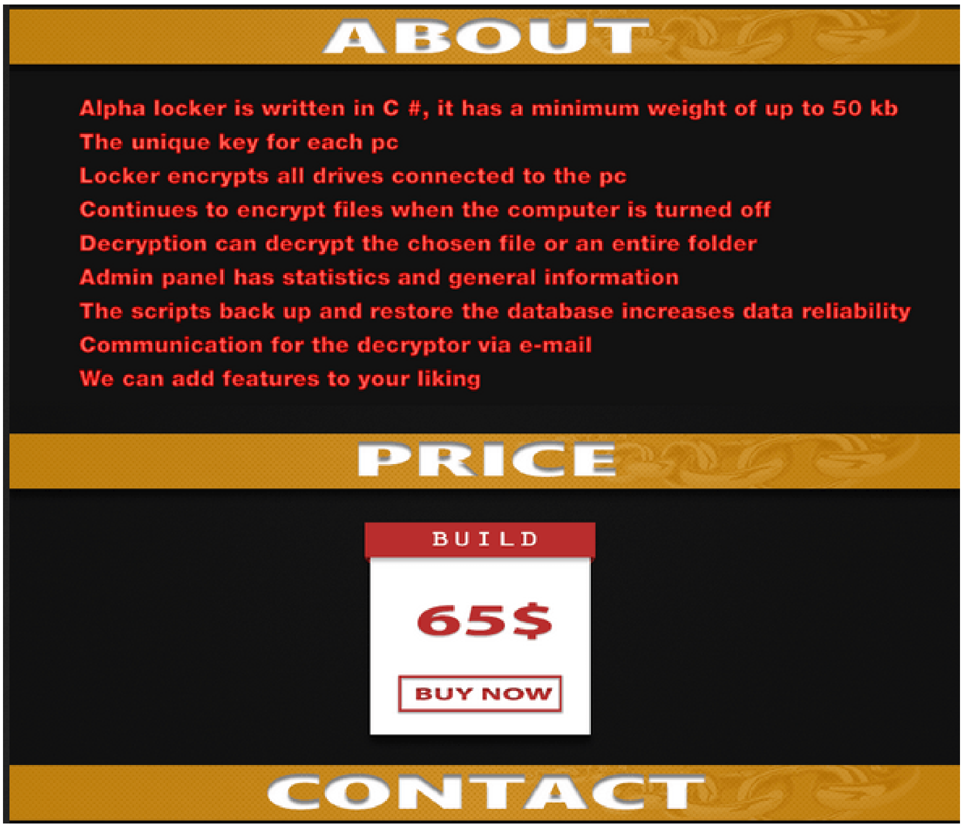
Основные параметры

☑ Не выполнять запуск в виртуальной машине
□ Не выполнять запуск на машинах с российской, белорусской и украинской локалью
☑ Производить самоудаление при запуске
□ Задать имя процесса локера trust.exe
☑ Продолжать шифрование при перезагрузке (автозапуск)
□ Удалять все теневые копии и точки восстановления системы (нужны права администратора)
☑ Сначала производить шифрование файлов пользователя (Документы, Загрузки и т.д.)
☑ Выполнять сканирование доступных папок на всех дисках
☑ Сканировать расшаренные папки локальной сети
☑ Шифровать файлы на рабочем столе в последнюю очередь
☑ Шифровать имена файлов
□ Производить поиск и шифрование файлов во время бездействия пользователя (> 10мин)
□ Выполнять запуск с правами администратора (может вызвать уведомление UAC)
□ Запрашивать права администратора до их получения
□ Изменить расширение для зашифрованных файлов globe
□ Установить изображение на рабочий стол ...
□ Завершать работу Windows после шифрования

The interface of the Globe ransomware builder

Builders are usually much cheaper than the full source code of unique ransomware – hundreds of dollars. However, authors (and owners) of software like this often charge customers for each new build of malware created with help of their software.

Pay-per-build is another type of monetization used by the authors of the original ransomware. In this case the price drops even lower, to tens of dollars, but the client would receive the malware with a fixed list of functions.

