Targeted ransomware: it’s not just about encrypting your data!

securelist.com/targeted-ransomware-encrypting-data/99255/

Authors

-  Dmitry Bestuzhev
- Expert Fedor Sinitsyn

Part 1 - “Old and New Friends”

When we talk about ransomware, we need to draw a line between what it used to be and what it currently is. Why? Because nowadays ransomware is not just about encrypting data – it’s primarily about data exfiltration. After that, it’s about data encryption and leaving convincing proof that the attacker was in the network, and finally, it’s extortion. And again, it’s not about the data loss itself but about publishing stolen data on the internet. Let’s call it “Ransomware 2.0”.

Why is it so important to state this? Because many organizations still believe that it's all about malware, and if your anti-malware protection is good enough, you'll be OK. As long as people think this way, the ransomware threat actors will continue to succeed again and again.

In most cases, the initial vector of attack is exploiting some already known vulnerabilities in commercial VPN software. Other cases involve abusing RDP-enabled machines exposed to the internet. Then there's the exploitation of the vulnerable router firmware. As you can see, it's not necessarily about malware but also bad practices, a lack of patching cycles, and general security procedures.

Sometimes ransomware threat actors may rely on traditional malware like botnet implants previously dropped by other cybercriminal groups. And finally, if we recall the Tesla story, the attempt to infect that factory was through someone working at the company. That means physical human access is also a vector. It is complex.

In all cases, the original entry point is to start network reconnaissance, then lateral movement, then data exfiltration. Once it is done, it finally comes to the "coup de grace" – the ransomware. By the time ransomware is deployed, the anti-malware product might be already deleted or disabled by the threat actor because they already had full control over the domain network and could operate as legitimate administrators. So it is about a full red team operation that relies on different hacking techniques, including those to disable anti-malware solutions mostly through legitimate tools and misc scripts. That way, the threat actor doesn't bother if the ransomware itself will be detected or not.

Different ransomware groups use different TTPs and different encryption techniques. Today we want to talk about two of them: Ragnar Locker and Egregor – a veteran and a newbie. Both singular and distant at the same time.

Ragnar Locker

Early variants of this malware were discovered in 2019; however, Ragnar Locker gained notoriety in the first half of 2020 when it started to attack large organizations.

Ragnar Locker is highly targeted, to the extent that each individual sample is specifically tailored for the organization the actors are attacking. The group behind it loves to abuse RDP, while their preferred payment method is bitcoins.

This group owns three .onion domains available on Tor and one Surface Web domain registered on June 16, 2020.

If the victims refuse to pay, their stolen data is published in a so-called Wall of Shame section.

Screenshot of the Wall of Shame where stolen data is exposed

Curiously, this group is positioning itself as a bug bounty hunting group. They claim the payment is their bounty for discovering vulnerabilities that were exploited and to provide decryption for the files and OpSec training for the victim; and, finally, for not publishing the stolen data. Of course, if the victim refuses to pay, the data goes public. Besides that, if the victim chats with the Ragnar Locker threat actor and fails to pay, then the chat is exposed along with the stolen data.

In July 2020, Ragnar Locker made a public announcement that they had joined so-called "Maze Cartel" distraction concept. It means to say that the groups cooperated, exchanging information stolen from victims and publishing it on their websites.

Example of a victim allegedly provided by Maze and published on the Ragnar Locker Wall of Shame page

You can read more about Maze Ransomware here.

Based on the list of victims who refused to pay, the main target of Ragnar Locker are US based companies, while the type of industry varies.

Geography of Ragnar Locker victims (download)

Ragnar Locker victims by industry (download)

Technical description

For our analysis we chose a recently encountered sample of the malware:
1195d0d18be9362fb8dd9e1738404c9d

