

SUPPORT CENTER ([HTTPS://SUPPORTCENTER.CHECKPOINT.COM/SUPPORTCENTER/PORTAL?EVENTSUBMIT_DOHOME](https://supportcenter.checkpoint.com/supportcenter/portal?EVENTSUBMIT_DOHOME))

USER CENTER / PARTNERMAP ([HTTPS://USERCENTER.CHECKPOINT.COM/USERCENTER/INDEX.JSP](https://usercenter.checkpoint.com/usercenter/index.jsp))

THREAT PREVENTION RESOURCES ([HTTP://WWW.CHECKPOINT.COM/THREAT-PREVENTION-RESOURCES/INDEX.HTML](http://www.checkpoint.com/threat-prevention-resources/index.html))

(<https://usercenter.checkpoint.com/>)



Check Point (<http://www.checkpoint.com>)
SOFTWARE TECHNOLOGIES LTD.

PRODUCTS / SOLUTIONS ([HTTP://WWW.CHECKPOINT.COM/PRODUCTS-SOLUTIONS/](http://www.checkpoint.com/products-solutions/))

SUPPORT / SERVICES ([HTTP://WWW.CHECKPOINT.COM/SUPPORT-SERVICES/](http://www.checkpoint.com/support-services/))

PARTNERS ([HTTP://WWW.CHECKPOINT.COM/PARTNERS/](http://www.checkpoint.com/partners/))

COMPANY ([HTTP://WWW.CHECKPOINT.COM/ABOUT-US/](http://www.checkpoint.com/about-us/))



Home (<http://www.checkpoint.com>) > Company (<http://www.checkpoint.com/about-us/index.html>) > Check Point Blog (<http://blog.checkpoint.com>) > Threat Research (http://blog.checkpoint.com/category/threat_research/) > "Offline" Ransomware Encrypts Your Data without C&C Communication

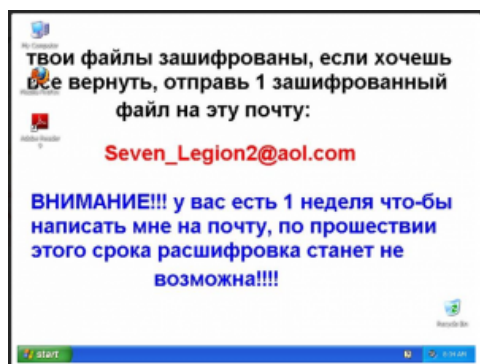
"Offline" Ransomware Encrypts Your Data without C&C Communication (<http://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/>)

by Omer Dembinsky, Lead Intelligence Analyst; Stanislav Skuratovich, Malware Reverse Engineering Team; Lotem Finkelsteen, Security Analyst
posted 2015/11/04



(<http://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/>)

Early in September, Check Point obtained a sample of a ransomware. When the sample was run, the following message, written in Russian, appeared:



([http://blog.checkpoint.com/wp-content/uploads/2015/11/figure-](http://blog.checkpoint.com/wp-content/uploads/2015/11/figure-1.png)

1.png)

Translation:

"Your files are encrypted, if you wish to retrieve them, send 1 encrypted file to the following mail address:

Seven_Legion2@aol.com (mailto:Seven_Legion2@aol.com)

*ATTENTION!!! You have 1 week to mail me,
after which the decryption will become impossible!!!!"*

All personal files were indeed encrypted, with each file renamed to the following format:

email-[address to contact].ver-[Ransomware internal version].id-[Machine identifier]-[Date & Time][Random digits].randomname-[Random name given to the encrypted file].cbf

Example:

email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-NPEULAODSHUJYMAPESHVKYNBQETHWKZOBQFT-10@6@2015 9@53@19 AM5109895.randomname-EFWMERGVKYNBPETHVKZNBQETHWKZNB.RGV.cbf

When running, the ransomware does not interact with the user, other than changing the wallpaper. Furthermore, while most known ransomware requires Internet connection and successful communication to their C&C servers before initiating the encryption, this sample does not need Internet connection to encrypt files and display the ransom message. This means that there is no key exchange between the infected machine and the attacker, which eliminates one option of stopping the attack.

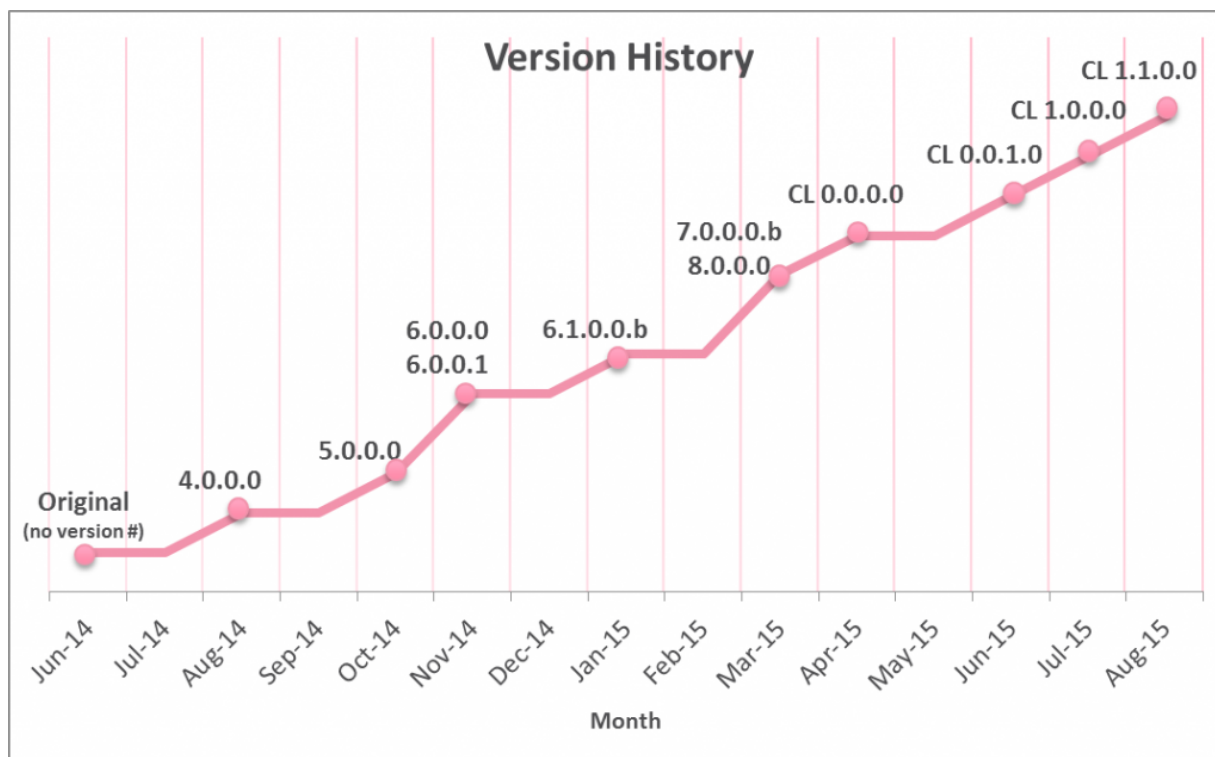
Check Point reached out anonymously to the attacker's email, and received a reply requesting a payment of 20,000 Russian Ruble (approx. \$300) on the same day or 25,000 (approx. \$380) on the following day, to receive a decryption program and key.

As the behavior is quite different from most known samples, we decided to explore the ransomware in greater depth, in both the intelligence and technical aspects.

-

Intelligence Analysis

During our research, we found many online references to this ransomware, especially in Russian language forums. This ransomware family appears to have been around for over a year, with the first reference in June 2014 to the original version (no associated version number). Since then, 11 new versions have been reported. The chart below shows the version history (dates according to first appearance in forums or reports online):



(<http://blog.checkpoint.com/wp-content/uploads/2015/11/fig-2.png>)

Note: Between March and April 2015, the file version schema changed. A "CL" prefix was added and the version numbers were restarted. A parallel change was also made to the format of the encrypted file name. The older format (pre-April 2015) is as follows:

[original file name].id-[[Machine identifier]-[Date]-[Time]][Random digits]]-email-[address to contact]-ver-[Ransomware internal version].cbf

Example:

excel4.xls.id-{AHMSYEKQVBHMSYEJVPAGMSXDJOAGLRWCHNT-11@09@2014 00@47@473042530}-email-ivanivanov34@aol.com-ver-4.0.0.0.cbf

*For the original version, which did not have a specific version number, the format was identical to the older format, except for the lack of the version section at the end of the file name. For example:

001.jpg.id-{NKYVGVEZRTCVMENMHRALUDMXGPKJSBXWFAJ-03.09.2014 1@45@403928355}-email-sishelp100@gmail.com.cbf

Differences between the two formats:

- The older encrypted file name includes the name of the original file. In the current format, the file is given a random name.
- The older format has the email address and the version at the end. The current format has them at the beginning.

Many email addresses, mainly AOL and Gmail accounts (but also others) have been associated with this ransomware:

ivanivanov34@aol.com	marivanna1953@gmail.com
mserbinov@aol.com	moshiar@aol.com
masfantomas@aol.com	d_madre@aol.com
load180@aol.com	ninja.gaiver@aol.com
trojanencoder@aol.com	scasiva@aol.com
vpupkin3@aol.com	igor_svetlov2@aol.com.
base1c1c1c@gmail.com	Seven_Legion2@aol.com
deskriphen1c@gmail.com	cryptolocker@aol.com
helpdecrypt123@gmail.com	iizomer@aol.com
vernutfles@gmail.com	ivanivanov34@aol.com
helpfiledeskript111@gmail.com	gcaesar2@aol.com
watnik91@aol.com	help163btc@163.com
watnik91@gmail.com	hontekilla@aol.com
systemsinfo32@gmail.com	monica.moka@aol.com
sishelp100@gmail.com	eric.decoder10@gmail.com
deskr1000@gmail.com	madeled@mail.ru

(<http://blog.checkpoint.com/wp-content/uploads/2015/11/fig-3.png>)

Note the email address madeled@mail.ru, which is the only one found to be associated with a Russian email provider, and was also one of the email addresses associated with the original version of this ransomware. It has not appeared after version 4.0.0.0.

This ransomware (at least specific versions of it) has been given unique names by different vendors:

- **Ransomcrypt.U** (Symantec) – See https://www.symantec.com/security_response/writeup.jsp?docid=2015-092211-0927-99&tabid=2 (https://www.symantec.com/security_response/writeup.jsp?docid=2015-092211-0927-99&tabid=2)

This includes a comprehensive analysis of the ransomware behavior on the machine (not including the encryption mechanism).

- **Win32.VBKryjetor.wfa** (Kaspersky) – Refers to version CL 1.0.0.0 (for the specific sample we analyzed)
- **Ninja Ransomware** (Enigma Software) – Refers to the email gaiver@aol.com, although there is no apparent difference from other emails.
- **Troj/Agent-AOTR** (Sophos) – Refers to version CL 1.0.0.0
- **Troj/Drop-HQ** (Sophos) – Refers to version CL 1.0.0.0
- **Troj/Ransom-AZT** (Sophos) – Refers to version CL 1.0.0.0
- **Troj/Ransom-BGX** (Sophos) – Refers to version CL 1.0.0.0
- **Troj/Ransom-BJQ** (Sophos) – Refers to version CL 1.0.0.0
- **Troj/Ransom-BJV** (Sophos) – Refers to version CL 1.0.0.0
- **Troj/Agent-ANBL** (Sophos) – Refers to version CL 0.0.1.0
- **Troj/Ruftar-H** (Sophos) – Refers to version CL 1.0.0.0
- **Troj/VB-IHK** (Sophos) – Refers to version 6.1.0.0.b
- **Mal/Delp-AI** (Sophos) – Refers to version 4.0.0.0

Technical Analysis (Encryption)

Ransomware Details

The ransomware sample investigated by Check Point was from version CL 1.0.0.0 (as can be seen in the encrypted file name). It uses a protector that was written in *Visual Basic* compiled language. To unpack the payload, the ransomware restarts its own process using section mapping and overwrites four times. The payload that is responsible for file encryption is most likely written in *Delphi* language using some additional *Pascal* modules (for example, *FGInt* that is used to represent large numbers). We mention this fact as it is not usual for ransomware to utilize *Pascal*-based languages. The ransomware does not contain much functionality except for the file encryption capability.