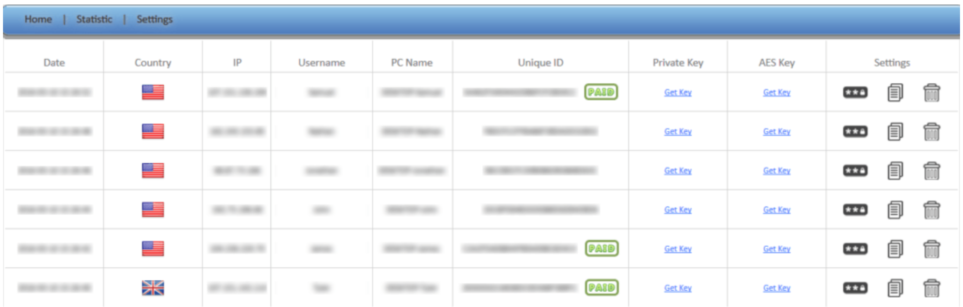


Alpha locker is written in C #, it has a minimum weight of up to 50 kb
The unique key for each pc
Locker encrypts all drives connected to the pc
Continues to encrypt files when the computer is turned off
Decryption can decrypt the chosen file or an entire folder
Admin panel has statistics and general information
The scripts back up and restore the database increases data reliability
Communication for the decryptor via e-mail
We can add features to your liking

65$

An advertisement offering unique crypto ransomware with a pay-per-build model

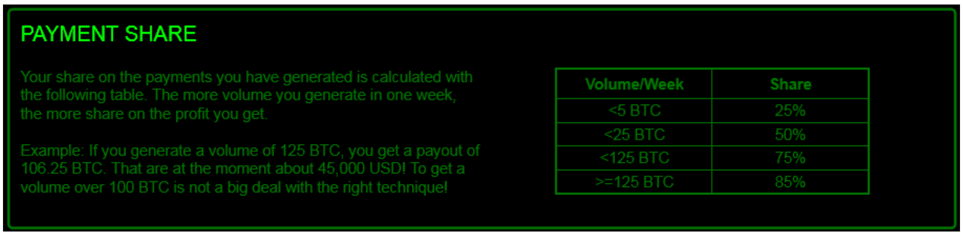
The build often includes not only the malware code itself, but also tools for statistics and interaction with infected PCs.



Date	Country	IP	Username	PC Name	Unique ID	Private Key	AES Key	Settings
[redacted]	🇺🇸	[redacted]	[redacted]	[redacted]	[redacted] PAID	Get Key	Get Key	🔒 📄 🗑
[redacted]	🇺🇸	[redacted]	[redacted]	[redacted]	[redacted]	Get Key	Get Key	🔒 📄 🗑
[redacted]	🇺🇸	[redacted]	[redacted]	[redacted]	[redacted]	Get Key	Get Key	🔒 📄 🗑
[redacted]	🇺🇸	[redacted]	[redacted]	[redacted]	[redacted]	Get Key	Get Key	🔒 📄 🗑
[redacted]	🇺🇸	[redacted]	[redacted]	[redacted]	[redacted] PAID	Get Key	Get Key	🔒 📄 🗑
[redacted]	🇬🇧	[redacted]	[redacted]	[redacted]	[redacted] PAID	Get Key	Get Key	🔒 📄 🗑

An example of a command and control panel which comes with the build of a certain ransomware family

Affiliate programs, the third type of involvement in the ransomware criminal business, is a rather standard form of cybercrime: owners of the program provide partners with all the necessary infection tools, and then the partners work on distributing the malware. The more successful their efforts, the more money they receive. Participation in such programs requires nothing but the will to conduct certain illegal activities and couple of bitcoins as a partnership fee.



PAYMENT SHARE

Your share on the payments you have generated is calculated with the following table. The more volume you generate in one week, the more share on the profit you get.

Example: If you generate a volume of 125 BTC, you get a payout of 106.25 BTC. That are at the moment about 45,000 USD! To get a volume over 100 BTC is not a big deal with the right technique!

