Root Level Resources presents a two-part article, inviting you to review the key causes and stages of development of the ransomware industry, the detailed insights of some affiliate programs, and the analysis of the most attacked countries and industries in the world.

CYBER EMPIRE OF CRYPTO RANSOMWARE

Part 1

We believe that an analysis of the development of the cyber empire will make it possible to assess the background of the situation that businesses worldwide are facing today, losing millions of dollars due to cryptographic attacks. In order to get a sense of how cybercrime shifted from sophisticated targeted attacks to non-targeted ransomware affiliate programs, we need to examine the evolution of such service.

First of all, we should make clear what the terms "crypto ransomware" or "ransomware" mean:

The main feature of this type of malware activity is blocking access to a system or files and demanding a ransom to restore access. The very idea of a ransom demand is inspired by the famous DDoS attacks that were extremely popular in the early 2000s. Back then the attackers used to send letters threatening a DDoS attack and demanding a ransom to prevent such an attack from happening. Such blackmail generated quite a good income: businesses were not ready either for downtime or to repel such attacks. However, the commercial potential of such incidents has decreased with the emergence of various CDN services featuring integrated DDoS protection options. Therefore, criminals had to find new ways of extortion attacks.

Actually, the ransomware class has traditionally been divided into two subtypes:

Locker Ransomware

The goal is to block access to the device itself, for example, to deny a victim access to MS Windows without entering an additional password.

Crypto Ransomware

The goal is to find and encrypt valuable data found on the victim's device.

An interesting fact is that the ransomware market evolved from crypto ransomware, then switching to lockers, and now back to crypto malware again.

In our report below, you can trace this chain:

Key trends

- The first **Data Leak Site** (hereinafter referred to as DLS) with false attack data appeared.
- Approximately **30%** of companies accept the terms and pay the ransom.
- The leading victim countries are still the **U.S.** (49.2%), **Canada** (5.6%), and **France** (5.2%), which replaced the U.K.
- By far the most monetized industries are under attack, namely: **Manufacturing** (9.6%), **Real Estate** (9.5%), and **Transportation** (8.2%).
- The new top three ransomware groups are Conti (16.5%), Lockbit (11.5%), and Avaddon (7.5%). Please note that last year's leader, the **Maze** group, has ceased to exist.
- DLS posts data on only **10%** of the companies under attack.
- The number of new affiliate programs increased by **23%**.
- The number of DLSs to be uploaded from encrypted networks has increased by **115%**.
- The number of victims at DLS has increased by **935%**.
- Most affiliate programs **(87%)** switch to private work, but it is still possible to join them if you know the offenders personally.
- The ransom will not prevent data leaks, as many attackers delete company data from DLS, but compromised files are still available through links.

RANSOMWARE-AS-A-SERVISE market outlook (hereafter referred to as RaaS)

Following the ban, the RAMP forum, where extortionist activity was allowed, appeared on the underground forums of public affiliate programs. This suggests that the number of new affiliate programs persists.

The risk of selling compromised companies on DLS remains high. Such malicious activity used to be widespread but has not yet become a trend.

We presume that the main industries to be attacked will not change, since the attackers consider them to be the most monetizable.

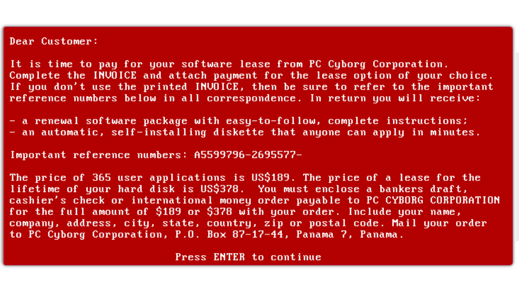
The number of compromised company data published on the public resources of ransomware operators will increase. The number of DLSs will also grow.