When started, Ragnar Locker checks the system locale of the machine it is executing on. If determines that it is the locale of one of the countries listed in the screenshot below, it will cease operation and exit without doing anything else.

```
ES Stack[00000B18]:0099CAF0 38 CB 99 00                         dd offset aAzerbaijani  ; "Azerbaijani"
   Stack[00000B18]:0099CAF4 8C CB 99 00                         dd offset aArmenian     ; "Armenian"
   Stack[00000B18]:0099CAF8 20 CB 99 00                         dd offset aBelorussian  ; "Belorussian"
   Stack[00000B18]:0099CAFC D0 CB 99 00                         dd offset aKazakh       ; "Kazakh"
   Stack[00000B18]:0099CB00 C0 CB 99 00                         dd offset aKyrgyz       ; "Kyrgyz"
   Stack[00000B18]:0099CB04 64 CB 99 00                         dd offset aMoldavian    ; "Moldavian"
   Stack[00000B18]:0099CB08 EC CB 99 00                         dd offset aTajik        ; "Tajik"
   Stack[00000B18]:0099CB0C B0 CB 99 00                         dd offset aRussian      ; "Russian"
   Stack[00000B18]:0099CB10 A0 CB 99 00                         dd offset aTurkmen      ; "Turkmen"
   Stack[00000B18]:0099CB14 E0 CB 99 00                         dd offset aUzbek        ; "Uzbek"
   Stack[00000B18]:0099CB18 50 CB 99 00                         dd offset aUkrainian    ; "Ukrainian"
   Stack[00000B18]:0099CB1C 78 CB 99 00                         dd offset aGeorgian     ; "Georgian"
```

For countries not on the above list, it will proceed to stop services with names containing any of the substrings hardcoded in the malware sample and obfuscated by RC4:

```
   .didata:0128D260 76 73 73 2C 73 71 6C 2C+aVssSqlMemtasMe db 'vss,sql,memtas,mepocs,sophos,veeam,backup,pulseway,logme,logmein,'
   .didata:0128D260 6D 65 6D 74 61 73 2C 6D+                                  ; DATA XREF: Stack[00000B18]:0099FDF8↑o
   .didata:0128D260 65 70 6F 63 73 2C 73 6F+                                  ; start+3C3↑o
   .didata:0128D260 70 68 6F 73 2C 76 65 65+                  db 'connectwise,splashtop,wuauserv',0
```

Afterwards, Rangar Locker will terminate running processes according to another substring list contained inside the Trojan body:

```
   .didata:0128D668 73 71 6C 2C 6F 72 61 63+aSqlOracleOcssd db 'sql,oracle,ocssd,dbsnmp,synctime,agntsvc,isqlplussvc,xfssvccon,my'
   .didata:0128D668 6C 65 2C 6F 63 73 73 64+                                  ; DATA XREF: start+3E6↑o
   .didata:0128D668 2C 64 62 73 6E 6D 70 2C+                  db 'desktopservice,ocautoupds,encsvc,firefox,tbirdconfig,mydesktopqos'
   .didata:0128D668 73 79 6E 63 74 69 6D 65+                  db ',ocomm,dbeng50,sqbcoreservice,excel,infopath,msaccess,mspub,oneno'
   .didata:0128D668 2C 61 67 6E 74 73 76 63+                  db 'te,outlook,powerpnt,steam,thebat,thunderbird,visio,winword,wordpa'
   .didata:0128D668 2C 69 73 71 6C 70 6C 75+                  db 'd',0
```

Finally, when all the preparation is done, the Trojan will search for available drives and encrypt the victim's files.

For file encryption RagnarLocker uses a custom stream cipher based on the Salsa20 cipher. Instead of the standard initialization 'magic' constants sigma = "expand 32-byte k" and tau = "expand 16-byte k" normally used in Salsa20, the Trojan generates new random values for each processed file. This is an unnecessary step which makes the cipher incompatible with the standard Salsa20, but doesn't in fact enhance its security.

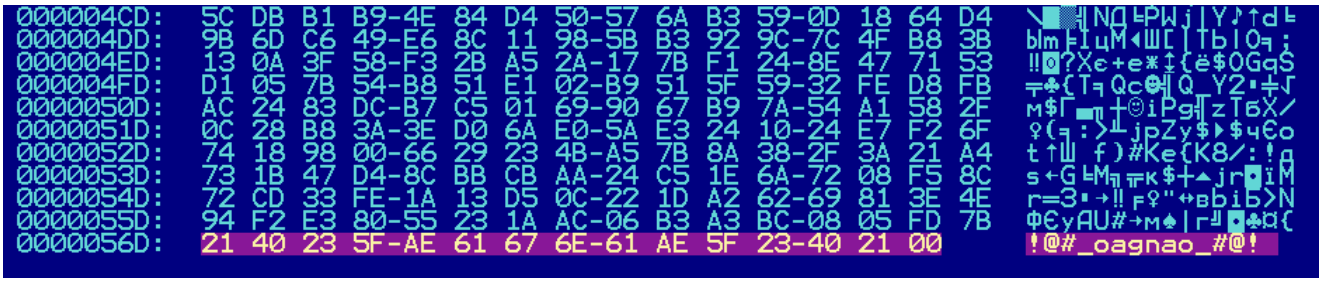
The key and nonce values are also uniquely generated for each file, and will be encrypted along with the constants described above by RSA using the public 2048-bit key hardcoded in the Trojan's body.

