Blackmailer: the story of Gpcode

securelist.com/blackmailer-the-story-of-gpcode/36089

Authors

- Expert Denis Nazarov
- Expert Olga Emelyanova

On June 7th, 2006, breaking news appeared on Analyst's Diary, the Kaspersky Lab weblog: "New Gpcode with a 660 bit key…cracked by Kaspersky Lab! And we've contacted the hosting company – the virus file's been removed from the site."

Analysts at Kaspersky Lab had successfully cracked a 660 bit RSA encryption key. This was the latest victory against a cyber blackmailer that had been plaguing users in Russia for over a year and a half.

Blackmail is as easy as 1, 2, 3

Virus.Win32.Gpcode marked the beginning of a new era in cyber crime. This new approach is reminiscent of a hostage/ ransom situation. An avalanche of emails from users in Russia, and a significantly smaller number from users in the rest of the world, shows that blackmail and racketeering are becoming widespread on the Internet.
Alexander Gostev, Malware Evolution: April – June 2005

It is easy to imagine how upset a user would be when they wake up on a sunny June morning and discover that their files are unusable: either they can't be opened or, in the case of .txt files, they contain garbage. And it's not only MS Office documents – over 80 different types of file are affected.

However, a few text files do open – files with suspiciously simple names such as readme.txt. But the text these files contain isn't going to make the victims happy: it makes it clear to the victims that there's an easy way to recover their data – simply buy a decoder program that will unlock 'certain files', i.e. those which have been encrypted using the RSA encryption algorithm.

Unfortunately, this wasn't a scene from a movie about cyber crime, but something that's been happening for over a year. Moreover, until recently it was unclear how victim machines became infected in the first place.

Thanks to some detective work by Kaspersky Lab virus analysts we do finally know how Gpcode has been spreading – at least the wave of new variants that hit Russia in early June.

The email shown below (originally in Russian) was mass mailed using spammer technologies, and was the first step in the infection process:

Hello !We are writing to you regarding the resume you have posted on the job.ru website. I have a vacancy that is suitable for you. ADC Marketing LTD (UK) is opening an office in Moscow and I am searching for appropriate candidates. I will soon be asking you to come in for an interview at a mutually convenient time.
If you are interested in my offer, please fill out the attached form related to compensation issues and email the results to me.
Sincerely,
Viktor Pavlov
HR manager

The email had an MS word .doc file called anketa.doc attached. (Anketa is the Russian for application form). This file actually contained a malicious program called Trojan-Dropper.MSWord.Tored.a. When the recipient opens the attachment, a malicious macro installs another Trojan – Trojan-Downloader.Win32.Small.crb – on the victim machine. This Trojan then downloaded Gpcode from [skip].msk.ru/services.txt and installed it to the victim machine.

Gpcode then scans all accessible directories and encrypts files with certain extensions such as .txt, .xls, .rar, .doc, .html, .pdf etc. It also encrypts mail client databases.

Gpcode and the Trojans used to install it then self-destruct, leaving a file called readme.txt in every folder which contain encrypted files. This text file provides information on how to contact the virus writer:

Some files are coded by RSA method.
To buy decoder mail: k47674@mail.ru
with subject: REPLY

Gpcode's author regularly changed the version of the virus placed on the website. S/he also changed the email address contained in the 'readme.txt' file. When a victim contacted the author, s/he offered to provide a decoder program. But naturally, this came at a price. The money was to be deposited in a Yandex account (Yandex is a major Russian web portal, which provides a payment system similar to PayPal.)

The infection and blackmail process is now clear, but this was far from the case when the first encrypted files were received in late 2004.

The first step is the hardest

In December 2004 we received the first samples of a number of files which were encrypted by an unknown encryption program. There was no hint that in six months time, such files would become so common that we would be receiving several dozen a day. Nor was there any clue that in the space of a single week in June, the different encryption methods used would exceed two dozen.
Alexander Gostev, Malware Evolution: April – June 2005

Kaspersky Lab virus analysts first encountered Gpcode in December 2004. Users reported that their files had been encrypted and no one could establish which program had been used to encrypt them. The only trace left by the virus (apart from encrypted files) was a text file called !_Vnimanie_!.txt ('vnimanie' is the Russian word for 'attention'). This file pointed to the Russian origin of the virus; the file name and text it contained were in Russian, and some encrypted files were of a format almost exclusively found in Russia.

The first wave of Gpcode hit mostly business users: Russian banks, advertising and real estate agencies, and other organizations using a large number of documents. Only a few companies outside Russia were affected.

The virus writer tried to trick users and analysts by placing a reference to PGP – "PGPcoder" in the headers of encrypted files. Thankfully, Gpcode's author initially used an encryption algorithm of his/ her own, which was easy for Kaspersky Lab analysts to crack.

The second wave of Gpcode infections hit in June 2005 and again, only Russian users were targeted. The encryption algorithm used was more complex than the one implemented in December 2004, but still relatively simple for Kaspersky Lab analysts to crack – after all, we'd seen over 25 variants of the first version of Gpcode. Best of all, this time we were able to get some samples of the program which was used to encrypt data.

So far so good. But one question remained unanswered – how did the virus actually get onto victim machines? As it turned out, this wasn't the only puzzle our analysts would have to solve.

A little learning can be a dangerous thing

Internet rackets are becoming more and more popular with virus writers. This is a very dangerous trend, which is intensifying with each passing month. However crude it may seem, this is a separate type of cyber crime.
Alexander Gostev, Malware Evolution: October – December 2005

The creator of Gpcode seemed to decide that blackmail was an easy way to make a living, and that his/ her creation needed some improvement. S/he spent almost 6 months studying encryption, and in early 2006 decided to test his/ her newfound strength.

