

# ‘Locked Out’

PUBLICATIONS

12 MAR 2015

minute read

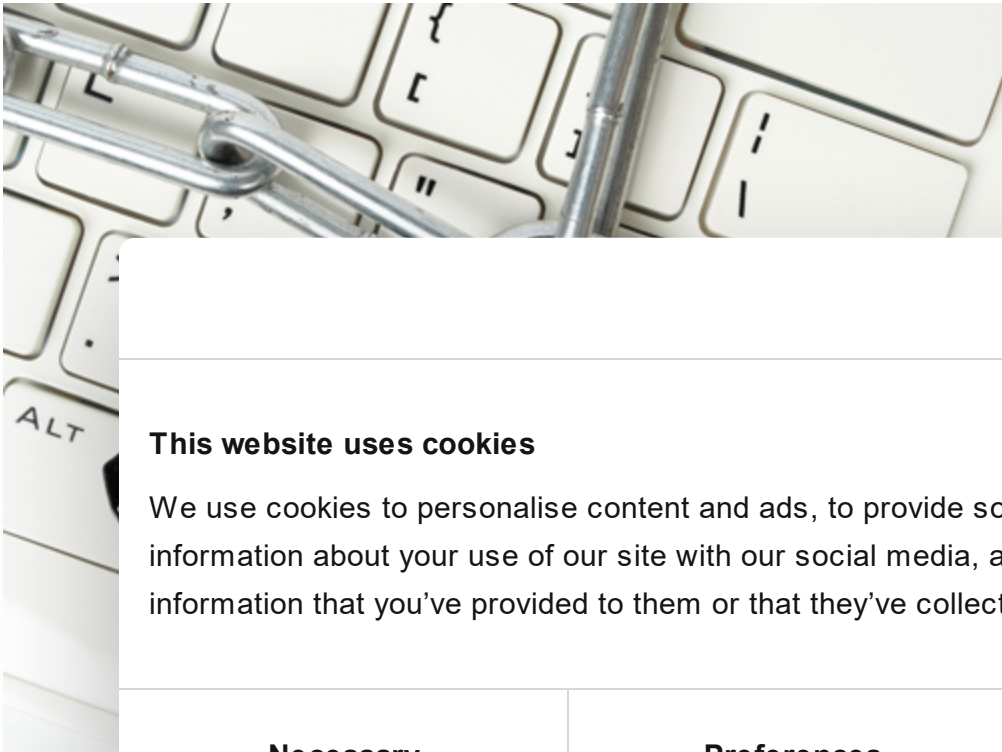


Table of Contents

[The evolution of encrypters: from simple to complex](#)

**Cookiebot**  
by Usercentrics

## This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details

Use necessary cookies only

Allow all cookies

// AU

Expert

ART

## The e

Today the world is full of threats. Cyberattacks are often used as a tool for espionage, sabotage, or even terrorism. Kaspersky Lab classes such programs as Trojan-Ransom malware, although there is another widely used and resonant name – **encrypters**.

Encrypters have become a serious problem for users, especially corporate users. And related topics attract the most posts and readers on our forum.

Despite all the efforts of the anti-virus companies we don’t expect an easy victory over encrypters in the short term. There are at least two good reasons for this:

- 1 Encrypters are constantly evolving. It is a battle of arms and armour: the defence gets better – the weapons get better.
- 2 The attack is not carried out on the **user’s computer** but on the system of **computer + user**. That is, one of the attack vectors is human. A person is subject to emotions and irrational acts. A person is capable of ignoring the warnings of the defence systems or turning it off altogether. This is precisely what the evildoers are counting on.

In this article we look at the evolution of complication of the encryption schemes used by virus writers and the methods they adopt to put pressure on their victims. At the end of the article there is some advice for users which might help them protect important files.

**To the aid of the bad guys: the human factor**

**Traps for the unwary: how users are attacked**

RDP attack

Attack via electronic mail

Letter topics

The thing about filenames

**Recommendations for users**

## The evolution of encrypters: from simple to complex

Serious antivirus companies devote special attention to protection against encrypters. To counter the improved systems of defence virus writers need to change their programs regularly. And they change almost everything: the encryption schemes, means of obfuscation and even the formats of executable files.

## Virus writers change the encryption schemes, means of obfuscation and even the formats of executable files



We will consider the evolution of encryptions in terms of the methods of encryption and cypher schemes employed. Depending on the cypher scheme used and the method of obtaining the key, in some cases it is possible to easily decypher the encrypted data and in others it is impossible to do so within a reasonable time.

## Encryption with an XOR operation

We begin with programs that use the most primitive encryption. A typical example of such malware is the Trojan-Ransom.Win32.Xorist family. It has the following characteristics:

- XOR is used to generate a stream cipher when the key is a stream of bits
- An XOR operation can be used to generate a stream cipher head and an initial value
- To compute the output of the stream cipher, the input is XORed with the stream

A screenshot of a Cookiebot consent banner. The banner has a white background with a thin grey border. At the top right is the "Cookiebot by Usercentrics" logo. Below it, the heading "This website uses cookies" is followed by a paragraph explaining cookie usage. A row of four toggle switches allows users to manage different types of cookies: Necessary (on), Preferences (off), Statistics (off), and Marketing (off). Each toggle switch is accompanied by its category name. At the bottom right, there is a link labeled "Show details" with a chevron icon.

**Fragment of a file encrypted by an encrypter of the Xorist family: the eight byte key is clearly visible**

On the whole, despite all the cunning of the creators of Xorist the files encrypted by it can be entirely decrypted relatively easily. Maybe for that reason at the moment the Xorist family of malware is hardly ever encountered in the wild.

To combat Trojan-Ransom.Win32.Xorist the specialists of Kaspersky Lab created the utility [XoristDecryptor](#).

# Symmetrical Encryption

A symmetrical encryption scheme is a scheme that uses a pair of keys for encryption and decryption that are symmetrical to each other (this is why this scheme is called symmetrical). In the great majority of cases in such schemes one and the same key is used for encryption and decryption.

If the key is embedded in the body of the encrypter, if one has access to the body of the malware it is possible to extract the key and create an effective utility to decrypt the files.

Such malware usually tries to delete itself after encrypting the files. An example of this type of program could be one of the modifications of the Rakhni family. Keys that were detected were added to the utility [RakhniDecryptor](#).

If the key is recieved from the attacker's server or generated and sent to it then having an example of the malware yields little — an example of the key is necessary, and it is on the attacker's server. If it is possible to recover the key (for obvious reasons the malware tries to delete such key after use) then it is possible to create a utility for decryption. In this case a system that caches the internet traffic of the user may be useful. An example of this type of malware is Trojan-Ransom.Win32.Cryakl.

## Assymetric encryption

Assymetric encryption is the name given to those schemes in which the encryption and decryption keys are not related in an obvious symmetrical way. The encrytion key is called the open or public key and the decryption key is the secret or private key. Calculating the private key from a known public key is a very complicated mathematical task which is not possible in a reasonable time using modern computing capabilities.

At the heart of assymetrical cypher schemes is the so-called trapdoor one-way function. Put simply this is a mathematical function that depends on a parameter (secret). Without knowing the secret parameter it is difficult to invert the function. The function is called one-way (for obvious reasons) because it is difficult to invert. The function is called trapdoor because the argument of the function is the secret parameter and the result is the output. The function is called trapdoor because the argument of the function is the secret parameter and the result is the output. The function is called trapdoor because the argument of the function is the secret parameter and the result is the output.

## Assymetric encryption

If the public key is known, the private key can be calculated. This is the case of the private key in the program. The private key is the secret parameter and the result is the output. The function is called trapdoor because the argument of the function is the secret parameter and the result is the output.

However, the private key is not known. The private key is the secret parameter and the result is the output. The function is called trapdoor because the argument of the function is the secret parameter and the result is the output.

An example of this type of malware is Trojan-Ransom.Win32.Cryakl. The private key is the secret parameter and the result is the output. The function is called trapdoor because the argument of the function is the secret parameter and the result is the output.

- Uses the private key to decrypt the file.
- To speed up the encryption of files it doesn't encrypt them all at once but in small sections. The encrypted sections are added on to the end of the file and their space is filled in with sequences with a frequency of one byte. Because of this the encrypted file gains a typical 'scratched' appearance.

- One defect of this scheme for the evildoer is that for the decryption of the files it is necessary to hand over the private key, which can be used to decypher all files encrypted by this modification of the malware.

Thus, although direct decryption of the files is impossible, several users suffering from one and the same modification of the malware can unite and buy one decoder for all of them. Also users and other interested persons send decoders to us. The private codes received are added to the [RectorDecryptor](#).

If the public key is obtained from the evildoer's server (which allows the use of a unique public key for each user) then the presence of the body of the malware doesn't help in the decryption of the data — it is necessary to have the private key. However the body of the program helps identify and block the malware server and this helps protect other users.

### Encryption using several keys

To ensure a unique decoder for each user schemes with several keys are used. For this the key for encryption of data is generated on the victim's computer. It might be a symmetric key or an assymetric key pair. The algorithm for key generation is chosen so that the resulting key is unique for each affected user. In other words the chances of these keys being the same in any two cases should be extremely small. However sometimes the malware creators make a mistake

the user have been

The user decypher earlier and private key deleted

Now, having that is not be useful improve



An example family. The Scatter family has several significant features:

- A more advanced encryption scheme is used with two pairs of assymetric keys, which allows the evildoers to encrypt the files of the victim without revealing their private key.
- Samples of this family are written in scripting languages, which allows the malicious functions to be easily changed. Scripts are easier to obfuscate and this process is easier to automate.
- The samples have a modular structure. The modules are downloaded from the wrongdoers' website during the running of the script.
- Renamed legitimate utilities are used for the encryption of files and deletion of the keys.
- A high level of automation of the process has been achieved. Almost everything is automated, the malware objects are automatically generated, letters are sent out automatically. Furthermore, according to the malefactors the process of handling letters from victims and further contact with the victims has been automated. The decyphering of test files of the victim, evaluation of the cost of the information, the provision of bills, checking payment and sending out decoders all happen automatically. It is difficult for us to check the truth of this information but taking into account data obtained from studying the modules of Trojan-Downloader.BAT.Scatter there is no reason not to believe these claims.



#### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >



Tweet

26 FEB 2021, 12:00PM

**GReAT Ideas. Green Tea Edition**

JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM

**GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots**

MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

26 AUG 2020, 2:00PM

**GReAT Ideas. Powered by SAS: threat actors advance on new fronts**

IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM

**GReAT Ideas. Powered by SAS: threat hunting and new techniques**

The Scatter family appeared quite recently: the first samples were detected by Kaspersky Lab specialists at the end of July 2014. In a short time it significantly evolved, providing itself with the functionality of Email-Worm and Trojan-PSW.

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,  
BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT,  
FABIO ASSOLINI


From 25 July 2014 to 25 January 2015 we detected 5989 attacks with the use of Trojan-Downloader.JS.Scatter on 3092 users.

staff.

| FullName   | HitsCount |
|--|-----------|
| ./draft collation act.zip// unpaid bills. Draft collation act for two months – accountancy dept agreed till 14 October 2014_mail.attachment_scanned.avast.ok.doc .js   | 4386      |
| scan copy of debts 2014.zp//unpaid bills . Draft collation act for two months – accountanct dept agreed till 14 October 2014._mail.attachment_scanned.avast.ok.doc .js | 402       |
| unpaid bills. Draft collation act for two months – accountancy dpet agreed till 14 October 2014_mail.attachment_scanned.avast.ok.doc .js                               | 241       |
| Draft collation act.zip  | 22        |

***The most popular names of the Scatter download modification appearing in the first half of October***


If a user attempts to open the attachment they start the downloader, which is an obfuscated JavaScript and is detected by Kaspersky Lab as Trojan-Downloader.JS.Scatter.i




**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.


Necessary




Preferences



Statistics



Marketing



**Frag**

After  
malef  
all of t

[Show details](#) >

- *fake.keybtc* – is a renamed version of the legitimate program gnupg gpg.exe intended for carrying out cryptographic operations.
- *night.keybtc* – is a renamed version of the library iconv.dll necessary for gpg.exe to work properly
- *trash.keybtc* – is a renamed version of the utility sdelete.exe from Microsoft designed to reliably delete files.
- *key.block* – is a malicious command script that uses the utilities above to encrypt files. This object is detected by Kaspersky Lab as Trojan-Ransom.BAT.Scatter.ab
- *doc.keybtc* – this file is in the Microsoft Word format. The downloader renames this file as word.doc and then tries to run it. If there is a program for looking at .doc files on the user’s computer the user sees the following picture:

*The beginning of the Microsoft Word document shown to the user by the downloader Trojan-Downloader.JS.Scatter.i*

This document doesn't contain any malicious code. Its task is too reduce the alertness of the user and distract his attention from the processes taking place on his/her computer.

In the work c



**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

**1. Pre**

- 1.1. Ren
- 1.2. Ch
- current
- and de
- UNIQUE
- 1.3. Ch
- later t
- 1.4. Ch
- earlier

**Necessary**



**Preferences**



**Statistics**



**Marketing**



[Show details](#) >

- in some communications infected computers and the hackers offered their victims to decypher their files in exchange for certain services and even promised money for these services. It is possible that in this way they are trying to turn the user into a partner.)
- 1.5. Generate a key pair (public and private keys: files **pubring.gpg** and **secring.gpg** **respectively**) with the parameters:  
Key-Type: RSA  
Key-Length: 1024

This type of encryption is currently considered effective: there is no algorithm to decrypt files encrypted with the algorithm RSA with a key length of 1024 bits in an acceptable time without knowing the private key.

- 1.6. Extract the public key from the body of the malware and use it to encrypt the file **secring.gpg**, the private key of the key pair, as a result obtaining the file **secring.gpg.gpg**. After that **secring.gpg** is deleted with the help of the legitimate utility sdelete.exe and its location rewritten 16 times. If for some reason it is impossible to delete the unencrypted key using sdelete the Trojan tries to delete it itself, writing over it several times with rubbish. Multiple rewriting of the location of the file is necessary so that the private key can not be recovered even using special programs for restoring deleted data.
- 1.7. Copy the encrypted private key (**secring.gpg.gpg**) under the name %TEMP%KEY.PRIVATE", which the malware tries to do twice for reliability. Then it once more

**Subscribe to our weekly e-mails**

The hottest research right in your inbox



checks the presence of KEY.PRIVATE. If it isn't there and neither is secring.gpg the Trojan doesn't carry out encryption and goes straight to distribution of its loader (item 3)

2. Encryption

2.1. Before the start of encryption the Trojan generates a script with a list of files which it will encrypt. It does this in two stages:

- First it looks for and adds to the file databin.lst the paths to files with the following extensions:  
\*.xls \*.xlsx \*.doc \*.docx \*.cdr \*.slddrw \*.dwg \*.pdf.
- Then it adds to databin.lst the paths to files with the following extensions:  
\*.mdb \*.lcd \*.accdb \*.zip \*.rar \*.max \*.cd \*.jpg.

Why does it do this? The RSA algorithm is reliable but extremely slow. Therefore the malware 'is afraid' that it might start encrypting large files or a directory with a lot of photographs and that something might interfere with it. For instance the user might switch off the computer. Therefore the Trojan first of all tries to encrypt small files that are potentially important for the organisation and then moves on to media such as disks and other large volumes of data.

Apart  
UNIQUE  
name  
value c  
maxim

Then t  
result

2.2. Th  
gener  
renam  
2.3. Th  
that th  
them v  
2.4. Th


Fragm

For s

1. Your information has been encrypted using RSA-1024 assymetric encryption, used by the military. Breaking it is impossible.  
During encryption the special ID-file KEY.PRIVATE was copied to various places on the computer. Do not lose it!  
For each computer a new ID-file is created. It is unique and contains the code for decryption. You will need this.  
'Temporarily blocked' means that the files are modified on the byte-level using a public 1024 bit RSA key.
2. And so, our further actions are as follows:
  - 2.1. You can contact us only using the email address \*\*\*\*\*@gmail.com
  - 2.2. First of all you need a guarantee that we can decypher your files.
  - 2.3. Contact us. The structure of your email should be as follows:
    - include your ID-file KEY.PRIVATE (!!)
    - 1-2 encrypted files to check the possibility of decryption
    - the approximate number of encrypted files/computers

Email(Required)

☐ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

 **Subscribe**



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

| Necessary   | Preferences   | Statistics  | Marketing   |
|---|---|---|---|
|  |  |  |  |

Show details >



2.4. You will recieve a guarantee and the cost of your key within one hour  
2.5. Next payment should be made, the minimum cost will be 150 euros  
2.6. We will send you your key, you should put it in the same directory as the decoder (DECODE.exe)  
2.7. When the decoder is started the concealed decryption of your data is carried out. You should not start this process more than once.  
2.8. The process of decryption might take up to 12 hours in stealth mode. At the end of the process the computer will reboot.

2.5. The Trojan renames bitdata1.bin (the script for the encryption of data generated earlier) as bitdata.cmd and starts it running. As a result the user’s files are encrypted and the email address of the evildoers is added to their extensions.

2.6. After successful encryption the mark BITM is added to all files UNIQUE.PRIVATE and KEY.PRIVATE

### 3. Distribution of loader by electronic mail

3.1. The Trojan downloads additional components allowing it to collect passwords from the same site of the wrongdoers that the loader used earlier. These components are downloaded in parts and assembled on the victim’s computer.

3.2. With the help of the downloaded components the evildoers take from the victims for mail services, social networks, etc. The victims’ passwords are sent to the evildoers’ wallets.

3.3. The Trojan also collects the victims’ account data from the sites of the wrongdoers. With the help of the collected data the evildoers send mail services and social networks messages. The victims’ account data is one of the most important information for generating new attacks.

It is interesting that the Trojan also adds the victims’ account data to the attack letters. The evildoers’ Russian language letters contain the following text:

Компьютер заражен вирусом. Для  
диспетчера паролей и ключей

In several cases the theme of the letter and the name of the attachment do not match each other — this is a drawback of the automatic generation of letters and malware objects.

The object with the long name is the JavaScript Trojan-Downloader.JS.Scatter.i described earlier but already with another obfuscation.

**Code fragment of the downloader Trojan-Downloader.JS.Scatter.i with another obfuscation**



**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

| Necessary | Preferences | Statistics | Marketing |
|-----------|-------------|------------|-----------|
|           |             |            |           |

Show details >

Despite the obfuscation both scripts are successfully detected by Kaspersky Lab products, both by signature and using heuristics written over a year ago, before the appearance of this type of malware.


## To the aid of the bad guys: the human factor

The business of cyber-blackmailers is flourishing. In 2014 Kaspersky Lab recorded more than seven million attacks on its users with the use of objects from the Trojan-Ransom family.







**In 2014 Kaspersky Lab recorded more than 7 million attacks with the use of encrypters**

 **Tweet**



**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

|   |   |   |   |
|---|---|---|---|
| <b>Necessary</b>  | <b>Preferences</b>  | <b>Statistics</b>   | <b>Marketing</b>  |
|  |  |  |  |

[Show details](#) >

Num Malefac Although decrypti case of on avera decryption. Unfortunately, for companies that have lost their data it is often simpler to pay than lose important information. It is no surprise that organisations are the main target of evildoers utilising encrypters.

Why are encrypters able to inflict such damage?

As was mentioned above, most antivirus companies constantly improve their defences against encrypters. For instance Kaspersky Lab has implemented special technical ‘[Protection against Encrypter Programs](#)’ in its products. However, as is well known, the weakest point in IT protection is the user. And in the case of encrypters this is extremely relevant.

We conduct special events dedicated to combatting this type of malware. These events include a whole complex of measures: analysis of all incidents that have occurred at organisations contacting our technical help service (using both our own and other antivirus products); search for and collection of samples of encrypters; analysis of the work of each defensive component of our products in each event that happened; improvement of existing and development of new methods of detecting and remedying the consequences of the actions of encrypters. This is painstaking work and takes a lot of time, but it is necessary for our products to deal successfully with this constantly changing threat.

 **Tweet**

It seems to us that one possible reason for such carelessness among users, strange as it may seem, is down to significant technical progress. The improved defences of browsers and operating systems has led to a state where today users encounter the threats of malicious programs less often than previously. As a result some of them, not thinking, switch off individual components of their antivirus products or don't use them at all.

**This website uses cookies**

The lack  
Earlier it  
of failure  
data. Bu  
And mos  
is infect  
chances

## Traps for the unwary: how users are attacked

If you compile a hit parade of the methods used to spread encrypters the first and second places would be taken resoundingly by email. In the first case the dangerous object is contained directly in the letter and in the second the letter doesn't contain the object itself but a hyperlink to it. In third place in terms of popularity we see attacks via a system for remote control of the computer (Microsoft's Remote Desktop Protocol or RDP). Such attacks as a rule are carried out on an organisation's servers.

## RDP attack

- a password must be tough to crack (complicated);
- a password should be known only to its user;
- a password should be changed regularly.

## Finding a needle in a haystack: Machine learning at the forefront of threat hunting research

## State of ransomware in 2024

## Financial cyberthreats in



are in

**Friday:**  
**st**

**Show details** >

## Attack via electronic mail

If an attack by RDP occurs without the user’s involvement; an attack via email must be activated by the user him or herself by running a received file or clicking on a link in a letter. This is achieved by social engineering methods used by the wrongdoer or, to put it more simply, by lying to the user. The wrongdoer’s strategy is often built on the fact that the person under attack is chosen because they have a job totally unrelated to information security. Such people may not even know of the existence of such threats as malicious encryption of files.

**The person under attack is chosen because they have a job totally unrelated to information security**



Tweet

### Letter topics

The organisation receives a letter that sounds frightening, for instance a court case has been initiated against the organisation, the details of which are contained in the document attached.



#### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details



A c

The think  
some im  
attachm

For organisations this approach works especially well: the simple employee receiving such a letter bears an unexpected responsibility. The employee tries to share the responsibility and consults his/her colleagues. The evildoer’s chances that someone will open the attachment increase. In several incident investigations it turned out that the in-house lawyers of the victim organisations insisted that the attachment be opened.

**Be suspicious of links and attachments in unexpected letters**



Tweet

And to reduce the suspicions of the recipient the author of the letter might use official logos:

Or the executable file might be built into a Microsoft Word document and be masked by an icon:

The male  
text and  
fact after

***The red text says 'To correct the display switch on macros'***

## Page 13 of 16

The next social engineering technique is the use of special words in the names of files contained in the archives attached to the letter (or downloaded by the user). For instance it could be the word 'checked' or 'secure' plus the name of various anti-virus products. The aim of the malefactors is to make the user believe that the attachment has been checked by an anti-virus product.

*An example of a malicious attachment using the name of an anti-virus product and the extension .js*

The extensions for executable files are specially chosen to be unknown to the casual user. Usually .scr, .com and .js are used.

A special mention goes to attachments apparently providing 'free security tutorials from Kaspersky

Recommendations

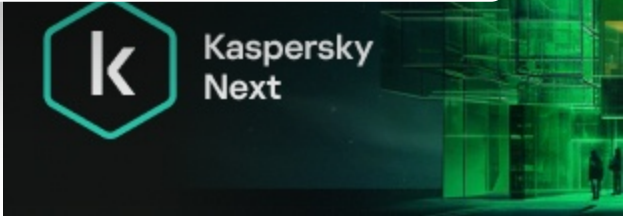
Detailed recommendations

Here we have:

- Make sure that the system is protected by an up-to-date anti-virus product.
- Switch off automatic updates for documents and applications on this computer.
- Be suspicious of e-mails from unknown sources, especially those favoring opening attachments or clicking on links.
- Use the latest version of the operating system and all installed applications.
- And finally, wait for the anti-virus database to be updated before reading your morning mail.
- System administrators (in addition to everything else) should keep users aware of threats.

ENCRYPTIONMALICIOUS SPAMMALWARE STATISTICS

MALWARE TECHNOLOGIESRANSOMWARESPAM LETTERSTROJAN



‘Locked Out’

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

Type your comment here

Name \*

Email \*

Comment

## // LATEST POSTS

SAS

**The Crypto Game of Lazarus APT: Investors vs. Zero-days**

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

**Grandoreiro, the global trojan with grandiose goals**

GREAT

CRIMEWARE REPORTS

**Stealer here, stealer there, stealers everywhere!**

GREAT

CRIMEWARE REPORTS

**Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia**

KASPERSKY

## // LATEST



### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

04 SEP 2024

THRILLER

**Inside the world of the human cybercriminal**

ANNA PAVLOVA

Necessary

☐

Preferences

☐

Statistics

☐

Marketing

☐

Show details >

## // RECENT

**Beyond the expansion of the SideWinder APT group**

Kaspersky analyzes SideWinder APT’s recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

**EastWind campaign: new CloudSorcerer attacks on government organizations in Russia**

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

**BlindEagle APT: Kaspersky shares insights into the activity and TTPs**

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

**APT trends report Q2 2024**

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.

New product

**Let’s go Next: redefine your business's cybersecurity**


 **Kaspersky Next**



# // SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

☐ I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >