Philadelphia Ransomware Brings Customization to Commodity Malware

proofpoint.com/us/threat-insight/post/philadelphia-ransomware-customization-commodity-malware

April 25, 2017

Blog
Threat Insight
Philadelphia Ransomware Brings Customization to Commodity Malware

April 25, 2017 Proofpoint Staff

Overview

Philadelphia ransomware is a relatively new ransomware variant, first observed in September of last year. Designed as an easy-to-use piece of malicious software with low barriers to entry for new ransomware actors, Philadelphia is simple to customize and deploy. Although we most often associate ransomware, including Philadelphia, with large-scale, "spray and pray" campaigns that send high message volumes to a wide spectrum of consumers and organizations, we are beginning to see significant differentiation among attacks, ransoms, scale, and even targeting.

In this blog, we focus on a recent Philadelphia ransomware campaign used in a series of targeted email attacks against a small number of organizations using lures and attachments highly customized for the targeted organizations. In addition to explicit targeting, recent attacks using Philadelphia highlight the ability to customize what is essentially commercial off-the-shelf (COTS) malware, personalizing aspects of attacks such as the ransom note and ransom amounts.

Analysis

Since late last month, we have seen actors using Philadelphia to target specific healthcare institutions, among other organizations in the same city. In this case, email messages purporting to be from an employee at a targeted company with subjects such as "Patient Referral" contained bit.do (URL shortener) links leading to the download of Philadelphia.

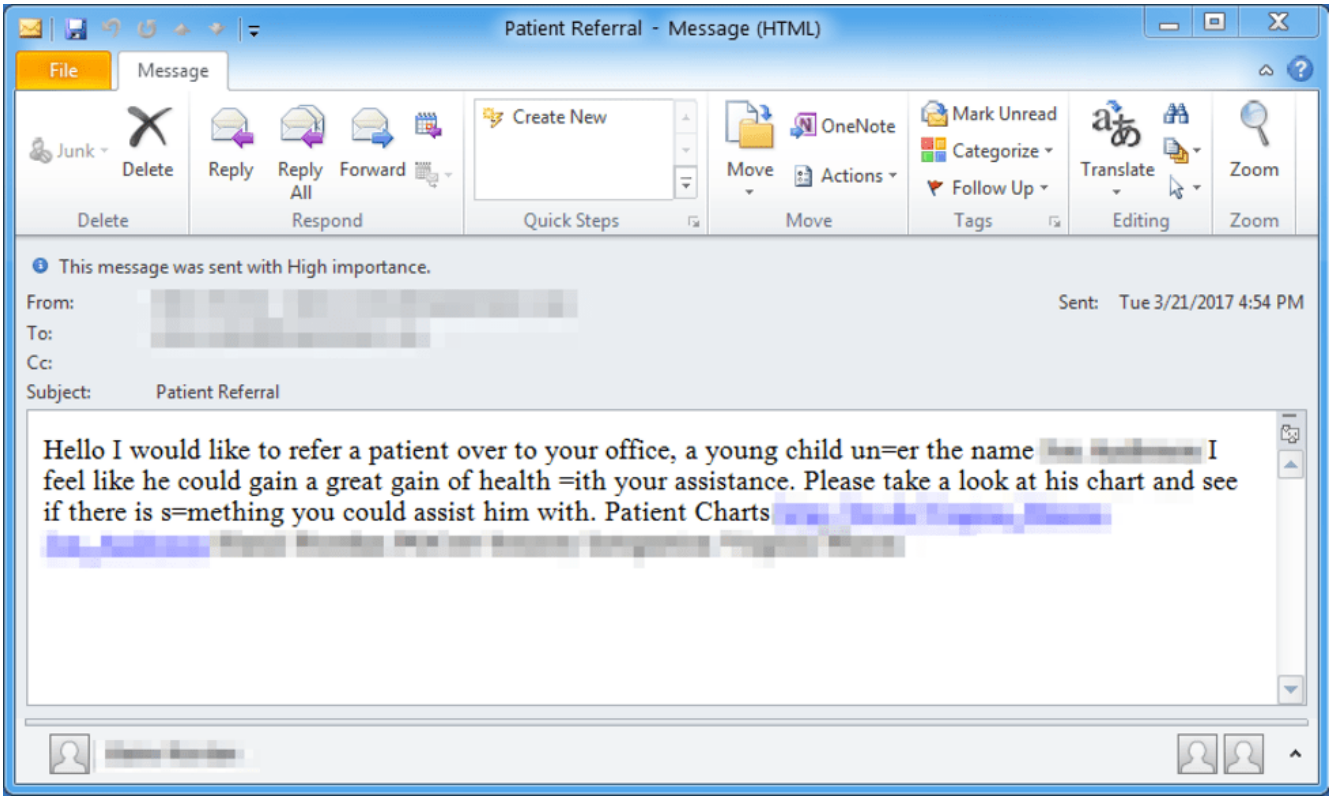

Figure 1: Email sample with patient referral lure

Although redacted in Figure 1, the use of so-called "display name spoofing" to make the emails appear to be from internal senders is a technique commonly associated with targeted attacks and has been on the rise among business email compromise (BEC) actors.

Additionally, the actor took an extra step to customize the ransom note by:

(1) Calling out the potential victim organization by name
(2) Setting the ransom to a high amount of 15 Bitcoins (approximately $18,000 USD) and
(3) Threatening to delete 99 files every 45 minutes

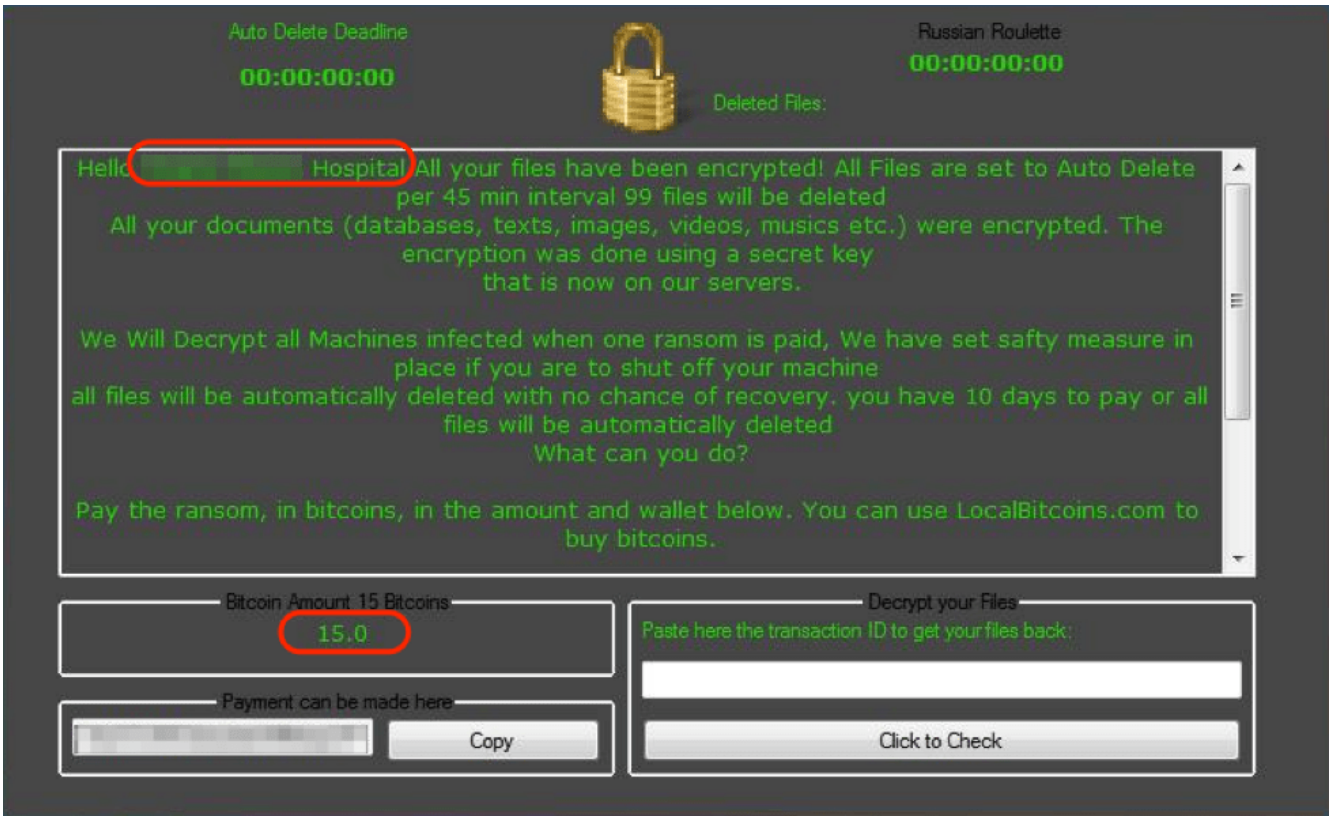

Figure 2: Customized ransom note

Ransom Note Customizations

We determined that the demanded ransom amount is configurable and is returned in the command and control (C&C) server response to the initial check-in beacon by the victim machine. The Bitcoin address and victim ID are returned in the same response. However, this is the first instance of ransom note customization we have observed with Philadelphia ransomware. This customization occurs through a setting that is built into the malware itself. Examining our malware corpus, we found several other instances of ransom note customization for Philadelphia ransomware, tailored to a variety of different situations.

In one case, the ransom note was colored pink and included a small payoff amount of 0.05 Bitcoins. The note threatened the victim, claiming “YOU HAVE BEEN EXPOSED!” and that three files will be deleted every hour, ostensibly as a consequence for browsing pornography. At this time, we have not determined how this particular instance of Philadelphia ransomware was spread to potential victims.

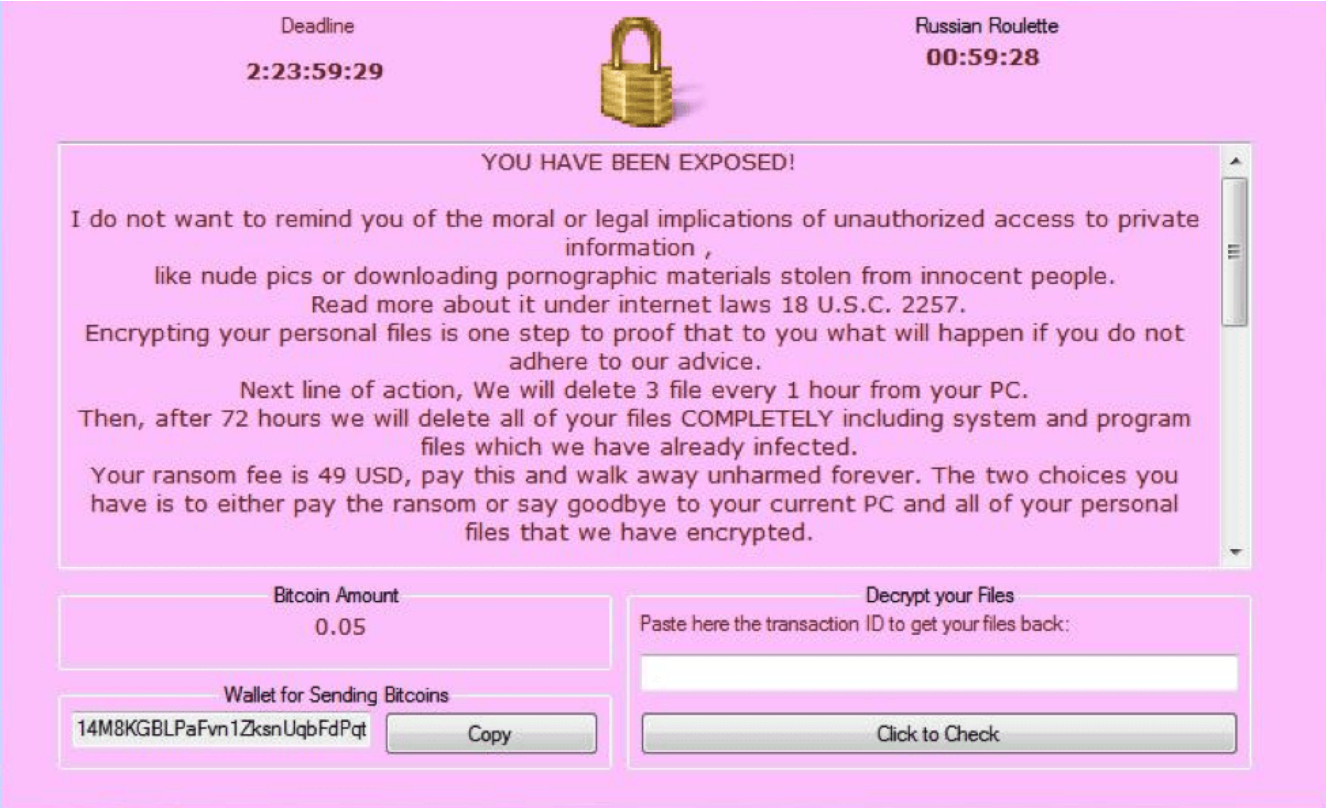

Figure 3: Pink ransom note displayed by a sample with SHA256 hash of a1e1b22f907b4b5d801e7c1dd3855d77bf28831eaadc2fbf9ed16ee0cdcc8ccf

In another case, we found a sample with a Russian-language ransom note. The English translation (see full text in Appendix A) told victims “Do not write to us if you do not like the price. We do not bargain.”

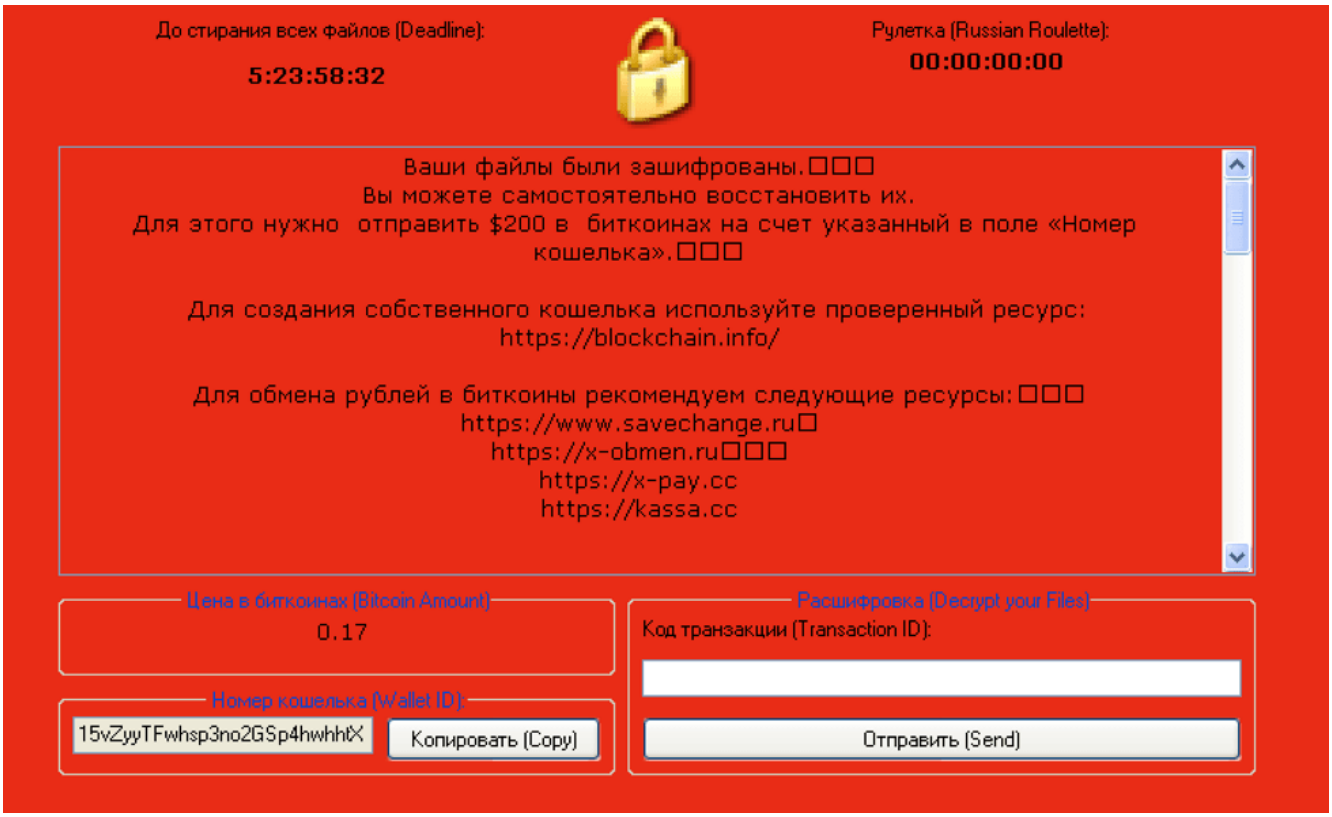

Figure 4: Red ransom note displayed by a sample with SHA256 hash of 55793f2cd2a061646e73f0520f5f43a82da1c890624c0317777d5917efe68761

Delivery

As in the healthcare-targeted campaign, we have seen Philadelphia ransomware spreading via URLs linking to zipped executables in email. A related healthcare campaign from the same actor also targeted hospitals with URLs, but in that case led to macro-laden Microsoft Word documents.

We also found a sample of a Microsoft Word document named CV.doc (Figure 5) that used macros and Powershell to download Philadelphia from a payload site.

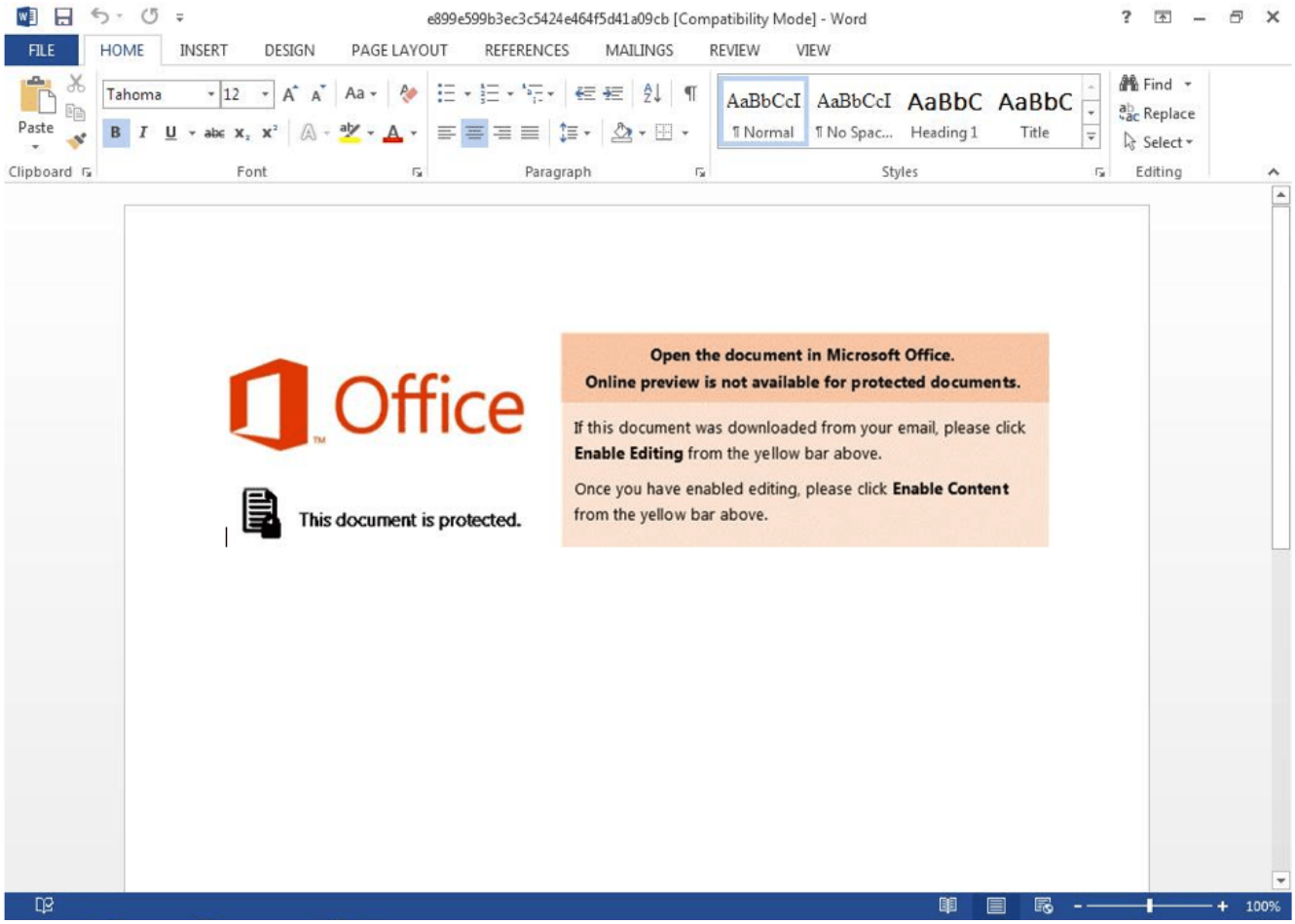

Figure 5: Document attachment sample with SHA256 hash of 6c852f2dcd2189f2c24c7b779dce62b114b293b983b5daa0858f7648af4a5424, which downloads the final payload

It appears that Philadelphia is also spread via keygen and cracking sites as we found samples of the ransomware bundled with various keygen programs and Bitcoin-related software.

Figure 6: The ransomware sample with SHA256 of e5d52926187e2b4b3086b14fe718d1896516a6d99e20efeb77e44b25e2f3de3e) is bundled with this keygen program

Figure 7: The ransomware sample with SHA256 hash of a4450709af37731f17d29ddf4d83f9daafbae7dc67393e7f13fb2dcaf9a321e6 is bundled with this program

Finally, we have also observed Philadelphia being distributed via Sundown and RIG exploit kits.

Configuration File

As noted above, a server-side script controls several parameters, including the ransom amount. In Figure 8, this parameter is set to 0.2 Bitcoins. The “confirmations” parameter, shown with the value “3”, appears to be the number of times the victim has to confirm that he or she paid the ransom.

```
a: 5: {
    s: 6: "amount";
    s: 3: "0.2";
    s: 13: "confirmations";
    i: 3;
    s: 8: "increase";
    i: 1;
    s: 13: "increase_type";
    s: 1: "a";
    s: 9: "tolerance";
    s: 1: "6";
}
```

Figure 8: Example Philadelphia configuration as stored on the C&C server for the sample with SHA256 hash of b6be75155ca197c4931ed166dcc7725ad44adcfc8b9b6947f7cb69d2bf63ff64

```
HTTP/1.1 200 OK
Date: Fri, 14 Apr 2017 21:35:35 GMT
Server: Apache/2.4.10 (Debian)
Content-Length: 52
Content-Type: text/plain; charset=UTF-8

5[redacted]c|1AzT9hEww4bu3hjPeVu[redacted]|0.2
```

Figure 9: The server response to the initial victim check-in returns the victim ID, followed by a Bitcoin address (highlighted) and then by the ransom amount. In this case, the amount is 0.2 as specified in the configuration file.

Conclusion

While geographically targeted ransomware has been a part of the threat landscape for some time, targeting of ransomware at specific companies or verticals has been rare. As these recent Philadelphia ransomware examples show, even ‘entry-level’ ransomware is adopting the techniques of targeted email-based attacks, including:

- Email lures and attachment filenames customized for the targeted organization
- Spoofing to make it appear that the message was sent internally
- Customized payment amounts, deletion schedules, ransom messages, languages, and even colors per organization.

These targeted campaigns are carried out even as we continue to observe broad-based distribution of Philadelphia ransomware through both email and web-based attacks.

Ransomware can be quite lucrative for threat actors in broad-based campaigns where actors generally rely on high volumes and relatively low ransoms to monetize ransomware. However, healthcare organizations are becoming a favorite for more targeted, higher-ransom attacks as well. Philadelphia

ransomware in particular is not considered especially sophisticated in its coding or encryption but is notable for being an early example of "commodity ransomware", sold cheaply for widespread use among various threat actors. We have also observed cracked versions of Philadelphia in the wild that do not require any upfront costs for would-be ransomware actors.

Changes in the ransomware landscape are not limited to Philadelphia. For example, we have recently observed narrow-spread Sage ransomware campaigns being delivered to small numbers of organizations in a few verticals. On the other hand, Locky returned to large-scale distribution recently but in sporadic campaigns using new distribution vectors and demanding a higher ransom. In our recent first quarter Threat Report, we highlighted the continued rapid growth of ransomware variants in the wild. While many of these new variants fail to gain traction, others come with new approaches and features.

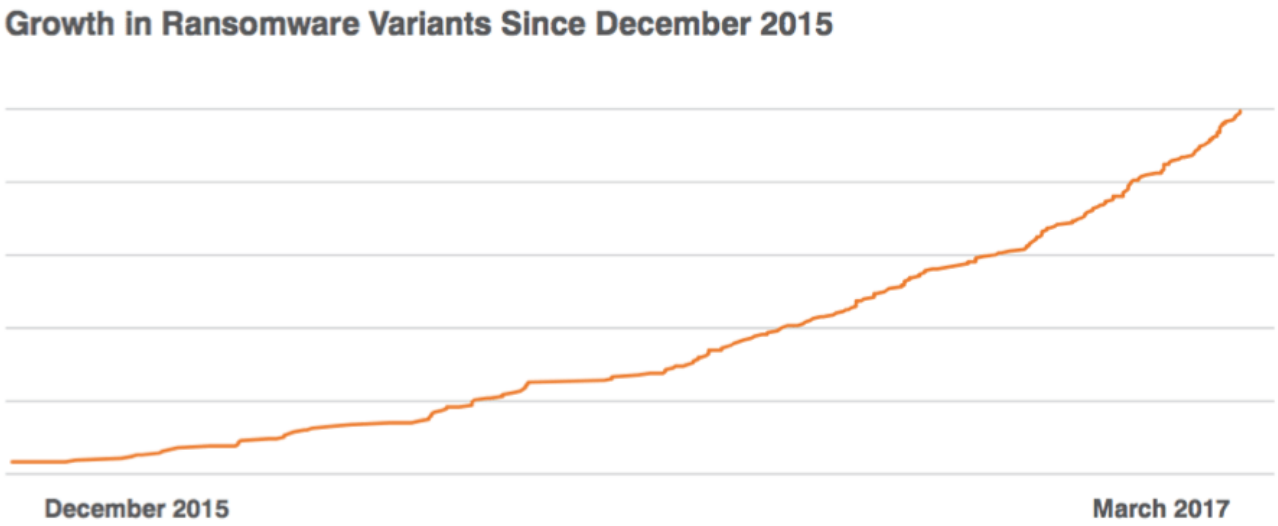

Figure 10: Indexed growth of ransomware variants reported or observed since December 2015

As commodity ransomware becomes more sophisticated and customizable, new strains emerge rapidly, and ransomware-as-a-service becomes more commonplace, the possibilities for threat actors to use this type of malware in unexpected ways increase. Organizations need to adopt robust strategies to stop ransomware messages at the door as effective attacks can have major financial impacts, both directly in terms of large ransoms and indirectly in terms of time, productivity, and effectiveness.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
a1e1b22f907b4b5d801e7c1dd3855d77bf28831eaadc2fbf9ed16ee0cdcc8ccf	SHA256	Philadelphia ransomware
6c3d69053a19e336289efbe0ee65eba1ef21076019a4b71b39bca8bd105e86cd	SHA256	Philadelphia ransomware

55793f2cd2a061646e73f0520f5f43a82da1c890624c0317777d5917efe68761	SHA256	Philadelphia ransomware
b6be75155ca197c4931ed166dcc7725ad44adcfc8b9b6947f7cb69d2bf63ff64	SHA256	Philadelphia ransomware
6c852f2dcd2189f2c24c7b779dce62b114b293b983b5daa0858f7648af4a5424	SHA256	MS Word document spreading Philadelphia
e5d52926187e2b4b3086b14fe718d1896516a6d99e20efeb77e44b25e2f3de3e	SHA256	Philadelphia bundled with keygen program
a4450709af37731f17d29ddf4d83f9daafbae7dc67393e7f13fb2dcaf9a321e6	SHA256	Philadelphia bundled with keygen program
foolonthehill[.]website	Domain	Philadelphia C&C
whole-sale-deals[.]com	Domain	Philadelphia C&C
191.101.242[.]123:53161	IP	Philadelphia C&C
95.211.147[.]156:80	IP	Philadelphia C&C

ET and ETPRO Suricata/Snort Coverage

2822596 | ETPRO TROJAN Win32/Philadelphia Ransomware Encryption Activity
2822136 | ETPRO TROJAN Win32/Philadelphia Ransomware CnC Checkin

Appendix A

Full ransom note for sample with SHA256
55793f2cd2a061646e73f0520f5f43a82da1c890624c0317777d5917efe68761

Original ransom note text:
Ваши файлы были зашифрованы.

Вы можете самостоятельно восстановить их.
Для этого нужно отправить $200 в биткоинах на счет указанный в поле «Номер кошелька».

Для создания собственного кошелька используйте проверенный ресурс:
https://blockchain.info/

Для обмена рублей в биткоины рекомендуем следующие ресурсы:
https://www.savechange[.]ru
https://x-obmen[.]ru
https://x-pay[.]cc
https://kassa[.]cc

После оплаты необходимо ввести код транзакции в поле «Код транзакции».
Затем отправить его нам, нажав кнопку «Отправить».

После получения 3-х подтверждений мы начинаем расшифровку ваших файлов.
В течение от 5 минут до часа Ваши файлы будут расшифрованы автоматически,
если компьютер будет подключен к интернету.

В случае возникновения проблем с расшифровкой обратитесь по адресу:
kenthottoren@gmail[.]com

В письме требуется указать Ваш IP-адрес и имя пользователя.
Эту информацию можно посмотреть на сайте:
http://2ip[.]ru

Не пытайтесь восстановить данные с помощью антивирусных утилит, испортите все файлы.

Если хотите попробывать, пробуйте на другом ПК и минимум файлов, иначе потом даже я не смогу помочь.

И помните пожалуйста, что цена каждый день растет.

P.S. Пишите четко, ясно, предельно понятно, учитывайте, что кроме Вас пишет много людей.

В диалоги не вступаю, работа по приницпу быстро заплатил, сразу получил.
Не устраивает цена услуги, больше не пишите.

Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.

Ransom note translation:
All the important files on your computer were encrypted.

To decrypt the files you should send $200 in Bitcoin to address written in form «Wallet ID».
To create your ouw wallet use trusted resource:
https://blockchain.info/

For currency exchange you can use follow links:
https://www.savechange[.]ru
https://x-obmen[.]ru

https://x-pay[.]cc
https://kassa[.]cc

After successfull payment, paste the transaction number in «Transaction ID» and send it to us «Send».

Within 5 minutes to an hour after payment, all your files will be decrypted automatically, but required internet access.

In case of problems, contact:
kenthottoren@gmail[.]com

We cant help you without your IP address and username. So you should put this information in your e-mail.

All the attempts of decryption by yourself will result only in irrevocable loss of your data.

Quickly paid/immediately received. Do not write to us if you do not like the price.
We do not bargain.

And please remember that the price is growing every day.

Subscribe to the Proofpoint Blog