History of the emergence of a new criminal world and RAAS market development 1989–2021

Date	Event
01.1989	AIDS Trojan
04.2004	The emergence of the first well-known Krotten OS locker
12.2004	The emergence of the first pseudo-modern PGPcoder crypto ransomware
03.2006	Emergence of the first quasi-modern crypto-ransomware PGPcoder
06.2006	The first guides on writing crypto ransomware in the underground
05.2009	The first appearance of the Winlocker locker on underground forums
06.2009	A surge in sales of various lockers on the forums
07.2009	The emergence of articles on locker development in the underground
01.2010	The emergence of the first locker affiliate programs
12.2010	Return of crypto ransomware, free access publication of Encoder builder
07.2011	Sales of the improved Encoder
01.2012	The appearance of lockers with MBR overwrite function
09.2012	The start of a series of crypto-ransomware attacks in Australia
06.2013	The first crypto-ransomware affiliate program
09.2013	Affiliate program and the first Cryptolocker attacks
12.2013	Famous users of the underground report that the trend for lockers is dead, and the era of crypto lockers has come
01.2014	The emergence of many new crypto lockers and affiliate programs
05.2015	The appearance of the public crypto locker Tox Ransomware
11.2015	Chimera crypto ransomware attack only legal companies and threaten to release data
11.2015	The emergence of the first crypto ransomware for Linux Linux.Encoder
12.2015	There are many threads on underground forums where attackers discuss the need to attack only legal entities
02.2016	Launch of one of the most famous and largest affiliate programs Cerber Ransomware
03.2016	The emergence of the first crypto ransomware for MAC OS KeRanger
03.2016	The emergence of the famous Petya crypto ransomware with MBR overwriting
11.2016	Some ransomware programs start using Telegram as C&C
05.2017	Start of ransomware attacks with WannaCry autodistribution function
06.2017	The emergence of the NotPetya ransomware, which continued the activity of WannaCry
01.2018	The emergence of the first modern ransomware affiliate program targeting legal entities, GandCrab
03.2019	The emergence of the first RaaS with the double extorsion Snatch technique
05.2019	The emergence of the Maze ransomware
12.2019	The emergence of the first DLS (maze)
06.2020	A surge of new RaaS affiliate programs
05.2021	"No more ransom!" - banning RaaS publications on the forums
07.2021	The emergence of Ramp - a forum for Ransomware

The very first "proto crypto ransomware" resembling modern methods was **AIDS Trojan**, which spread on floppy disks or via CDs back in 1989 and ransomed money from users using social engineering. Back then it was more like a low-level scam and, of course, that Trojan could not encrypt data, while its authors had no idea of other monetization methods other than simple fraud. Meanwhile, it will be another three decades before the first DLS - sites publishing data of victims who refused to pay the ransom - appear, while the first RaaS affiliate programs are about twenty years away.

Recall that AIDS, also known as Aids Info Disk or PC Cyborg Trojan, started to extort money from users, referring to some license agreement of a non-existent PC Cyborg Corporation, which must be paid, otherwise AIDS will hide directories and encrypt the names of all files on C drive. It looked like this:



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                         Press ENTER to continue
```

2004 – 2008

One of the most relatively modern encryption tools appeared at the end of 2004. It was then that users complained on many IT resources that they "caught" some malware encrypting their files using the CRZ algorithm. Each of the victims had a special text file generated on their device, which is now commonly referred to as a Ransom Note. Simply put, it was a "message" informing them that the data was encrypted and that in order to decrypt it, they would need to contact certain email addresses. Once they had done this, the users got a link to a website where they could buy a decoder. At the beginning of each encrypted file there was a PGPcoder signature, thanks to which the first crypto ransomware got its name. **PGPcoder** was distributed via mailing lists in .doc format with malicious macros, but by 2006 the developer had improved the encryption algorithm and switched to RSA.

PGPcoder is considered to be the originator of the first wave of crypto-ransomware Trojans, which lasted from 2004 to 2008. However, PGPcoder failed to become widespread, because it was aimed solely at individuals and overloaded low-performance computers, making it easy enough to detect its activity.

A new malware called **Cryzip** appeared in March 2006. It used simple logic to encrypt files: it archived files into a password-protected ZIP archive and deleted the original. This malware contained a text file about the ransomware in English. To unzip the files, a password was required, which could be obtained by paying a ransom. E-Gold was used as the payment system. After the success of the Cryzip attacks, this ransomware scheme became popular. Cryzip was even called a new generation of Trojans.

Such a great interest in the Cryzip ZIP Trojan led to a similar VPO, **Archiveus (aka MayArchive)**, which used RSA-1024 to encrypt files. One of the most difficult moments of such malware was to get the money (since there was no BTC yet). It is believed that this malware was distributed in private communities, or there was only one criminal group involved in its development and distribution, since no information about its sale appeared on IT resources.

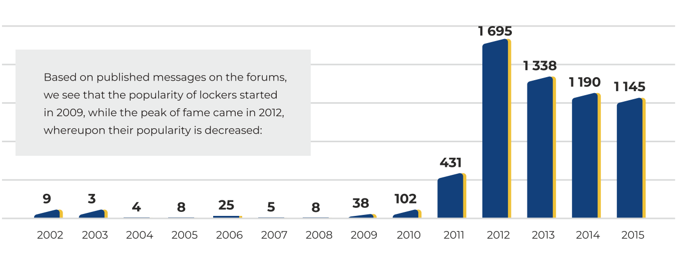
The period of locker ransomware and the emergence of affiliate programs

2009 – 2012

After PGPcoder, another well-known Trojan appeared in 2005, **Krotten**, which used a very different ransomware scheme. Instead of encrypting files, it edited the registry, making it impossible for the system to function normally (blocking the operation of the operating system, after which it displayed a message demanding a ransom). This Trojan belongs to the locker type of ransomware.

The same scheme was followed by **SMS Lockers Trojans**. Their most famous representative was a Trojan named **Winlock (aka winlocker)**. Prior to the spread of this VPO, Winlock Pro was popular among users, blocking access to the operating system after a certain period. Many varieties of such Trojans had already appeared by 2009 but their idea did not change.

Winlock was the first malware to be sold and distributed on underground forums in May 2009, causing an enormous explosion of attacks involving it. Moreover, Winlocker was the one who started developing the first ransomware affiliate programs. One of the first locker affiliate programs appeared in January 2010. Its basic idea was to provide an affiliate member with a Trojan, which he had to distribute among users and get a percentage of the profit for unlocking it, or, more precisely, for sending SMS.



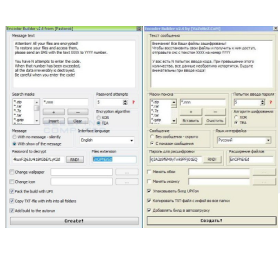
Based on published messages on the forums, we see that the popularity of lockers started in 2009, while the peak of fame came in 2012, whereupon their popularity is decreased:

Persistent Locker Dominance and the First Modern Crypto Ransomware

2011 – 2013

Just as the popularity of Winlockers waned, Trojans returned to the forums, allowing users to encrypt their data and demand a ransom. Thus, the era of crypto ransomware began.

The first known Trojan based on this scheme appeared at the end of 2010 – **Encoder (aka xorist)**. Its author posted not only the source code of the malware, but also the builder, which allowed users to automatically generate malicious samples with their own settings:



Encoder Builder v2.4 from [Pastorok]

Attention! All your files are encrypted!
To restore your files and access them, please send an SMS with the text XXXX to YYYY number.

You have N attempts to enter the code. When that number has been exceeded, all the data irreversibly is destroyed. Be careful when you enter the code!

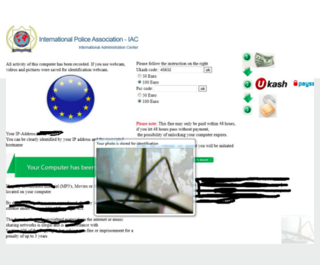
Внимание! Все Ваши файлы зашифрованы!
Чтобы восстановить свои файлы и получить к ним доступ, отправьте смс с текстом XXXX на номер YYYY

У вас есть N попыток ввода кода. При превышении этого количества, все данные необратимо испортятся. Будьте внимательны при вводе кода!

However, the attackers who tested the software found its conversion rate too low. The problem was that the victims didn't understand what happened and how to work with the decoder.

At first, lockers and crypto ransomware were highly unpopular, as this type of software was considered to attract too much attention, while the ransomware scheme was still an ongoing issue. Judging by the messages on the forums, cybercriminals continued to show an interest in Winlockers because they were easier to monetize, including via affiliate programs. Attackers started using Ukash and Paysafecard vouchers to accept payments.

In July 2012, a new **Ulocker** locker appeared. According to the description, it worked in the following countries: Austria, Cyprus, Finland, France, Germany, Greece, Italy, Netherlands, Poland, Portugal, Romania, Spain, Sweden, and Switzerland. Furthermore, the Ulocker had very advanced landings, which allowed displaying images from a web-camera intercepted by malware:



International Police Association - IAC

International Administration Center

All activity of this computer has been recorded. If you use webcam, videos and pictures were saved for identification webcam.

Your IP-Address [redacted]

Please follow the instruction on the right

Ukash code: 45632

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

Your photo is stored for identification

Somewhat later, some lockers started using a new tactic: they overwrote the Master Boot Record (MBR), causing the user to not even be able to start the OS.

At the same time, another famous **Reveton** locker appeared, which blocked the OS and demanded to pay a fine. The linking was in the form of a demand from the U.S. Department of Justice and was distributed through the famous **Citadel** malware.

The old **GPCode** crypto ransomware has also continued to evolve, but its victims were still regular individuals.

By the end of 2012, four Australian companies had fallen victim to crypto ransomware attacks:

TDC Refrigeration and Electrical
September 2012
Ransom amount **3 000**
Industry Manufacturing

Byron Community Primary School
October 2012
Ransom amount **5 000**
Industry Education

Deanes Buslines
November 2012
Ransom amount **3 000**
Industry Transportation services

Gold Coast medical centre
December 2012
Ransom amount **4 000**
Industry Health Care

The criminals demanded extremely small amounts of money to decrypt the data. However, it became clear that attacks on businesses could be much more effective than those on individuals. Time to switch to crypto lockers arrived.

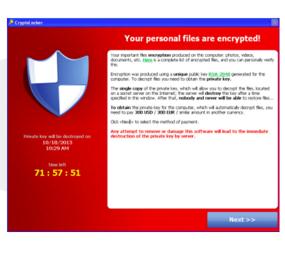
The first crypto affiliate programs

2012 – 2014

One of the first affiliate locker programs involving file encryption appeared in June 2013. Such a locker encrypted files using the RSA1024 algorithm, and the developers worked on a 50/50 scheme. Unfortunately, no names or reviews for this affiliate program were found.

But as soon as September 2013, one of the most famous encryption tools named **CryptoLocker** (the campaign for its distribution was launched on 05.09.2013). Today its name has become a stable term and is used for any malware of this type, but previously they were called either "lockers" or "crypto ransomware" as well as "ransomware".

After infection the Trojan window looked like this:



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

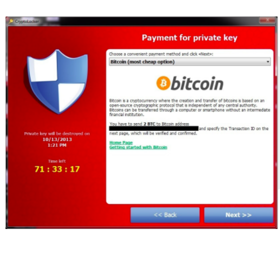
Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on 10/18/2013 10:29 AM

Time left 71 : 57 : 51

Once you continue, it suggested ways to pay:



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send 2 BTC to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page

Getting started with Bitcoin

Private key will be destroyed on 10/13/2013 1:21 PM

Time left 71 : 33 : 17

The Cryptolocker was one of the first coders that infected a huge number of victims in an extremely short period of time. According to the researchers, by mid-December 2013 (within 3 months) more than 200,000 computers had been infected. In May 2014 this encryption tool was isolated during the Tovar operation. At that time, access was gained to the secret keys for encryption and special software was released to decrypt files without payment. The affiliate program participants are believed to have earned about $3,000,000 over the entire time.

Development of RaaS line of business, change of focus on business, the threat of publishing files

2014 – 2016

The popularity and effectiveness of Cryptolocker contributed to the fact that in 2013-2014 the number of attackers who sell various versions of malware with file encryption functionality increased:

December 2013
PowerLocker

January 2014
File encoder

February 2014
TorrentLocker
Tor Locker

May 2014
Obertone

June 2014
CryptvouFiles
CTB-Locker
Gates of Cerberus

July 2014
Exaction
Cryptolocker

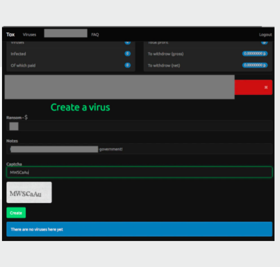
August 2014
RSA Locker

November 2014
Coinvault

The famous crypto ransomware **VaultCrypt** started its activity in February 2015. And already in March 2015 a full-fledged affiliate program was launched for this crypto ransomware.

TorrentLocker was recognized as the most widespread crypto locker in 2014. At the end of 2014, its owners earned about $500,000.

Separately, we should note the emergence in May 2015 of the affiliate program **Tox Ransomware**, which offered an online builder for malware, available on a particular site in .onion and looked like this:

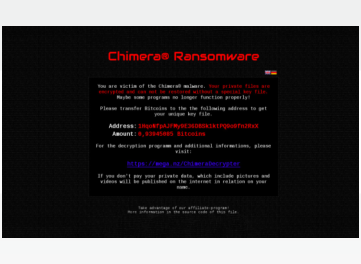


So, any user could generate a crypto ransomware sample, specify an amount of money to decrypt it, and use it to make profits.

One of the major encryption attacks took place in May 2015: computers of the Vietnamese Ministry of Justice were infected. The ransom amount was not specified. Meanwhile, in October 2015, there was an attack on a school network in New Jersey, and here the attackers demanded about $124,000, which is beginning to resemble the current rates of known ransomware attack groups.

Moreover, in October 2015, users complained that their Windows Server servers had fallen victim to a certain **LowLevel04** malware. At the time, it became apparent that some criminal groups were beginning to use advanced attack tactics. In this case it was about brute-force attacks on RDP. Since then, the victims of encryption attacks include more and more legal entities.

The famous **Chimera** crypto ransomware tool appeared in November 2015. It had two distinctive features: it attacked only legal entities and threatened victims with the publication of encrypted data in the public domain.



Chimera® Ransomware

```
You are victim of the Chimera® malware. Your private files are
encrypted and can not be restored without a special key-file.
Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get
your unique key file.

Address: 1HqoNfpAJFMy9E36DBSk1ktPQ9o0fn2RxX
 Amount: 0,93945085 Bitcoins

For the decryption programs and additional informations, please
visit:

https://mega.nz/ChimeraDecrypter

If you don't pay your private data, which include pictures and
videos will be published on the internet in relation on your
name.

Take advantage of our affiliate-program!
More information in the source code of this file.
```

The attackers didn't fulfill the threat and didn't release the data, but this technique was later adopted by all modern groups of ransomware operators.

In November 2015, the **Linux.Encoder** crypto ransomware appeared, targeting Linux-run systems that are mostly owned by companies rather than individuals.

However, the most famous crypto ransomware in 2015 was a malware attack called **CryptoWall**. It was first discovered back in the spring of 2014. Experts estimate that in 2014 the attackers earned $18,000,000, and in 2015 they already earned $325,000,000. Judging by the use of the same Bitcoin wallets, it is assumed that they had no public affiliate program, and one criminal group was responsible for the program.

Thus, 2015 marks a turning point in the development of crypto-attacks - the focus of cybercriminals is increasingly shifting toward businesses. Financially motivated groups start to realize that it is much more profitable to attack legal entities.

Ransomware popularization, Wannacry

2016 – 2018

As mentioned above, at the end of 2015, attackers switched to attacking companies. Criminals started "collecting" emails from various corporations and government agencies to conduct attacks. We won't cover every new crypto ransomware in detail below, focusing only on the most interesting events that have occurred over the years and influenced the development of the ransomware cyber empire as a whole.

One of the most famous and major crypto affiliate programs at the time, **Cerber Ransomware** was launched on February 24, 2016, and in July 2016 it became the most widespread ransomware. To decrypt the data, it was required to pay $500 on a site hosted on the Tor network.

The first full-fledged encryptor for Mac OS X called **KeRanger** was detected in March 2016. In order to distribute it, the resource of the famous Transmission program was hacked and replaced with its own copy.

At the end of March 2016, the **Petya** Trojan appeared. Besides encryption, it overwrote the Master Boot Record (MBR), causing the user to fail to start the operating system (a similar technique was used by common lockers in 2012). Somewhat later, **Mischa**, one of the most widely used lockers, started to spread, encrypting files without the MBR when rights were insufficient.

In July 2016 the same technique was used by another crypto ransomware - **Satana**.

The **ZCryptor** crypto ransomware appeared in May 2016. It had a new technique typical for classic viruses, namely, self-distribution to various devices.

In November 2016, crypto ransomware that used the Telegram messenger as a control server for their Trojans appeared. The encoder contained the bot's API key in Telegram and reported infections and other actions to specific channels or directly to attackers.

This technique is now very commonly used in steelers.

CTB-Locker, Locky, and TeslaCrypt were the most common crypto ransomware in 2016.

On 12.05.2017, users started to complain on underground forums that their files were encrypted by a new encryption tool that changes the extension to WNCRY. In a short time, about half a million devices were encrypted with this malware. The main reason for such a rapid spread was that the Trojan had the ability to self-propagate using the **EternalBlue** exploit and the subsequent installation of the **DoublePulsar** backdoor. This story showed attackers that it was possible to exploit known vulnerabilities to spread malware en masse. Therefore, a little later, on June 27, 2017, another crypto-cracker **NotPetya** used the same vulnerability for its attacks.

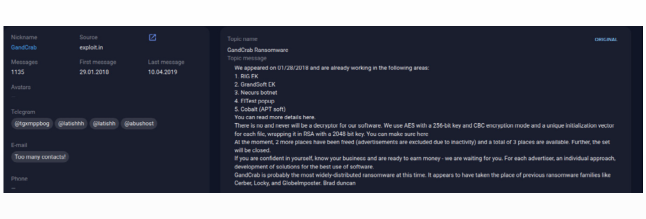
Emergence of Modern RaaS Trends: GandCrab

2018 – 2019

In January 2018, one of the most famous affiliate programs, **GandCrab**, appears. The **REvil** group used the source codes of this very malware to develop their Trojan.

This affiliate program has served as the progenitor of almost all the major trends that are still in use today.

GandCrab described in detail how to attack its victims and pointed out a very popular method with the Cobalt Strike framework at the moment.



Nickname: GandCrab
Source: exploit.in
Messages: 1135
First message: 29.01.2018
Last message: 10.04.2019
Avatars: –
Telegram: @tgxmppbog @latishhh @latishh @abushost
E-mail: Too many contacts!
Phone: –

Topic name: GandCrab Ransomware

Topic message:

We appeared on 01/28/2018 and are already working in the following areas:
1. RIG EK
2. GrandSoft EK
3. Necurs botnet
4. EITest popup
5. Cobalt (APT soft)
You can read more details here.
There is no and never will be a decryptor for our software. We use AES with a 256-bit key and CBC encryption mode and a unique initialization vector for each file, wrapping it in RSA with a 2048 bit key. You can make sure here
At the moment, 2 more places have been freed (advertisements are excluded due to inactivity) and a total of 3 places are available. Further, the set will be closed.
If you are confident in yourself, know your business and are ready to earn money - we are waiting for you. For each advertiser, an individual approach, development of solutions for the best use of software.