On 26th January 2006, we intercepted yet another variant, Gpcode.ac, which was the first to use RSA encryption algorithms. RSA is one of the best known and most secure public encryption algorithms. The proud blackmailer even created a website; effectively 'RSA for dummies'.

The use of RSA encryption was a major leap forward from the simple encryption techniques the blackmailer had used previously. We were able to cope with this, but another Gpcode version, released in April, clearly showed that the author was continuing to hone his/ her encryption skills. This latest variant partially used the RSA algorithm, as had previous versions, but this time the encryption key was 67 bits, rather than 56 bits. Not a huge jump, but a sign of things to come.

New variants were used to launch a mass attack on Russian internet users at the beginning of June 2006.

The final round?

Since the beginning of 2006, the authors of such programs have attempted to radically alter the encryption methods used, in order to hinder the abilities of the antivirus industry to decrypt encrypted data. Previously, the author had used his own encryption algorithms, but with GpCode.ac, clearly decided to bring in the heavy guns
Alexander Gostev "Malware Evolution January – March 2006

In early June 3 variants of Gpcode appeared in the space of 5 days. Each variant used a longer encryption key: the first variant, Gpcode.ae had a 260 bit RSA key, while Gpcode.af already had 330 bit key. The longer the key, the more difficult it would be for antivirus companies to crack the encryption algorithm.

The situation was challenging. It took us 10 hours of manpower and some serious computing power to break the 330 bit key used by Gpcode.af. We added decryption routines to our databases and heaved a sigh of relief.

However, our relief was premature – the next day brought Gpcode.ag – with a 660 bit key. Currently, the longest factorized key on the RSA website is 640 bits. Even using a computer with a 2.2 GHz processor it would take 30 years to break such a key. We released detection and decryption routines on the day that Gpcode.ag was detected.

How did we do this? Well, that's a trade secret. And what does the future hold? That's not an easy or a pleasant question.

For a fistful of roubles

In order for our law enforcement agencies to take action (e.g. open a criminal case in accordance with section 273 of the Russian Criminal Code) at least one victim has to make an official complaint to the police.
Alexander Gostev, Kaspersky Lab weblog

One should never underestimate one's opponent – even if they lose. The Gpcode author planned the attacks carefully, using social engineering methods to spread the virus.

Spam containing malware was sent to email addresses harvested from job.ru – one of Russia's main recruitment websites. People who left their contact information received email which appeared to be from a major Western company. Naturally, they clicked on the attachment which supposedly contained details of the financial package. Given the circumstances, it would be hard to see how anyone could resist.

Opening the attachment didn't appear to trigger any malicious payload. But a Trojan was installed on the victim machine, and this Trojan then downloaded Gpcode soon after. This meant that very few people connected the recruitment email with their files becoming encrypted, and made it very difficult to determine the original infection vector.

It's a real shame that so much energy was expended for criminal purposes. Moreover, the fact that the author continued to create more variants is surprising given the financial rewards: s/he asked 2,000 rubles (approx $70) to decrypt the files. At the beginning, in December 2004, the asking price was 1000 rubles, though messages posted on the Internet showed that s/he was willing to accept as little as 500 rubles (approx $20).

Obviously, the Gpcode author is interested in volume, not individual sums. S/he was clearly counting on the fact that victims would find it easier to part with a relatively small sum of money rather than contact an antivirus company or a law enforcement agency.

Success clearly spurred the blackmailer (or blackmailers) to repeat the crime. According to Russian law, the police cannot open a case until a victim files an official complaint. Unfortunately, most victims are either unaware of this or have personal reasons for concealing their plight. A great shame, as this means that cyber criminals such as the author of Gpcode continue to go unpunished.

Protect your data

I think that a computer which is connected to the Internet is rather like sex – it can be safe, or it can be unsafe.
Eugene Kaspersky "The contemporary antivirus industry and its problems"

One of the most surprising aspects of the Gpcode story is that a large percentage of the victims who contacted Kaspersky Lab during the June attacks had Kaspersky Anti-Virus installed. It's surprising because Kaspersky Anti-Virus blocks the attacks 3 times. First, the infected attachment is detected as Trojan-Dropper.MSWord.Tored.a. Next, the downloader that loaded Gpcode was detected as Trojan-Downloader.Win32.Small.crb. Finally, Gpcode itself was detected. Even users whose antivirus databases were not up to date should have been protected, as detection for most Gpcode modifications has been available since January 2006.

Obviously, the victims had either turned their antivirus solution off, or chose to ignore the warnings it showed. Kaspersky Lab virus analysts did issue decryption and disinfection along with antivirus database updates. We even created special tools for restoring mail databases which were damaged when mail clients were unable to recognize the format of encrypted files. However, some users did lose critical data.

In the course of the past few years, antivirus companies have come across other malicious code which is used to blackmail users. Two examples are Cryzip and MayArchive, which in 2006 infected users in the USA and Great Britain. Both these programs archive files using an unknown password, and cracking the password is as difficult as cracking Gpcode's encryption algorithms.

These programs demonstrate that using malicious code to blackmail users is not a purely Russian phenomenon. They also demonstrate that it's essential to back up your data regularly. Why make life easy for cyber criminals?

The history of Gpcode highlights several points. Firstly, you never know where the next threat is coming from or what it will do to your computer. Secondly, under no circumstances should money be paid to the author of such malicious programs; users should contact an antivirus company instead, which will be able to help. And finally, although it might be boring, and it might slow your computer down a fraction, antivirus protection, regularly updated, is a must if you care about your data.

- Gpcode
- Ransomware

Blackmailer: the story of Gpcode

Your email address will not be published. Required fields are marked *