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

An advertisement for an affiliate program

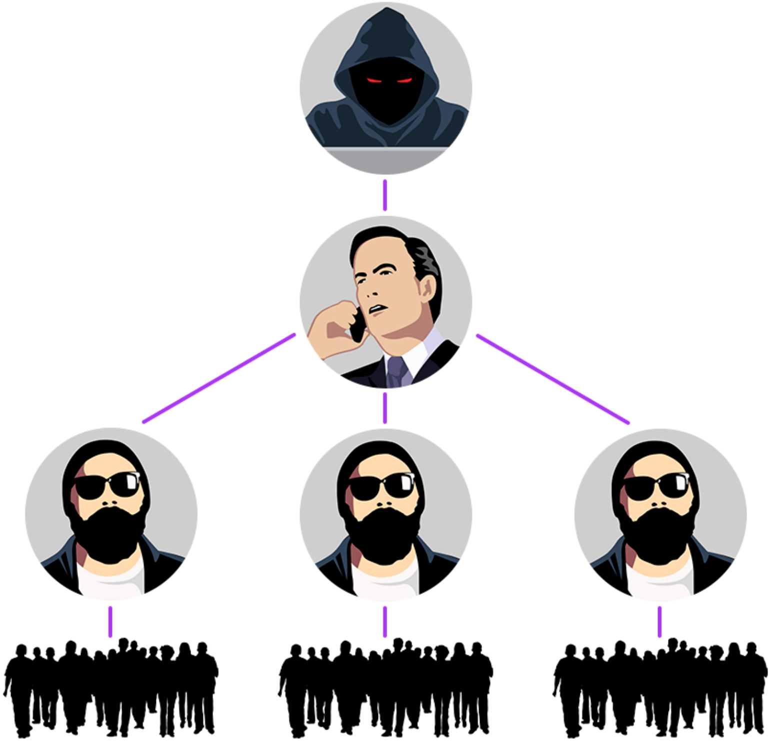
Interestingly, while researching the development of the underground ransomware ecosystem, we discovered two types of affiliate programs: one for all, and one for specific partners.

Unlike the programs for everyone, “elite” programs won’t accept just any kind of partner. In order to become a partner in an elite program, a candidate has to provide a personal recommendation from one of the acting partners in the program. Besides that, the candidate must prove that they have certain malware distribution capabilities. In one case we observed in the last year, the candidate had to demonstrate their ability to complete at least 4000 successful downloads and installations of the malware on victim PCs. In exchange, the partner gets some free tools for the obfuscation of ransomware builds (in order to make them less visible to security solutions) and a good conversion rate – up to 3%, which is a very good deal, at least compared to rates that legal affiliate programs offer.

To summarize all that is written above: flexibility is the key feature of the current underground ransomware ecosystem. It offers lots of opportunities to people with a propensity towards criminal behavior, and it almost doesn't matter what level of IT experience they have.

3. There are some really big players on this market

If you think that being the owner or a partner of an "elite" affiliate program is the highest possible career milestone in the world of ransomware, you are mistaken. In reality, ransomware creators, their stand-alone clients, partners and owners of affiliate programs are often working for a bigger criminal enterprise.



The structure of a professional ransomware group contains the malware writer (aka the creator of the group), affiliate program owners, partners of the program, and the manager who connects them all into one invisible enterprise

There are currently several relatively large ransomware groups with Russian-speaking participants out there. In the last few months we've been researching the operation of one such group and now have an understanding of how it operates. We consider this group an interesting one, because it is built in a way that made it really hard for us to identify all its affiliates. It consists of the following parties: The creator, the manager, the partners, and affiliate programs. According to our intelligence the creator and the leader of this group is the ransomware author. He developed the original ransomware, additional modules for it and the IT infrastructure to support the malware operation. The main task of the manager is to search for new partners and support existing ones. According to our knowledge, the manager is the only person who interacts with the creator. The primary task of partners is to pick up the new version of ransomware and distribute it successfully. This means successfully infecting as many PCs as possible and demanding a ransom. For this – among other tools – partners utilize the affiliate programs which they own. The creator earns money by selling exclusive malware and updates to the partners, and all the other participants of the scheme share the income from the victims in different proportions. According to our intelligence, there are at least 30 partners in this group.

4. Costs and profits on the underground ransomware market are high

We estimate that the revenue of a group like the one described above could reach as much as thousands of dollars a day in successfully demanded ransom payments. Although, of course, as with any other type of malicious activity at a professional level, the professional ransomware player spends a lot on resources in order to create, distribute and monetize the malicious code.