The RNG is based on the MS CryptoAPI function CryptGenRandom, which is considered secure, and the SHA-256 hash algorithm. The RNG implementation looks a bit awkward, but we haven't found any critical flaws in it.

```
ptr = pbBuffer;
CryptAcquireContextW(&phProv, 0, 0, PROV_RSA_FULL, 0xF0000040);
CryptGenRandom(phProv, dwLen, pbBuffer);
CryptReleaseContext(phProv, 0);
CryptAcquireContextW(&phProv, 0, 0, PROV_RSA_FULL, 0x10u);
CryptAcquireContextW(&hProv, 0, 0, PROV_RSA_FULL, 0xF0000040);
CryptGenRandom(hProv, 0x40u, rand_64);
CryptReleaseContext(hProv, 0);
CryptAcquireContextW(&hProv, 0, 0, PROV_RSA_FULL, 0x10u);
if ( (int)dwLen > 0 )
{
  while ( 1 )
  {
    SHA256_Init(sha_ctx);
    SHA256_Update(sha_ctx, rand_64, 64);
    SHA256_Update(sha_ctx, ptr, dwLen);
    if ( (int)dwLen <= 64 )
      break;
    SHA256_Final(ptr, (int)sha_ctx);
    ptr += 64;
    dwLen -= 64;
    v4 = GetProcessHeap();
    HeapFree(v4, 0, rand_64);
    if ( (int)dwLen <= 0 )
      return;
  }
  SHA256_Final(v6, (int)sha_ctx);
  memcpy(ptr, v6, dwLen);
}
```

The RNG procedure pseudocode used by a recent Ragnar Locker variant

After encrypting the content of each of the victim's files, Ragnar Locker will append the encrypted key, nonce and initialization constants to the encrypted file, and finalize by adding the marker "!@#_®agna®_#@!"



Trailing bytes of a file encrypted by Ragnar Locker

The ransom notes dropped by the Trojan contain the name of the victim organization which clearly indicates that the criminals utilize a targeted approach, identify their victim and carefully prepare the attack.

```
**********************************************************************************************************************
                                          HELLO                !
 IF YOU ARE READING THIS, IT'S MEAN YOUR DATA WAS ENCRYPTED AND YOU SENSITIVE PRIVATE INFORMATION WAS STOLEN!
                    READ CAREFULLY THE WHOLE INSTRUCTION NOTES TO AVOID DIFFICULTIES WITH YOUR DATA

                                          by R A G N A R     L O C K E R !
**********************************************************************************************************************
                   *YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL*
                         (contact information you will find at the bottom of this notes)

                                          !!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT Use any third-party or public Decryption software, it also may DAMAGE files.
DO NOT Shutdown or Reset your system, it can DAMAGE files
-------------------------------------

There is ONLY ONE possible way to get back your files - contact us via LIVE CHAT and pay for the special
DECRYPTION KEY !
For your GUARANTEE we will decrypt 2 of your files FOR FREE, to show that it Works.

Don't waste your TIME, the link for contact us will be deleted if there is no contact made in closest time and
you will NEVER restore your DATA.
!!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

                                          ! WARNING !
                                 Whole your network was fully COMPROMISED!

 We has BREACHED your security perimeter and DOWNLOADED more than 3 TB of your PRIVATE SENSITIVE Data, including
your: Accounting, Financial,
Confidential and/or Proprietary Business information, Confidential Contracts, Non-Disclosure Agreements,
Administrators directories, SQL Databases and etc.!
Also we have access to Corporate Correspondence, Personal information about your clients such as Social Security
Numbers and even more about your partners and your staff.
```

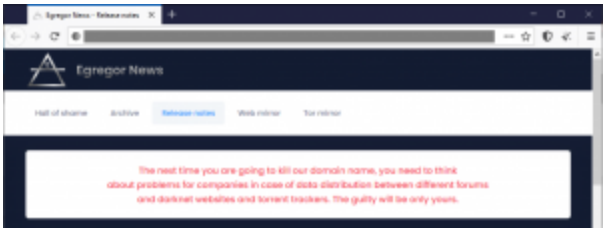
The ransom note also attempts to further scare the victim into paying by emphasizing that the threat actors have stolen confidential data in addition to the file encryption performed by the Trojan.

```
---------------------------------------------------------------------------------------------------------------------
Whole data that gathered from your private files and directories could be published in MASS MEDIA for BREAKING
NEWS!
Yours partners, clients and investors would be notified about LEAK, the consequences will have a DISASTROUS
effect on your company's reputation!

However if we make a Deal everything would be kept in Secret and all your data will be Restored, so it is much
cheaper and easier way for you than lawsuits expenses.

You can take a look for some more examples of what we have, right now it's a private, temporary and hidden page,
but it could become permanent and accessable for Public View if you decide NOT pay.
```

Egregor

Egregor ransomware is a new strain that was discovered in September 2020, and after the initial analysis we noticed code similarities between this new threat and Sekhmet ransomware, as well as the notorious Maze ransomware, which announced on November 1st, 2020 that they shut down.

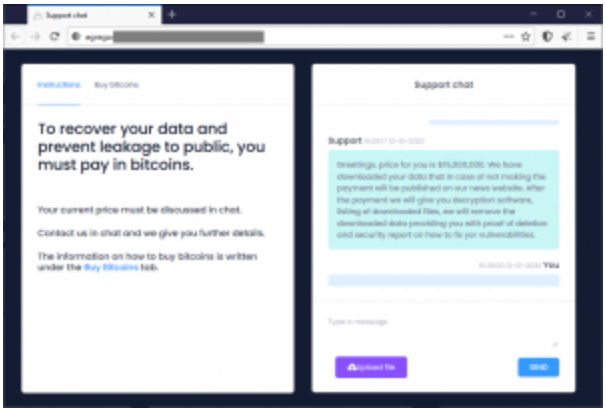
Egregor keeps at least one .onion domain and two Surface Web domains. The first Surface Web domain was registered on September 6, 2020 and the second one on October 19, 2020. At the time of writing, both Surface Web domains were intermittent. That is probably why on the main page of the Onion domain, there is a big disclaimer with this notice:



The Egregor ransomware is typically distributed by the criminals following a network breach. The malware sample is a DLL file that needs to be launched with the correct password given as a command line argument. The DLL is usually dropped from the Internet. On occasions, the domains used to spread it exploit names or words used in the victim's industry.

Egregor is probably the most aggressive Ransomware family in terms of negotiation with the victims. It gives only 72 hours to contact the threat actor. Otherwise, the victim's data is processed for publishing.

The ransomware payment is negotiated and agreed upon via a special chat assigned to each victim. The payment is received in BTC.



Example of a chat negotiating to pay the ransom

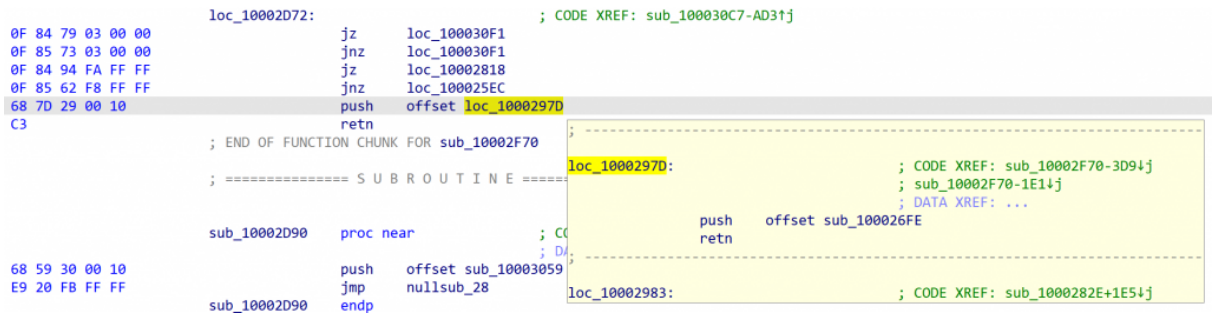
Technical description

b21930306869a3cdb85ca0d073a738c5

As mentioned above, the malware sample only works if a correct password is provided during launch. The packer of the malware will use this password to decrypt the payload binary. A missing or incorrect argument will result in an incorrect decryption of the payload, which will be unable to execute and will crash instead.

