# The Philadelphia Ransomware offers a Mercy Button for Compassionate Criminals

bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals

By
Lawrence Abrams

- September 8, 2016
- 05:43 PM
- 0

A new version of the Stampado ransomware called Philadelphia has started being sold for $400 USD by a malware developer named The Rainmaker, According to Rainmaker, Philadelphia is being sold as a low cost ransomware solution that allows any wannabe criminal to get an advanced ransomware campaign up and running with little expense or complexity.

On closer look, though, the Philadelphia Ransomware is not as sophisticated as advertised. As it is programmed in the AutoIT scripting language, it can be decompiled and analyzed for weaknesses. On closer inspection, Fabian Wosar of Emsisoft is confident that it can be decrypted.


**Lock Screen**

I was first notified of this new version by a poster in the forums who claimed he was able to intercept communications between a person going by the handle of SkrillGuide2015 and the Philadelphia developer The Rainmaker. This conversation was taking place on the AlphaBay Tor criminal site, and shows Rainmaker explaining how he has started selling his new Philadelphia ransomware project for $400 USD and that he plans on starting to distribute it today. Rainmaker's goal was to infect 20 thousand victims on his first day of distribution.

According to Rainmaker, Philadelphia "innovates" the ransomware market with features such as autodetecting when a payment has been made and then automatically decrypting, infecting USB drives, and infecting other computers over the network. Of particular note, is a Mercy Button that allows a compassionate criminal to automatically decrypt a particular victim's files for free. In order to demonstrate this new ransomware, Rainmaker has created a PDF showing its capabilities.

The advertised features are:

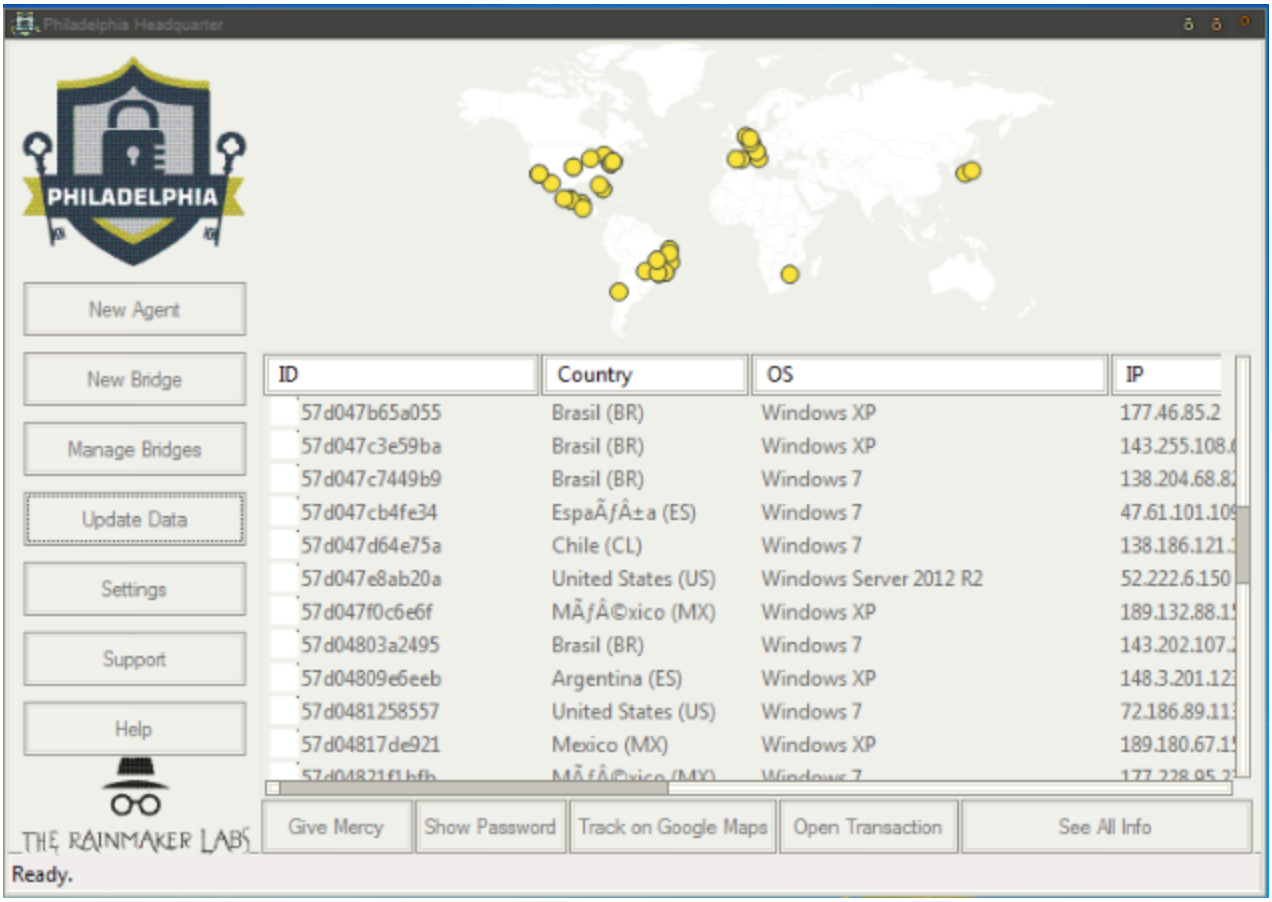
> Everything is customisable:
>
> - You can set the folders where the Ransomware will look for files as well as the depth/recursion level
> - You can set the extensions, you can enable, disable and define intervals for the deadline and the russian roulette (as well as editing how many files are deleted on every russian roulette interval and whether the files or the crypt key gets deleted once the deadline ends
> - You can edit file icon and Mutex
> - You can edit the UAC (user access control) in four available options: (1) do not ask for admin privilleges; (2) ask and insist until it is given; (3) ask but run anyway even if it is not given; (4) ask and give up if it is not given
> - You can edit all the interface texts as well as add multiple languages to the same file (it will detect the machine language and display the texts you edited for that locale or a default/fallback one)
> - You can enable or disable USB infect, network spread and Unkillable Process, as well as set the process name
>
> The Philadelphia Headquarter is a software that works on your machine and allows you to generate unlimited builds, see the victims on a map and on a list (with country flags and all the data you need) and also a "Give Mercy" button if you're too good 0:)
>
> But the coolest Philadelphia feature (and what makes its maintenance so cheap) is that, instead of huge servers on our controls where you must pay high amounts monthly, we present you the "Bridges". Bridges are the way victims and attacker enters in touch in a distributed network. It's simply a PHP script that uses itself as database (no MySQL or whatever needed, just PHP). Bridges store the clients keys, verifies payments and provide the victims informations to the headquarters safely. And they can be hosted on nearly any server: even hacked servers, shared hosting (free hosting works but it is not recommended as they can delete your account if it's not a fully functional website), dedicated or VPS (recommended for bigger attacks, although the requests are small and are only done a few times). As the bitcoin payment verification is done on the server side, by the bridge, there is no way to spoof it on the victim machine. Also, the distributed bridges network will grant a better anonimity.
>
> Everything very well documented on a plain-english help file!
>
> Prints: https://www.docdroid.net/vJV82cC/philadelphia-prints.pdf.html