The structure of the operating cost of a large ransomware group more or less looks like the following:

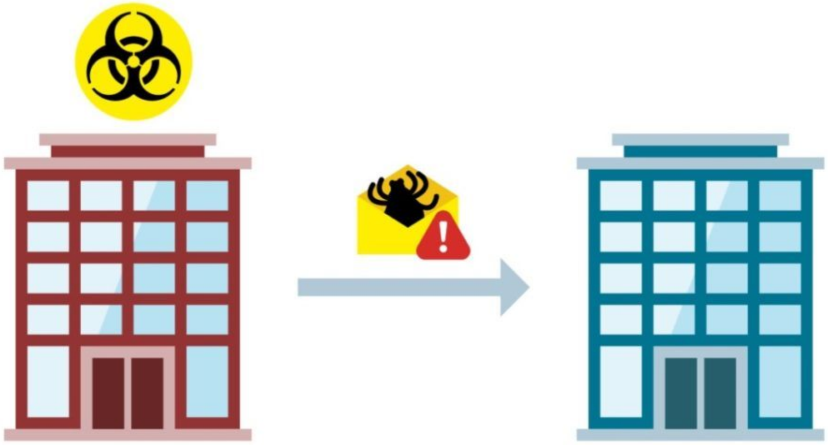
1. Ransomware modules update
   a. New features
   b. Bypass techniques
   c. Encryption improvement
2. Distribution (spam/exploit kits)
3. AV check service
4. Credentials for hacked servers
5. Salary for hired professionals (usually these are IT administrators who support the server infrastructure)

The core of the whole group's mechanics is ransomware code and the distribution channels.

They distribute ransomware in four main ways: exploit kits, spam campaigns, social engineering, hacked dedicated servers, and targeted hacks. Exploit kits are one of the most expensive types of distribution tool and could cost several thousand dollars per week, but, on the other hand, this type of distribution is one of the most effective in terms of the percentage of successful installations.

Spam emailing is the second most popular form of distribution. Spear phishing emails sent by criminals are usually disguised as an important message from a government organization or large bank, with a malicious attachment. According to what we've observed in the last year, spamming targets with malicious emails is a more than workable method, because in 2016 the amount of ransomware-related malicious spam blocked by our systems was enormous.

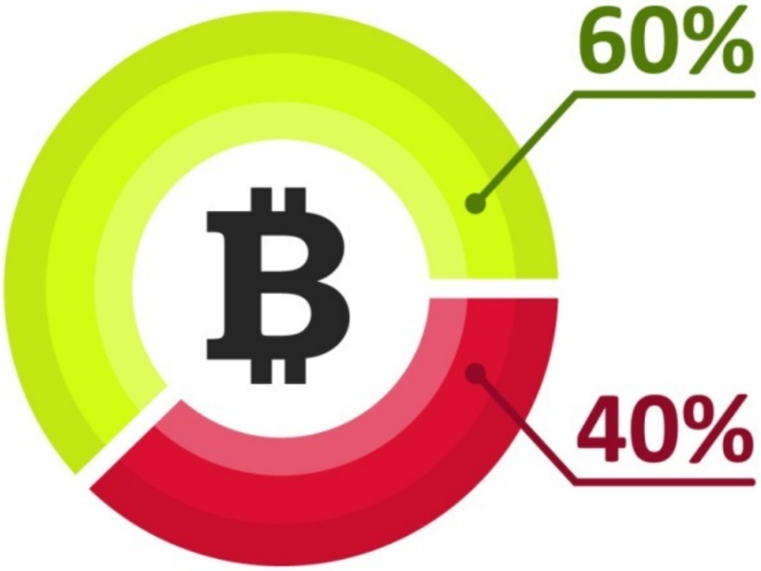
And sometimes the emails that the targets of ransomware hackers receive are technically legit. While working on incident response we've observed several instances where an email with a malicious attachment (which in the end encrypted important victim data) was sent out from a legitimate email, by a legitimate user. Very often, these are emails from clients or partners of an attacked organization, and after digging deeper and talking to representatives of the organization which sent the malicious emails, we learned that that organization was infected as well.



How criminals use one infected organization to attack another

It appeared to us that the ransomware criminals initially infected one organization, then got access to its email system and started sending out emails with a malicious attachment to the whole company's contact list. It is hard to underestimate the danger of this form of ransomware distribution: even if the recipient of an email like this is aware of the main methods used by cybercriminals use to distribute malware, there is no way for him/ her to identify the attack.

As we've learned, the operating costs that ransomware criminals face to support their campaigns may amount to tens of thousands dollars in some cases. Even so, this business is unfortunately extremely profitable. Based on what we've seen in conversations on underground forums, criminals are lining their pockets with nearly 60% of the revenue received as a result of their activities. So, let's go back to our estimate of the daily revenue of a group, which may be tens of thousands of dollars on a good day.



The typical distribution of profit (green) vs. operating costs (red) in a ransomware business

That’s of course an estimate of cumulative net income: the total sum of money which is used as payoffs to all the participants of the malicious scheme – starting from regular affiliate program members and ending with the elite partners, manager and the creator. Still, this is a huge amount of money. According to our observations, an elite partner generally earns 40-50 bitcoins per month. In one case we’ve seen clues that an especially lucky partner earned around 85 bitcoins in one month, which, according to the current bitcoin exchange rate, equals $85,000 dollars.

5. Professional ransomware groups are shifting to targeted attacks

An extremely worrying trend which we are observing right now is that ransomware groups with large budgets are shifting from attacking regular users and, occasionally, small companies, towards targeted attacks against relatively large organizations. In one of our incident response cases we have seen a targeted attack against a company with more than 200 workstations, and in another case one had more than 1000.

The mechanics of these new attacks are very different to what we’ve been used to seeing.

- For initial infection they have not used exploit packs, or spear phishing spam. Instead, if they were able to find a server belonging to the targeted company, they tried to hack it

- To get into the organization’s network, this group used open source exploits and tools
- If the organization had an unprotected server with RDP access this group tried to use brute force against it
- To get the necessary access rights to install ransomware in the network with psexec they used a Mimikatz tool.
- Then they could establish persistence using an open sourced RAT tool called PUPY
- Once they had gained a foothold in the attacked network, they studied it, choose the most important files and encrypted them with a custom, yet unseen, build of ransomware.

Another group which we have found in another large organization did not use any ransomware at all. They encrypted data manually. To do this they choose important files on a server and move it into a password protected archive.

Conclusion

In both cases described above the actors demonstrated a modus operandi that is characteristic of targeted attack actors – while we’re almost 100% sure that the groups behind these attacks are the ones that previously worked mostly on widespread ransomware campaigns. There are two main reasons why we think ransomware actors are starting to implement targeted methods in their operations.

1. Thanks to multiple successful massive campaigns they’re now funded well enough to invest big money in sophisticated operations.

2. A ransomware attack against a large corporation makes total sense, because it is possible to paralyze the work of a whole company, resulting in huge losses. Due to this, it is possible to demand a ransom larger than the one requested from home users and small companies.

We have already seen a mutation of this kind with another dangerous type of malicious activity: the financial cyberattack. These also started as massive attacks against the users of online banking. But as time passed, the actors behind these campaigns shifted their interests, firstly to small and medium companies, and then to large corporations, the banks themselves.

It is also important to note that so far the ransomware business has been considered a safe one by criminals. This is due to their certainty that the use of crypto currencies allows them to avoid being tracked by the “follow the money” principle, as well as the lack of arrests of gangs involved in ransomware. From our perspective all these conclusions are wrong. We hope that law enforcement agencies will soon start paying more attention to these groups.

Sun Tzu said: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

This article has two main purposes: to educate people interested in fighting ransomware and to raise awareness of the problem which targeted attacks with the use of ransomware can bring.

Although well-publicized prosecution cases against ransomware actors are yet to take place, people and companies can act now to make the job of ransomware actors harder and protect their data. First of all, make regular backups and store them on a drive that is air-gapped from your organization's main network.

Don't forget to protect your servers with proven security solutions. They identify and block the most recent versions of ransomware strains.

And the main advice – DO NOT PAY! If you pay the ransom, you money will be pumped into the malicious ecosystem, which is already flooded with funds. The more money criminals get, the more sophisticated tools they get access to, giving them access to much broader attack opportunities.

Related Posts

THERE IS 1 COMMENT

If you would like to comment on this article you must first login

Zunzutech
Posted on February 18, 2017. 5:32 am

You said "The first type of involvement requires advanced code writing skills, including a deep knowledge of cryptography."
Take a look at Stampado and think again.

Reply