Encryption Functionality

The encryption functionality is built with several layers of encoding and encryption, including two separate levels of RSA:

1. The beginning (first 30000 bytes) of each file is encrypted using two buffers of digits and letters that are randomly generated on the infected machine. The encryption process includes taking each original byte along with one byte from each of the randomly generated buffers and performing mathematical operations on them.
2. The remainder of each file (if it exists) is encrypted using an RSA public key ("local") that is randomly generated on the infected machine, along with the matching local RSA private key required for decryption of the data.
3. The randomly generated buffers and the local RSA private key that are required for decryption are added as metadata to each encrypted file, and are then encrypted using three hardcoded RSA 768 public keys that the offender created in advance ("remote"). The matching remote RSA private keys required to unlock the metadata are located on the attacker's side.

Due to this functionality, the ransomware is able to encrypt all files locally without connecting to a C&C server. Once the attacker receives a file from the infected machine, he can easily decrypt the metadata using his remote RSA private keys, and find the buffers and local RSA private key that were randomly generated on the infected machine which can be used to decrypt the file.


It is not feasible to try to decrypt the remote RSA encryption without the remote private key. The necessary time frame would be approximately 2 years and would involve using many computers. Therefore, paying the ransom to get the decryption application and the decryption keys from the attacker seems to be the only way to recover the encrypted files.

For More Details Read: Check Point Technical Report (<http://blog.checkpoint.com/wp-content/uploads/2015/11/Check-Point-Technical-Report-.pdf>)

Posted Under: Threat Research (http://blog.checkpoint.com/category/threat_research/)

Tags: Ransomware (<http://blog.checkpoint.com/tag/ransomware/>)


Link to this post: <http://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/> ()

 (<http://blog.checkpoint.com/2015/11/03/phishing-for-employees-in-russia/>)

Previous Post

Phishing for Employees in... (<http://blog.checkpoint.com/2015/11/03/phishing-for-employees-in-russia/>)

Leave a Reply

 (<http://blog.checkpoint.com/2015/11/05/check-point-discovers-critical-vbulletin-0-day/>)

Your email

Next Post

address will Check Point Discovers Critical vBulletin... (<http://blog.checkpoint.com/2015/11/05/check-point-discovers-critical-vbulletin-0-day/>)

not be published. Required fields are marked *

Name *

Email *

Website

Please complete the equation to verify your submission. *

8 × = twenty four

Start typing...

You may use these HTML (HyperText Markup Language) tags and attributes:

```
<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del  
datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>
```

Post Comment

Post Archives

- November 2015 (<http://blog.checkpoint.com/2015/11/>)
- October 2015 (<http://blog.checkpoint.com/2015/10/>)
- September 2015 (<http://blog.checkpoint.com/2015/09/>)
- August 2015 (<http://blog.checkpoint.com/2015/08/>)
- July 2015 (<http://blog.checkpoint.com/2015/07/>)
- June 2015 (<http://blog.checkpoint.com/2015/06/>)
- May 2015 (<http://blog.checkpoint.com/2015/05/>)
- April 2015 (<http://blog.checkpoint.com/2015/04/>)
- March 2015 (<http://blog.checkpoint.com/2015/03/>)
- February 2015 (<http://blog.checkpoint.com/2015/02/>)
- January 2015 (<http://blog.checkpoint.com/2015/01/>)
- December 2014 (<http://blog.checkpoint.com/2014/12/>)
- November 2014 (<http://blog.checkpoint.com/2014/11/>)
- October 2014 (<http://blog.checkpoint.com/2014/10/>)
- September 2014 (<http://blog.checkpoint.com/2014/09/>)
- August 2014 (<http://blog.checkpoint.com/2014/08/>)
- July 2014 (<http://blog.checkpoint.com/2014/07/>)
- June 2014 (<http://blog.checkpoint.com/2014/06/>)
- May 2014 (<http://blog.checkpoint.com/2014/05/>)
- April 2014 (<http://blog.checkpoint.com/2014/04/>)
- March 2014 (<http://blog.checkpoint.com/2014/03/>)
- February 2014 (<http://blog.checkpoint.com/2014/02/>)
- January 2014 (<http://blog.checkpoint.com/2014/01/>)
- December 2013 (<http://blog.checkpoint.com/2013/12/>)
- November 2013 (<http://blog.checkpoint.com/2013/11/>)
- October 2013 (<http://blog.checkpoint.com/2013/10/>)
- August 2013 (<http://blog.checkpoint.com/2013/08/>)
- July 2013 (<http://blog.checkpoint.com/2013/07/>)
- January 2013 (<http://blog.checkpoint.com/2013/01/>)
- December 2012 (<http://blog.checkpoint.com/2012/12/>)
- November 2012 (<http://blog.checkpoint.com/2012/11/>)



RSS

(<http://blog.checkpoint.com/feed/>)

Products

Next Generation Threat Prevention (<http://www.checkpoint.com/products-solutions/threat-prevention/>)

Mobile Security (<http://www.checkpoint.com/products-solutions/mobile-security/>)

Next Generation Firewalls (<http://www.checkpoint.com/products-solutions/next-generation-firewalls/>)

Security Management (<http://www.checkpoint.com/products-solutions/security-management/>)

Products A-Z (<http://www.checkpoint.com/products-solutions/all-products/>)

30-Day Free Trial (<http://www.checkpoint.com/try-our-products/>)

Find a Partner (<http://partners.us.checkpoint.com/partnerlocator/>)

Contact Sales (<http://www.checkpoint.com/about-us/contact-us/>)

Threat Prevention Resources

IPS Advisories & Protections (<http://www.checkpoint.com/advisories/>)

Under Attack? (<http://www.checkpoint.com/support-services/threatcloud-incident-response/>)

World Cyber Threat Map
(<https://www.checkpoint.com/ThreatPortal/livemap.html>)

Support and Services

Support Center
(https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doHome)

Support Plans (<http://www.checkpoint.com/support-services/support-plans/>)

Training and Certification (<http://www.checkpoint.com/support-services/training-certification/>)

Forums (<https://forums.checkpoint.com/>)

Design, Deploy, Operate and Optimize (<http://www.checkpoint.com/support-services/design-deploy-operate-optimize/>)

Lifecycle Management Services (<http://www.checkpoint.com/support-services/lifecycle-management/>)

Contact Support (<http://www.checkpoint.com/support-services/contact-support/>)

Partners

Become a Partner (<http://www.checkpoint.com/partners/channel/>)

Find a Partner (<http://partners.us.checkpoint.com/partnerlocator/>)

User Center Sign In
(<https://usercenter.checkpoint.com/usercenter/index.jsp>)

Solutions and Architecture

Retail / Point of Sale (POS) (<http://www.checkpoint.com/products-solutions/retail-point-of-sale-pos/>)

Financial Services (<http://www.checkpoint.com/products-solutions/financial-services-atm/>)

Critical Infrastructure (<http://www.checkpoint.com/products-solutions/critical-infrastructure/>)

Private & Public Cloud (<http://www.checkpoint.com/products-solutions/private-public-cloud/>)

Healthcare (<http://www.checkpoint.com/products-solutions/healthcare/>)

Service Provider / Telco (<http://www.checkpoint.com/products-solutions/service-provider-telco/>)

Software Defined Network (SDN) (<http://www.checkpoint.com/products-solutions/software-defined-network/>)

Governance, Risk & Compliance (<http://www.checkpoint.com/products-solutions/governance-risk-compliance/>)

Software Defined Protection (SDP) (<http://www.checkpoint.com/products-solutions/software-defined-protection-sdp/>)

Company

Facts at a Glance (<http://www.checkpoint.com/about-us/facts-a-glance/>)

Our History (<http://www.checkpoint.com/about-us/our-history/>)

News (<http://www.checkpoint.com/about-us/news-coverage/>)



Blog (<http://blog.checkpoint.com>)


Events (<http://store.checkpoint.com/events/eventsindex.htm>)



Contact Us (<http://www.checkpoint.com/about-us/contact-us/>)

Search Jobs (<http://careers.checkpoint.com/>)

Follow Us

 (<https://twitter.com/checkpointsw>) 
(<https://plus.google.com/+checkpoint/posts>)


(<https://www.facebook.com/checkpointsoftware>)


(https://www.youtube.com/channel/UCXnlgfiXZC8ZKA?sub_confirmation=1) 
(<http://www.checkpoint.com/rss/>)

©2015 Check Point Software Technologies Ltd. All rights reserved. Check Point Software Technologies, Inc. is a wholly owned subsidiary of Check Point Software Technologies Ltd.

Copyright (<http://www.checkpoint.com/copyright/>) | Privacy Policy

(<http://www.checkpoint.com/privacy/>) | Site Map (<http://www.checkpoint.com/site-map/>)