GandCrab is probably the most widely-distributed ransomware at this time. It appears to have taken the place of previous ransomware families like Cerber, Locky, and GlobeImposter. Brad duncan

So, they started recruiting teams of special partners who specialize in big targets. It was this affiliate program that became the ancestor of **Big Game Hunting**.

On February 28, 2018, the GandCrab web panel was hacked, causing a loss of about a quarter of their private keys. But already on March 07, 2018, they are restarting the affiliate program and now keep the keys on a server separate from the admin panel.

This affiliate program differed from the others by constantly improving the VPO and looking for new technologies to increase the conversion of downloads into payments from customers (they were the first, back in February 2018, who introduced payment acceptance in the cryptocurrency DASH), and thoughtful work with partners. They examined in detail different methods of getting access to the network. In addition to the standard **Cobalt Strike** and **MSF** frameworks, they used applications that allow the use of social engineering as a primary attack vector.

For example, **Mephistophilus**, a system for targeted phishing attacks. GandCrab was also the first to officially announce that they were contracting Recovery companies for data recovery.

In April 2018, they once again created a new trend - buying up access to dedicated servers to further develop an attack to gain full control of the company's internal network.

According to GandCrab's 2018 statistics about its partners:

In April, their weekly turnover was over $100,000

In May, some of them earned between $100,000 and $200,000

315,365 computers were infected in June

During July 2018, they signed 210 contracts with data recovery companies around the world. That same month, a new version of GandCrab came out that had automatic encryption of network drives, which was later used in another crypto ransomware. Since one of the very first Initial Access Brokers left the public access market, the forums have been flooded with new offers to sell access. GandCrab was the first group to start steadily buying up accesses from such users..

In August 2018, GandCrab changed the logic of accepting new partners - now an interview is required to participate in the program. Similar practices will then be adopted by other cybercriminals. Based on reports from this criminal group, they used Fallout as a bundle of exploits to gain access.

In September 2018, another GandCrab update comes out, bringing their monthly revenue to more than $1 million. Of the groundbreaking features, the following should be highlighted:

- The administrative panel of the new version has a **PowerShell** script builder, which allowed to load the payload, bypassing the anti-virus systems
- Now the encrypted files had a dynamic extension (they change from device to device)
- GandCrab started working directly with **NTCrypt** crypto service

In another October update, the developers decided to implement **Mimikatz** to automate the collection of credentials. And they also openly declared a fight against other encryptors: they considered it unacceptable to encrypt victims twice.

On October 17, 2018, attackers provided Syrian citizens with a free decryptor. As a result, on October 27, 2018, the anti-virus companies managed to get the master key by analyzing the generated keys and make a universal decryptor. Consequently, on October 28, 2018, the attackers made a new master key and began to switch to a new encryption scheme, which did not depend on it.

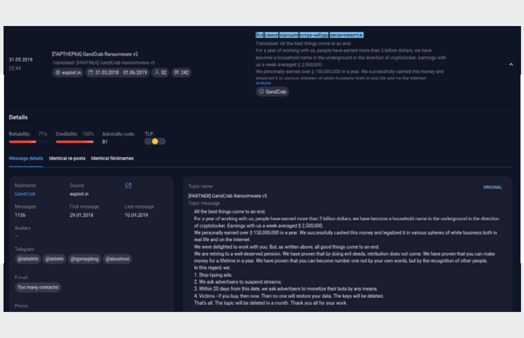
The update of October 31, 218 introduced the feature of scanning RDP and RDP brute force inside the network using passwords, which got to Mimikatz.

In January 2019, GandCrab launched a new service to monetize other users' access. That is, they start buying up RDP or VPN access and offer sellers to sell it for a percentage or buyout.

In February 2019, there was another attack on GandCrab servers, which again managed to get the secret keys, leading to another decryptor.

May 31, 2019, GandCrab suddenly stepped down from the market.

In its latest message, the owner of GandCrab asked to delete his accounts and everything associated with him.



31.05.2019 22:44

[ПАРТНЕРКА] GandCrab Ransomware v5

Translated: [PARTNER] GandCrab Ransomware v5

exploit.in · 31.03.2018 - 01.06.2019 · 82 · 242

Все самое хорошее когда-нибудь заканчивается

Details

Reliability: 71% · Credibility: 100% · Admiralty code: B1 · TLP:

Nickname: GandCrab
Source: exploit.in
Messages: 1135
First message: 29.01.2018
Last message: 10.04.2019
Avatars: –
Telegram: @latishhh @latishh @tgxmppbog @abushost
E-mail: Too many contacts!

Topic name: [PARTNER] GandCrab Ransomware v5

Topic message:

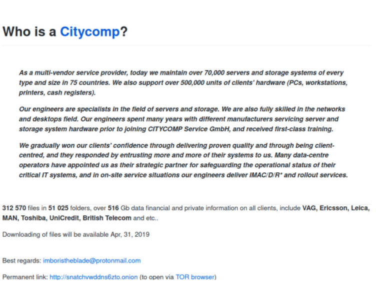
All the best things come to an end.
For a year of working with us, people have earned more than 2 billion dollars, we have become a household name in the underground in the direction of cryptolocker. Earnings with us a week averaged $ 2,500,000.
We personally earned over $ 150,000,000 in a year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.
We were delighted to work with you. But, as written above, all good things come to an end.
We are retiring to a well-deserved pension. We have proven that by doing evil deeds, retribution does not come. We have proven that you can make money for a lifetime in a year. We have proven that you can become number one not by your own words, but by the recognition of other people.
In this regard, we:
1. Stop typing ads;
2. We ask advertisers to suspend streams;
3. Within 20 days from this date, we ask advertisers to monetize their bots by any means;
4. Victims - if you buy, then now. Then no one will restore your data. The keys will be deleted.
That's all. The topic will be deleted in a month. Thank you all for your work.

Current trends: double extortion, the emergence of DLS, a ban on affiliate programs

2019 – 2022

In March 2019, a new **Ransomware Snatch** affiliate program was advertised on the exploit.in forum. Its distinctive feature was that it did not work with traffic and downloads but focused exclusively on attacks on corporate networks.

On April 28, 2019, a user nicknamed Truniger published an interesting post on the exploit.in forum, where it reports that Citycomp's network has been hacked and encrypted, and all the data has been uploaded. He claimed that the company refused to pay money for the decryption, so a certain group decided to put their data in the public domain:



Who is a Citycomp?

As a multi-vendor service provider, today we maintain over 70,000 servers and storage systems of every type and size in 75 countries. We also support over 500,000 units of clients' hardware (PCs, workstations, printers, cash registers).

Our engineers are specialists in the field of servers and storage. We are also fully skilled in the networks and desktops field. Our engineers spent many years with different manufacturers servicing server and storage system hardware prior to joining CITYCOMP Service GmbH, and received first-class training.

We gradually won our clients' confidence through delivering proven quality and through being client-centred, and they responded by entrusting more and more of their systems to us. Many data-centre operators have appointed us as their strategic partner for safeguarding the operational status of their critical IT systems, and in on-site service situations our engineers deliver IMAC/D/R and rollout services.*

312 570 files in **51 025** folders, over **516** Gb data financial and private information on all clients, include **VAG, Ericsson, Leica, MAN, Toshiba, UniCredit, British Telecom** and etc..

Downloading of files will be available Apr, 31, 2019

Best regards: imboristheblade@protonmail.com

Permanent link: http://snatchvwddns6zto.onion (to open via TOR browser)

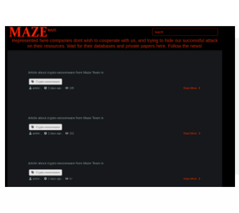
As we can see, there was also the .onion domain where they were going to store the leak in the future - snatchvwddns6zto.onion. While discussing this leak, the author of the post clarified that the data was to be published in the event of the company's decline.

Apparently Truniger previously worked for GandCrab and was involved in getting access to networks (then working for the **Snatch** affiliate program). Subsequently, the domain snatchvwddns6zto.onion was used to publish data about companies that refused to pay. This was the first time a ransomware group decided to put double pressure on a victim. However, other groups did not immediately adopt this technique.

A new crypto malware, which was distributed through the Fallout exploit kit, originally named **ChaCha** (after the encryption algorithm) appeared in May 2019. Previously, it was also used by GandCrab. In June 2019, the operators of this malware called it **Maze**. However, the most interesting thing happened in November 2019, when the criminal group registered an account on the underground forum xss.is and left a message about hacking and encrypting **Allied Universal**'s data. The latter contacted them but refused to pay them even after they provided proof. After that, the attackers decided to upload 10% of the obtained data to the public domain on an underground forum. In the same post, they said that they would pass the remaining 90% to Wikileaks if the company did not pay them. They also warned other companies that this would happen to anyone who refused to pay.

In December 2019, Maze realized that the best way to apply such pressure would be to create their own **Data Leak Site (DLS)**, where they would publish data from companies that refused to cooperate. As a result, they registered the domain mazenews.top on December 09, 2019, which Maze uses to publish leaks.

The first leak publications appeared there on December 15, 2019:



Represented here companies dont wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!

Most of the known ransomware groups have adopted the tactics of the Maze and Snatch criminal groups.

The latest significant event in the development of RaaS occurred in May 2021. Due to the large attacks of various groups, especially the **REvil** group, the forum owners decided to prohibit the distribution of affiliate programs on underground forums. The reason, according to them, is that it draws too much attention to the actions of other hackers.

The next day another large underground forum exploit.in joined the movement "No more ransom! However, this didn't stop the attackers, and in July 2021, the **Babuk** group's DLS page advertised a new forum called RAMP, whose main goal is to create a new site for advertising ransomware affiliate programs, instead of the compromised companies' data. This platform worked, and such programs as **Lockbit v.2**, **Avos**, **Caodabi Locker**, **RTM**, and **Hive** quickly appeared there.

The term Ransomware became synonymous with cyber ransomware online. In fact, it formed the technological backbone of a large-scale illicit industry, and its ransomware attacks turned into a major threat to the public and commercial sectors worldwide.

Ransomware operators and their affiliate programs make millions of dollars, damaging companies all over the world. This brought thousands of attackers involved in network hacking, traffic hacking, downloading, malware development, and targeted attacks into a giant new niche of the cybercriminal world.

This is how the cyber empire of cryptographers emerged.