Though the bridges + headquarters client looks interesting, it has some serious flaws as described in the next section.

## Taking a Bridge to the Headquarters

For an attacker to setup a Philadelphia campaign, they need to install a PHP scripts called Bridges on web sites. These Bridges will be connected to by the ransomware infection and will store the encryption key and information about the victim. They are also used by the ransomware to check if a ransom payment has been made.

The attacker then runs a management client called the Philadelphia Headquarters on their machine, which will connect to each configured bridge and download the victim data to their management console. This client allows the attacker to see who is infected, what countries have the most infections, and even offers a mercy button if a compassionate attacker wants to allow someone to decrypt their files for free.




**Philadelphia Headquarters Management Console**

There is a fundamental problem, though, with this Bridge implementation. Unless these bridges are stored on anonymous networks like TOR, they will most likely be discovered and taken down fairly quickly. As the addresses to these bridges are hard coded into the ransomware, once the bridge is disabled, a victim no longer has the ability to pay the ransom or decrypt their files.  For this implementation to really work, an attacker would need to setup bridges using Tor, which increases the complexity of the setup.

## Another malware dev unhappy with Researcher Fabian Wosar

The first two versions of Stampado were able to be decrypted by Fabian Wosar of Emsisoft and it also appears that this new Philadelphia variant is no exception. Like the Apocalypse Ransomware developer, Rainmaker has not taken kindly to Fabian's attention as can be seen by a note left in the ransomware's AutoIT script.

```
Func _h3($al)
   Return StringTrimLeft(_6("fuck you fabian" & $al, $n), 2)
EndFunc
```

**Insulting Fabian Wosar in the Code**

## How the Philadelphia Ransomware Encrypts a Victim's Files

Based on images and a mailing list software found on one of the Bridges, I believe that this ransomware is distributed through phishing emails that pretend to be an overdue payment notice from Brazil's Ministério da Fazenda, or the Ministry of Finance. You can see an example of the fake notice found on one of the Bridges below.