This technique is intended to hinder both automatic analysis in sandbox-type systems, and manual analysis by researchers: without the correct password it is impossible to unpack and analyze the payload binary.

After unpacking two layers of the malicious packer, we end up with an obfuscated binary which is still not suitable for static analysis. The obfuscation techniques used in Egregor strongly resemble those in Maze and Sekhmet: the code is 'torn apart' by control flow obfuscation using conditional and unconditional jumps, PUSH+JMP instead of RETN, and so on.



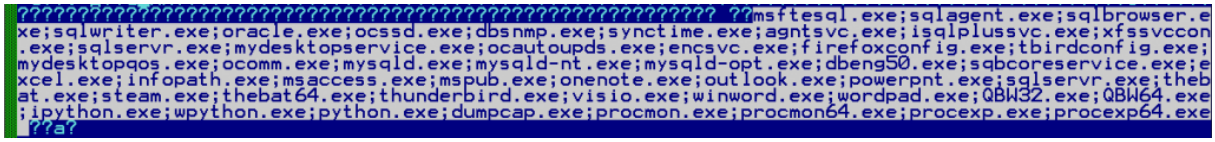
Control flow obfuscation example

When the payload starts executing, first of all, it will check the system and user language of the OS to avoid encrypting machines having one of the following languages installed:

Armenian (Armenia)
Azerbaijani (Cyrillic, Azerbaijan)
Azerbaijani (Latin, Azerbaijan)
Belarusian (Belarus)
Georgian (Georgia)
Kazakh (Kazakhstan)
Kyrgyz (Kyrgyzstan)
Romanian (Moldova)

Russian (Moldova)
Russian (Russia)
Tajik (Cyrillic, Tajikistan)
Tatar (Russia)
Turkmen (Turkmenistan)
Ukrainian (Ukraine)
Uzbek (Latin, Uzbekistan)

Then it will attempt to terminate the following processes:



This is intended to make writable potentially valuable files such as documents or databases that may have been in use at the moment of infection. In addition, some programs typically used by researchers, e.g., procmon or dumpcap, are also listed for termination to further hinder dynamic analysis.

Egregor uses a hybrid file encryption scheme based on the stream cipher ChaCha and the asymmetric cipher RSA.

The RSA-2048 master public key of the criminals is embedded in the trojan's body.

When executing on a victim's machine, Egregor generates a new unique pair of session RSA keys. The session private RSA key is exported and encrypted by ChaCha with a uniquely generated key + nonce, then the key and nonce are encrypted by the master public RSA key. The results are saved in a binary file (in our case it's named C:\ProgramData\dtb.dat), as well as a base64-encoded string in the ransom notes.

For each data file Egregor processes, it generates a new 256-bit ChaCha key and 64-bit nonce, encrypts the file content by ChaCha, then encrypts them using the session public RSA key, and saves them along with some auxiliary information in the end of the encrypted file.

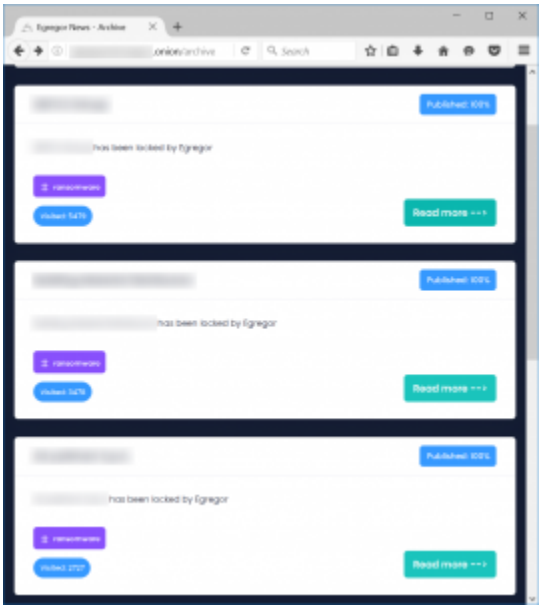
The last 16 bytes of each encrypted file are comprised of a dynamic marker: a random DWORD and this same DWORD xor'ed with the value 0xB16B00B5 which equals 'BIGBOOBS' in so-called leet speak, originally used by "hackers, crackers and script kiddies", according to Wikipedia.

```
157  hProv = (crypt->vtbl->Crypt_GetProv)(crypt, v31, v32, v33, v34);
158  if ( !CryptGenRandom(hProv, 0x20u, footer)
159    || !CryptGenRandom(hProv, 8u, &footer[32])
160    || (ChaCha_SetKey(&chacha_ctx, footer, 256),
161        ChaCha_SetNonce(&chacha_ctx, &footer[32]),
162        Buffer.LowPart = 40,
163        !(crypt->vtbl->Crypt_Encrypt)(crypt, footer, &Buffer, 256, 0, 0)) )
164  {
165LABEL_28:
166    v10 = 0;
167    v9 = 0;
168    goto LABEL_52;
169  }
170  v44 = GetTickCount();
171  *&footer[264] = Rand(&v44);
172  *&footer[268] = *&footer[264] ^ 0xB16B00B5;
173  *&footer[260] = *(g_strings + 28);
174  *&footer[256] = 0;
175  if ( v35 && __SPAIR64__(v35 >> 12, v35 << 20) < v8->QuadPart )
176    *&footer[256] = v35;
177  LOBYTE(v96[0]) = 0;
178  Buffer.QuadPart = 0i64;
179  if ( SetFilePointerEx(hFile, 0i64, 0, FILE_END) )
180    v36 = !WriteFile(hFile, footer, 0x110u, NumberOfBytesWritten, 0);
181  else
182    v36 = 1;
183  *NumberOfBytesWritten = LOBYTE(v96[0]);
184  SetFilePointerEx(hFile, LOBYTE(v96[0]), 0, 0);
```

Part of the file encryption procedure pseudocode

The main page of the data leak website contains news about recently attacked companies along with some sarcastic remarks written by the ransomware group.

The archive section of the site lists the victims of the extortionists and the links to download the stolen data.



Based on the information of those victims who refused to pay, the geographic reach of Egregor is way more extensive than that of Ragnar Locker:

Geography of Egregor victims (download)

The same is true for the number of attacked industries:

Egregor victims by industry (download)

Conclusions

Unfortunately, Ransomware 2.0 is here to stay. When we talk about 2.0, we mean targeted ransomware with data exfiltration. The whole extortion process is primarily about the victims' data not being published on the internet and only then about decryption. Why is it so important for the victims that their data is not published? Because possible lawsuits and fines due to violations of regulations like HIPAA, PIC or GDPR can result in immense financial losses, reputational damage and potential bankruptcy.

As long as companies see ransomware threat actors as typical malware threats, they will also fail. It is not about just endpoint protection; it is about red teaming, business analysts working with exfiltrated documents evaluating the ransom to pay. It is also about data theft, of course, and public shaming, leading to all sorts of problems in the end.

Our next chapter will cover something else – a perfect umbrella for different threat actors with different motivations operating under the aegis of Ransomware 2.0.

How to protect yourself

To keep your company protected against these types of ransomware attacks, Kaspersky experts recommend:

1. Do not expose remote desktop services (such as RDP) to public networks unless absolutely necessary and always use strong passwords for them.
2. Promptly install available patches for commercial VPN solutions providing access for remote employees and acting as gateways in your network.
3. Always keep software updated on all the devices you use to prevent ransomware from exploiting vulnerabilities
4. Focus your defense strategy in detecting lateral movements and data exfiltration to the Internet. Pay a special attention to the outgoing traffic to detect cybercriminals connections. Back up data regularly. Make sure you can quickly access it in an emergency when needed.
5. Use solutions like Kaspersky Endpoint Detection and Response and Kaspersky Managed Detection and Response service which help to identify and stop the attack on early stages, before attackers reach their final goals.
6. To protect the corporate environment, educate your employees. Dedicated training courses can help, such as the ones provided in the Kaspersky Automated Security Awareness Platform. A free lesson on how to protect from ransomware attacks is available here.
7. Use reliable endpoint security solution, such as Kaspersky Endpoint Security for Business that is powered by exploit prevention, behavior detection and a remediation engine that is able to roll back malicious actions. KESB also has self-defense mechanisms which can prevent its removal by cybercriminals.

- Cybercrime
- Data Encryption
- Malware Descriptions
- Malware Statistics
- Malware Technologies
- Ransomware
- RDP
- Trojan

Authors

-  Dmitry Bestuzhev
- Expert Fedor Sinitsyn

Targeted ransomware: it’s not just about encrypting your data!

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