

EXHIBIT 10



Account · Sign in

Malware Protection Center

Home Security software Malware encyclopedia Our research Help Developers

Follow:

TRANSLATE



Win32/Crowti

Summary

Technical information

Microsoft security software detects and removes this threat.

This **ransomware** encrypts the files on your PC and directs you to a webpage with instructions on how to unlock them. It asks you to make a payment using **bitcoins**.

The ransom or "lock" screen can use the name **CryptoDefense** or **CryptoWall**.

This threat can be downloaded by other malware, such as **TrojanDownloader:Win32/Onkods** or **TrojanDownloader:Win32/Upatre**. It can also be downloaded when you click on a link in a spam email.

More information about ransomware can be found on our **Ransomware** page.

Find out ways that malware can get on your PC.

What to do now

Microsoft doesn't recommend you pay the fine. There is no guarantee that paying the ransom will give you access to your files.

If you've already paid, see our **ransomware** page for help on what to do now.

Run antivirus or antimalware software

Use the following free Microsoft software to detect and remove this threat:

- **Windows Defender** for Windows 10 and Windows 8.1, or **Microsoft Security Essentials** for Windows 7 and Windows Vista
- **Microsoft Safety Scanner**

You should also run a full scan. A full scan might find hidden malware.

Advanced troubleshooting

To restore your PC, you might need to **download and run Windows Defender Offline**. See our **advanced troubleshooting** page for more help.

Enable MAPS

Enable the **Microsoft Active Protection Service (MAPS)** on your system to protect your enterprise software security infrastructure in the cloud.

1. Check if MAPS is enabled in your Microsoft security product:
 - i. Select **Settings** and then select **MAPS**.
 - ii. Select **Advanced membership**, then click **Save changes**. With the MAPS option enabled, your Microsoft anti-malware security product can take full advantage of Microsoft's **cloud protection service**.
2. Join the **Microsoft Active Protection Service Community**.

Prevent malware infections from spam emails

- For enterprise users:
 - Follow the appropriate **Exchange Online Protection** instructions to suit your business needs.
 - Learn about how Office 365 can help you block spam using machine learning. See **First look at Advanced Threat Protection: new tools to stop unknown malware & phishing attacks** for details.
- Be aware of the **dangers in opening suspicious emails**. Don't open email attachments or links from untrusted sources.
- The **Microsoft SmartScreen filter** can also help detect spam. It's built-in and enabled by default in Microsoft email programs.
- **Submit spam and non-spam messages to Microsoft for analysis**.

I want to...

Get help

Remove difficult malware
 Avoid tech support phone scams
 See and search the latest threats
 Find answers to other problems

Fix my software

Download and update

Submit a file

Alert level: Severe

This entry was first published on: Jun 09, 2014

This entry was updated on: Jun 12, 2015

This threat is also detected as:
 Dropper/Win32.Necurs (AhnLab)

Trojan-Ransom.Win32.Cryptodef.iu (Kaspersky)

Trojan horse Inject2.AHNI (AVG)

TR/Crypt.Xpack.64673 (Avira)

Trojan.Encoder.514 (Dr.Web)

W32/Cryptodef.AHIOltr (Fortinet)

PWSZbot-FBKQI86B6EE398F44 (McAfee)

Troj/Agent-AHIO (Sophos)

TSPY_ZBOT.SMCC (Trend Micro)

Cryptowall (other)

Cryptodefense (other)

Get more help

You can also visit our [advanced troubleshooting page](#) or search the [Microsoft virus and malware community](#) for more help.

If you're using Windows XP, see our [Windows XP end of support page](#).

[Top](#)

[Provide feedback](#)

Other Microsoft sites

-  [Windows](#)
-  [Office](#)
-  [Surface](#)
-  [Windows Phone](#)
-  [Mobile devices](#)
-  [Xbox](#)
-  [Skype](#)
-  [MSN](#)
-  [Bing](#)
-  [Microsoft Store](#)

Downloads

- [Download Center](#)
- [Windows downloads](#)
- [Office downloads](#)

Support

- [Support home](#)
- [Knowledge base](#)
- [Microsoft community](#)

About

- [The MMPC](#)
- [Evaluating our protection](#)
- [MMPC Privacy Statement](#)
- [Microsoft](#)
- [Careers](#)
- [Citizenship](#)
- [Company news](#)
- [Investor relations](#)
- [Site map](#)

Popular resources

- [Security and privacy blogs](#)
- [Security Response Center](#)
- [Security Intelligence Report](#)
- [Microsoft Safety & Security Center](#)
- [Malware Protection Center](#)
- [Security for IT Pros](#)
- [Security for developers](#)
- [Trustworthy Computing](#)


[Account](#) · [Sign in](#)

Malware Protection Center


[Home](#) [Security software](#) [Malware encyclopedia](#) [Our research](#) [Help](#) [Developers](#)

Follow:



Win32/Crowti

[Summary](#)
[Technical information](#)

Threat behavior

Installation

This threat can be downloaded by other malware, such as [TrojanDownloader:Win32/Onkods](#) or [TrojanDownloader:Win32/Upatre](#). It can also be downloaded when you click on a link in a spam email with a file name similar to *Fax-<random number>.zip* or *incoming_wire_report.zip*.

It injects code into system processes such as *explorer.exe* or *svchost.exe*.

Win32/Crowti installs a randomly named copy of itself in any of these paths:

- `c:\<random name>\<random name>.exe`
- `%APPDATA%\<random name>.exe`
- `<start menu> \programs\startup\<random name>.exe`

It modifies one of the following registry entries so that it runs each time you start your PC:

- In subkey: `HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\Run`
Sets value: "`<random name>`"
With data: "`c:\<random name>\<random name>.exe`"
- In subkey: `HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\Run`
Sets value: "`<random name>`"
With data: "`c:\<random name>\<random name>.exe`"
- In subkey: `HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\RunOnce`
Sets value: "`*<random name>`"
With data: "`c:\<random name>\<random name>.exe`"

Examples of `<random name>` can be:

- `3d0bbc8`
- `7716b6d`

Payload

This malware can encrypt the files on your PC using a public key. The files can be decrypted with a private key stored in a remote server.

It encrypts files with the following extensions:

- | | | |
|--------|--------|--------|
| • .asp | • .gif | • .pem |
| • .ass | • .h | • .pl |
| • .ava | • .hpp | • .png |
| • .avi | • .jpg | • .ppt |
| • .bay | • .js | • .ps |
| • .bmp | • .key | • .py |
| • .c | • .lua | • .RAW |
| • .cer | • .m | • .rm |
| • .cpp | • .mp3 | • .rtf |
| • .crt | • .mpg | • .sql |
| • .cs | • .msg | • .swf |
| • .db | • .obj | • .tex |
| • .der | • .odt | • .txt |
| • .doc | • .PAS | • .wb2 |
| • .DTD | • .pdb | • .wpd |
| • .eps | • .pdf | • .xls |

It does not rename the files it encrypts, it just overwrites them. So you may not realise the file is encrypted until you try to open it.

I want to...

[Get help](#)
[Remove difficult malware](#)
[Avoid tech support phone scams](#)
[See and search the latest threats](#)
[Find answers to other problems](#)
[Fix my software](#)
[Download and update](#)
[Submit a file](#)
Alert level: Severe

This entry was first published on: Jun 09, 2014

This entry was updated on: Jun 12, 2015

This threat is also detected as:

Dropper/Win32.Necurs (AhnLab)

Trojan-Ransom.Win32.Cryptodef.iu (Kaspersky)

Trojan horse Inject2.AHNI (AVG)

TR/Crypt.Xpack.64673 (Avira)

Trojan.Encoder.514 (Dr.Web)

W32/Cryptodef.AHIO!tr (Fortinet)

PWSZbot-FBKQ!86B6EE398F44 (McAfee)

Troj/Agent-AHIO (Sophos)

TSPY_ZBOT.SMCC (Trend Micro)

Cryptowall (other)

Cryptodefense (other)

It then displays a lock screen similar those shown below to tell you that you can recover the files using a personal link that directs you to a Tor webpage asking for payment using Bitcoin as currency.

All files including videos, photos and documents on your computer are encrypted by CryptoWall Software. 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 month. After that, nobody and never will be able to restore files.

In order to decrypt the files, open your personal page on the site [\[redacted\]](#) and follow the instructions.

If <https://12bocejargnqum.browser.com/mq> is not opening, please follow the steps below:

1. You must download and install this browser <http://www.torproject.org/projects/torbrowser.html.en>
2. After installation, run the browser and enter the address: <https://12bocejargnqum.browser.com/mq>
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

IMPORTANT INFORMATION:

Your Personal PAGE: [\[redacted\]](#)
 Your Personal PAGE(using TOR-browser): [\[redacted\]](#)
 Your Personal CODE(if you open site directly): [\[redacted\]](#)

What happened to your files?
 All of your files were protected by a strong encryption with RSA-2048 using CryptoWall. More information about the encryption keys using RSA-2048 can be found here [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?
 This means that the structure and data within your files has been irrevocably changed, you will not be able to work with them, read them or see them. It is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
 Especially for you, on our server was generated the secret key pair RSA-2048 - public and private. All your files were encrypted with the public key, which has been transferred to your computer via the Internet. Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
 Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining this private key will be changed. If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <https://12bocejargnqum.browser.com/mq>
2. <https://12bocejargnqum.browser.com/mq>
3. <https://12bocejargnqum.browser.com/mq>

If for some reasons the addresses are not available, follow these steps:

1. Download and install the browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: <https://12bocejargnqum.browser.com/mq>
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: [\[redacted\]](#)
 Your Personal PAGE(using TOR): [\[redacted\]](#)
 Your personal code if you open the site (or TOR) directly: [\[redacted\]](#)

Your files are encrypted.
 You did not pay time for decryption, that's why the decryption price increases 2 times. At the moment, the cost of decrypting your files is 1000 USD/EUR. In case of failure to 06/06/14, 02:05 your key will be deleted permanently and it will be impossible to decrypt your files.

Your system: Windows XP (32) File server: [redacted]

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter, which is allow to decrypt and return control to all your encrypted files. How to buy CryptoWall decrypter?

bitcoin

1. You should register Bitcoin wallet ([click here for more information with pictures](#))
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day. Here are our recommendations:
 - [Coinbase](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
 - [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly
 - [go2bitcoins.com](#) - Another fast way to buy bitcoins
 - [bitbuyers.com](#) - Buy Bitcoins instantly for Cash
 - [Buy to Buy Bitcoins](#) - An international directory of bitcoin exchanges.
 - [Cash into Bitcoin](#) - Bitcoin for cash
 - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site
 - [BitStamp.net](#)
 - [BitFlood.com](#)
 - [BitStamp](#) - BitStamp is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.59 BTC to Bitcoin address: [\[redacted\]](#) [Get QR code](#)
4. Enter the Transaction ID and select amount: [Cancel](#)

Note: Transaction ID - you can find it in detailed view about transaction you made (example: 442148a156c23255b8120a42d341a27142571e10a2ac511441c)

5. Please check the payment information and click "PAY".

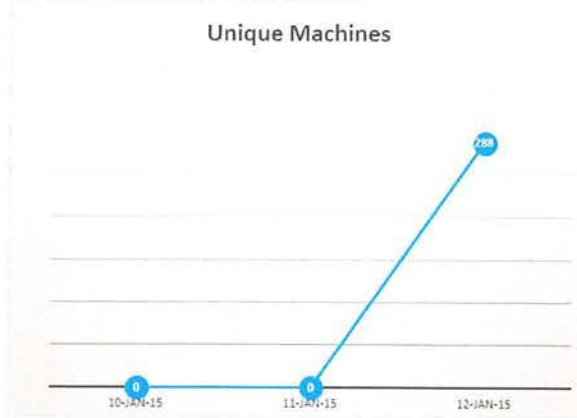
[PAY](#)

Your used drafts			
Num.	id# type	Link number of transaction ID	Amount
1	044306		1000

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 1000 USD/EUR.

Crowti also deletes shadow files to stop you from restoring your files from a local backup.

In early 2015, we saw an increase in Crowti detections:



Crowti uses the following file names for its ransom note, which contains instructions on how to decrypt your files:

- DECRYPT_INSTRUCTION.HTML
- DECRYPT_INSTRUCTION.TXT
- HELP_DECRYPT.HTML
- HELP_DECRYPT.PNG
- HELP_DECRYPT.TXT
- HELP_DECRYPT.URL

The following are examples of some of the ransom notes:

HELP_DECRYPT.HTML

What happened to your files?
 All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
 More information about the encryption keys using RSA-2048 can be found here: http://www.cryptowall.com/RSA_2048key.htm

What does this mean?
 This means that the structure and data within your files have been irrevocably changed. you will not be able to work with them. read them or see them. It is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
 Especially for you, our server was generated the secret key pair RSA-2048 - public and private.
 All your files were encrypted with the public key, which has been transferred to your computer via the internet.
 Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
 Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
 If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page. there are a few different addresses pointing to your page below:

1. [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
2. [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
3. [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)

If for some reasons the addresses are not available, follow these steps:

1. Download and install the browser: [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
 Your Personal PAGE: [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
 Your Personal PAGE (using TOR): [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
 Your personal code (if you open the site (or TOR's) directly): [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)

HELP_DECRYPT.PNG

What happened to your files?
 All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.
 More information about the encryption keys using RSA-2048 can be found here: http://www.cryptowall.com/RSA_2048key.htm

What does this mean?
 This means that the structure and data within your files have been irrevocably changed. you will not be able to work with them. read them or see them. It is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
 Especially for you, our server was generated the secret key pair RSA-2048 - public and private.
 All your files were encrypted with the public key, which has been transferred to your computer via the internet.
 Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
 Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
 If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page. there are a few different addresses pointing to your page below:

1. [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
2. [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
3. [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
4. [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)

If for some reasons the addresses are not available, follow these steps:

1. Download and install the browser: [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
 Your Personal PAGE: [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
 Your Personal PAGE (using TOR): [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)
 Your personal code (if you open the site (or TOR's) directly): [http://www.cryptowall.com/decrypt/yourpersonalcode.html](#)

HELP_DECRYPT.TXT



Related information

- [Six tips to help you stay safer online](#) provides basic guidance on protecting devices, information, and your family on the Internet.
- [How to recognize phishing email messages, links, or phone calls](#) provides basic guidance on discerning suspicious emails, and how to avoid its scams.
- [The dangers of opening suspicious emails: Crowti ransomware](#) explains the typical infection chain, encryption process, and what you can do to avoid falling into its trap.
- [Crowti update - CryptoWall 3.0](#) details the recent Crowti activity.

Analysis by Marianne Mallen

Symptoms

The following can indicate that you have this threat on your PC:

- You cannot open the following types of files:

• .asp	• .gif	• .pem
• .ass	• .h	• .pl
• .ava	• .hpp	• .png
• .avi	• .jpg	• .ppt
• .bay	• .js	• .ps
• .bmp	• .key	• .py
• .c	• .lua	• .RAW
• .cer	• .m	• .rm
• .cpp	• .mp3	• .rtf
• .crt	• .mpg	• .sql
• .cs	• .msg	• .swf
• .db	• .obj	• .tex
• .der	• .odt	• .txt
• .doc	• .PAS	• .wb2
• .DTD	• .pdb	• .wpd
• .eps	• .pdf	• .xls
- You have these files:
 - `c:\<random name>\<random name>.exe`
 - `APPDATA%\<random name>.exe`
 - `<start menu>\programs\startup\<random name>.exe`
 - `HELP_DECRYPT.HTML`
 - `HELP_DECRYPT.PNG`
 - `HELP_DECRYPT.TXT`
 - `HELP_DECRYPT.URL`
 - `DECRYPT_INSTRUCTION.HTML`
 - `DECRYPT_INSTRUCTION.TXT`
- You see these entries or keys in your registry:
 - In subkey: `HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\Run`
Sets value: "`<random name>`"
With data: "`c:\<random name>\<random name>.exe`"
 - In subkey: `HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\Run`
Sets value: "`<random name>`"
With data: "`c:\<random name>\<random name>.exe`"
 - In subkey: `HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\RunOnce`
Sets value: "`<random name>`"
With data: "`c:\<random name>\<random name>.exe`"

- You see one of these lock screens:

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here http://en.wikipedia.org/wiki/RSA_encryption

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them. It is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, our server generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

- [1. http://www.win32crowti.com/decryptor.html](http://www.win32crowti.com/decryptor.html)
- [2. http://www.win32crowti.com/decryptor.html](http://www.win32crowti.com/decryptor.html)
- [3. http://www.win32crowti.com/decryptor.html](http://www.win32crowti.com/decryptor.html)

If for some reasons the addresses are not available, follow these steps:

- Download and install Tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
- After a successful installation, run the browser and wait for initialization.
- Type in the address bar: `http://www.win32crowti.com/decryptor.html`
- Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: <http://www.win32crowti.com/decryptor.html>
Your Personal PAGE(Using TOR): <http://www.win32crowti.com/decryptor.html>
Your personal code (if you open the site (or TOR) directly): `...`

All files including videos, photos and documents on your computer are encrypted by CryptoDefense Software.
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 month. After that, nobody and never will be able to restore files.

In order to decrypt the files, open your personal page on the site <http://www.win32crowti.com/decryptor.html> and follow the instructions.

If `https://www.win32crowti.com/decryptor.html` is not opening, please follow the steps below:

- You must download and install this browser: <http://www.torproject.org/projects/torbrowser.html.en>
- After installation, run the browser and enter the address:
- Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

IMPORTANT INFORMATION:

Your Personal PAGE: <http://www.win32crowti.com/decryptor.html>
Your Personal PAGE(Using TorBrowser): <http://www.win32crowti.com/decryptor.html>
Your Personal CODE(if you open site directly): `...`

Your files are encrypted.
You did not pay in time for decryption, that's why the decryption price increases 2 times. At the moment, the cost of decrypting your files is 1000 USD/EUR. In case of failure to 06/09/14 - 02:05 your key will be deleted permanently and it will be impossible to decrypt your files.

Your system: Windows XP (x32) - First connect IP: <http://www.win32crowti.com/decryptor.html>

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We present a special software - CryptoWall Decrypter - which is able to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

bitcoin

- You should register Bitcoin wallet ([click here for more information with pictures](#))
- Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
 - Here are our recommendations:
 - [Coinbase](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
 - [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly
 - [Cryptsy.com](#) - Another fast way to buy bitcoin
 - [Bitcoin.de](#) - Buy Bitcoins instantly for Cash
 - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
 - [Cash to Bitcoin](#) - Bitcoin for cash
 - [Coinstar](#) - Coinstar allows direct bitcoin purchases on their site
 - [Bitstamp.com](#)
 - [Bitcoin.com](#)
 - [Daxx](#) - Daxx is a global cash payment network, enabling consumers to pay for digital currency.
- Send 1.59 BTC to Bitcoin address: [View QR Code](#) [Get QR Code](#)
- Enter the Transaction ID and select amount:

Note: Transaction ID - you can find it in explorer info about transaction you made (example: 4b21484b8e030398803042950416a27a2c7050f42a20311414141C)

- Please check the payment information and click "PAY".

Your best drafts				
Num	Card type	Card number (or check card ID)	Amount	Status
1	Discover	00000000000000000000000000000000	1000	OK (14)

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 1000 USD/EUR

Prevention

Take these steps to help prevent infection on your PC.

[Top](#)

[Provide feedback](#)

Other Microsoft sites

-  [Windows](#)
-  [Office](#)
-  [Surface](#)
-  [Windows Phone](#)
-  [Mobile devices](#)
-  [Xbox](#)
-  [Skype](#)
-  [MSN](#)
-  [Bing](#)
-  [Microsoft Store](#)

Downloads

- [Download Center](#)
- [Windows downloads](#)
- [Office downloads](#)

Support

- [Support home](#)
- [Knowledge base](#)
- [Microsoft community](#)

About

- [The MMPC](#)
- [Evaluating our protection](#)
- [MMPC Privacy Statement](#)
- [Microsoft](#)
- [Careers](#)
- [Citizenship](#)
- [Company news](#)
- [Investor relations](#)
- [Site map](#)

Popular resources

- [Security and privacy blogs](#)
- [Security Response Center](#)
- [Security Intelligence Report](#)
- [Microsoft Safety & Security Center](#)
- [Malware Protection Center](#)
- [Security for IT Pros](#)
- [Security for developers](#)
- [Trustworthy Computing](#)