EXHIBIT 10

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.AHIO!tr (Fortinet)
PWSZbot-FBKQ!86B6EE398F44 (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

Microsoft

Contact Us | Terms of Use | Trademarks | Privacy & Cookies | About our ads

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-<randomnumber>.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:

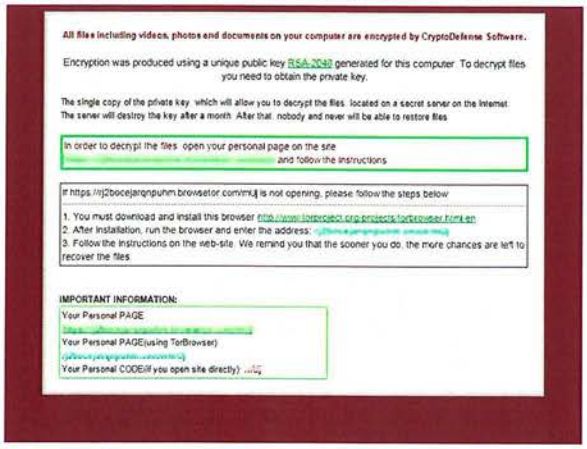
- .asp
- .ass
- .ava
- .avi
- .bay
- .bmp
- .c
- .cer
- .cpp
- .crt
- .cs
- .db
- .der
- .doc
- .DTD
- .eps
- .gif
- .h
- .hpp
- .jpg
- .js
- .key
- .lua
- .m
- .mp3
- .mpg
- .msg
- .obj
- .odt
- .PAS
- .pdb
- .pdf
- .pem
- .pl
- .png
- .ppt
- .ps
- .py
- .RAW
- .rm
- .rtf
- .sql
- .swf
- .tex
- .txt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

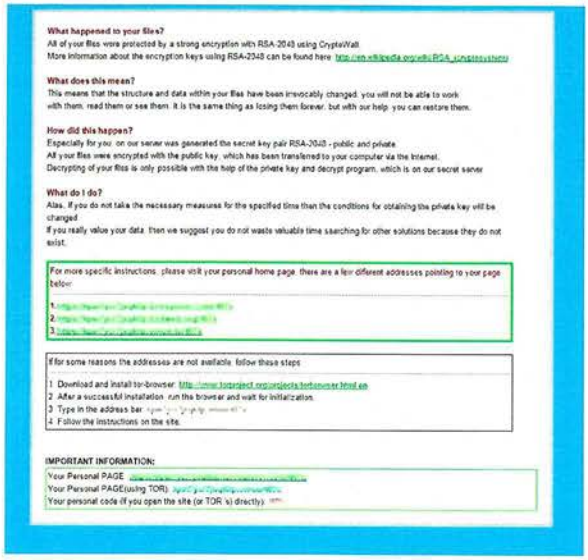
It does not rename the files it encrypts, it just overwrites them. So you may not realise the file is encrypted until you try to open it.

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)

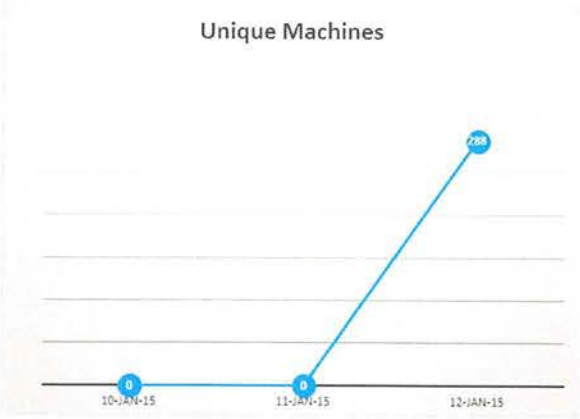
It then displays a lock screen similar those shown below to tell you that you can recover the files using a personal link that directs you to a Tor webpage asking for payment using BitCoin as currency.





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:

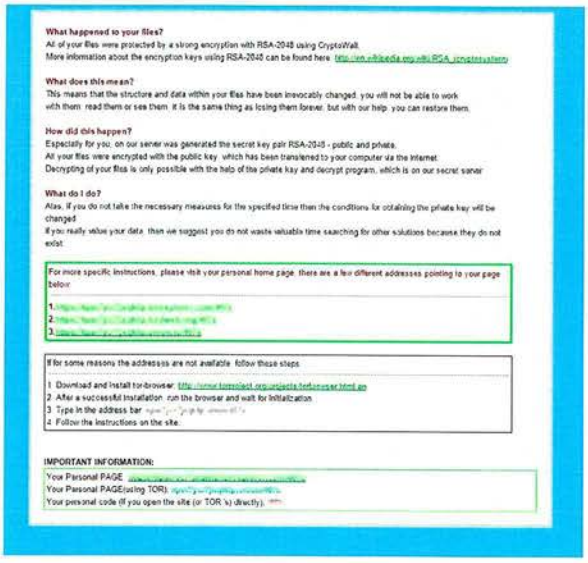


Crowti uses the following file names for its ransom note, which contains instructions on how to decrypt your files:

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

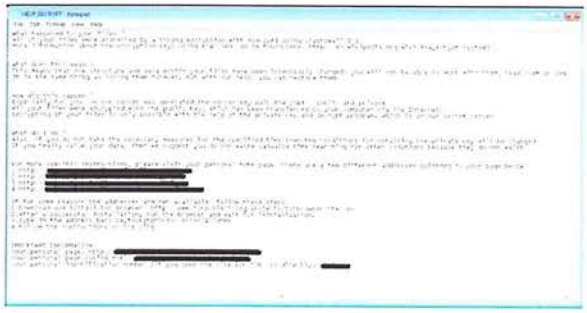
The following are examples of some of the ransom notes:

HELP_DECRYPT.HTML



HELP_DECRYPT.PNG

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.

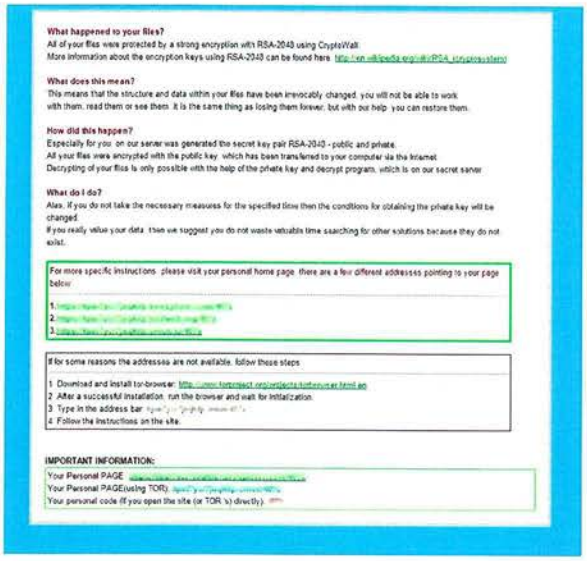
Analysis by Marianne Mallen

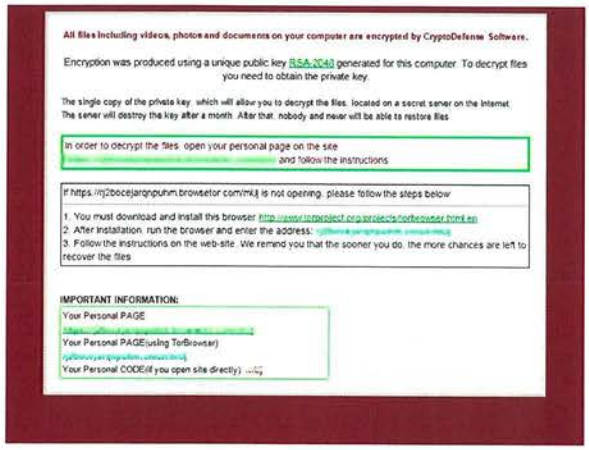
Symptoms

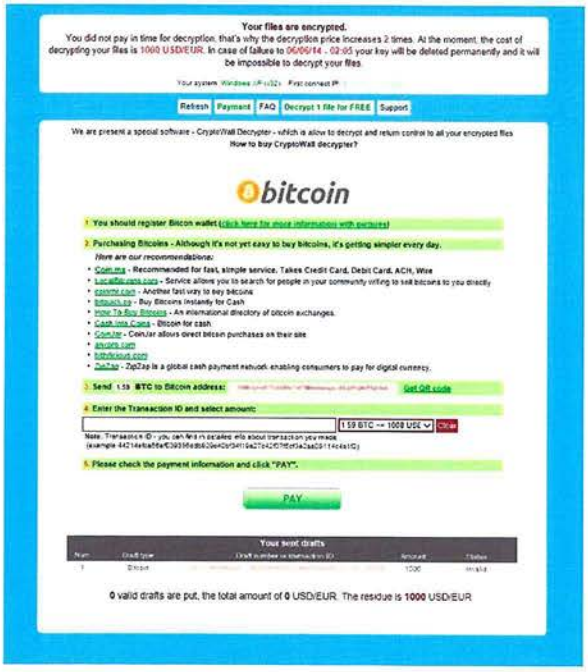
The following can indicate that you have this threat on your PC:

- You cannot open the following types of files:
  - .asp
  - .ass
  - .ava
  - .avi
  - .bay
  - .bmp
  - .c
  - .cer
  - .cpp
  - .crt
  - .cs
  - .db
  - .der
  - .doc
  - .DTD
  - .eps
  - .gif
  - .h
  - .hpp
  - .jpg
  - .js
  - .key
  - .lua
  - .m
  - .mp3
  - .mpg
  - .msg
  - .obj
  - .odt
  - .PAS
  - .pdb
  - .pdf
  - .pem
  - .pl
  - .png
  - .ppt
  - .ps
  - .py
  - .RAW
  - .rm
  - .rtf
  - .sql
  - .swf
  - .tex
  - .txt
  - .wb2
  - .wpd
  - .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:







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

Microsoft

Contact Us | Terms of Use | Trademarks | Privacy & Cookies | About our ads