MINISTÉRIO DA FAZENDA
SECRETARIA DA RECEITA FEDERAL
DEFIC RIO DE JANEIRO

Defic/RJO
002
ISABEL CRISTINA MARINHO
Mat. 82473

MANDADO DE PROCEDIMENTO FISCAL - DILIGÊNCIA Nº 07.1.90.00-2005-01708-9

CONTRIBUINTE/RESPONSÁVEL
CNPJ/CPF: 33.252.156/0001-19
NOME EMPRESARIAL/NOME: TV GLOBO LTDA
ENDEREÇO:R LOPES QUINTAS, 303 COMPLEMENTO:
BAIRRO: JARDIM BOTANICO UF: RJ
MUNICÍPIO: RIO DE JANEIRO CEP:22.460-010

PROCEDIMENTO FISCAL: DILIGÊNCIA
DESCRIÇÃO SUMÁRIA: ACOMPANHAMENTO/CONSTATAÇÃO PREVISTOS NA LEGISLAÇÃO TRIBUTÁRIA

AUDITOR-FISCAL DA RECEITA FEDERAL — MATRÍCULA
ANTONIO CESAR VALERIO DA SILVA 0056806
ALBERTO SODRE ZILE 0028032 SUPERVISÃO

ENCAMINHAMENTO

Determino, nos termos da Portaria SRF nº 3.007, de 26 de novembro de 2001, alterada pela Portaria SRF nº 1.238, de 31 de outubro de 2002, e pela Portaria SRF nº 1.468, de 6 de outubro de 2003, a execução do procedimento fiscal definido pelo presente Mandado, que será realizado pelo(s) Auditor(es)-Fiscal(is) da Receita Federal (AFRF) acima identificado(s), que está(ão) autorizado(s) a praticar, isolada ou conjuntamente, todos os atos necessários a sua realização.

Este Mandado deverá ser executado até 30 de Setembro de 2005. Este instrumento poderá ser prorrogado, a critério da autoridade outorgante, em especial na eventualidade de qualquer ato praticado pelo contribuinte/responsável que impeça ou dificulte o andamento deste procedimento fiscal, ou a sua conclusão.

RIO DE JANEIRO, 01 de Agosto de 2005.

WILSON FERNANDES GUIMARAES - Matrícula : 0015325
DELEGADO(A) DA RECEITA FEDERAL
DEFIC RIO DE JANEIRO

CIÊNCIA DO CONTRIBUINTE RESPONSÁVEL

Declaro-me ciente deste Mandado, do qual recebi cópia.

**SPAM Notice**

These phishing emails most likely contain a link back to the top level folder of the Bridge, which contains a Java program that automatically downloads and executes the installer for the Philadelphia ransomware.

When the ransomware is started, it will load an embedded configuration file that contains directives as to how the ransomware should encrypt a computer. The ransomware currently being distributed will target fixed, removable, and network drives, and drive root folders. When encrypting files it will use a custom encryption algorithm and target the following files:

```
*.7z;*.asp;*.avi;*.bmp;*.cad;*.cdr;*.doc;*.docm;*.docx;*.gif;*.html;*.jpeg;*.jpg;*.mdb
```

When a file is encrypted, its name will be scrambled and have the .locked extension appended to it. For example, test.jpg may become 7B205C09B88C57ED8AB7C913263CCFBE296C8EA9938A.locked.

When it is finished it will display the lock screen shown below.


**Lock Screen**

Last, but not least, if Russian Roulette is enabled, a counter will begin and when it runs down to zero, a certain preconfigured amount of files will be deleted.

As already said, this ransomware is most likely decryptable for free. So if you are infected with Stampado, or this Philadelphia variant, please do not pay the ransom. Instead, you should ask for help in our Stampado Ransomware Help & Support Topic.

## Files associated with the Philadelphia Ransomware:

```
%UserProfile%\[random]
%UserProfile%\[random]
%UserProfile%\Isass.exe
```

## Registry entries associated with the Philadelphia Ransomware:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Update
%UserProfile%\Isass.exe
```

## Network Communication:

```
http://sshtunnel.at
```

## IOCs:

```
Nov.peg - SHA256: 812ddd619e12fb2c90c8395fd02fe12638e997a29f86f7d39e42d50de832d4f0
Downloader - SHA256: ea75b18697b819e6d1d159fc3a0477870f1be7e6ca498a67eb797a829a9b1d7d
```

- Philadelphia
- Ransomware
- Stampado

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article



## You may also like: