

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $388 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaftNbBLX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
m0wsm1th123456@posteo.net. Your personal installation key:

hYH [REDACTED] 0ApN-ESERuN

If you already purchased your key, please enter it below.
Key:
```

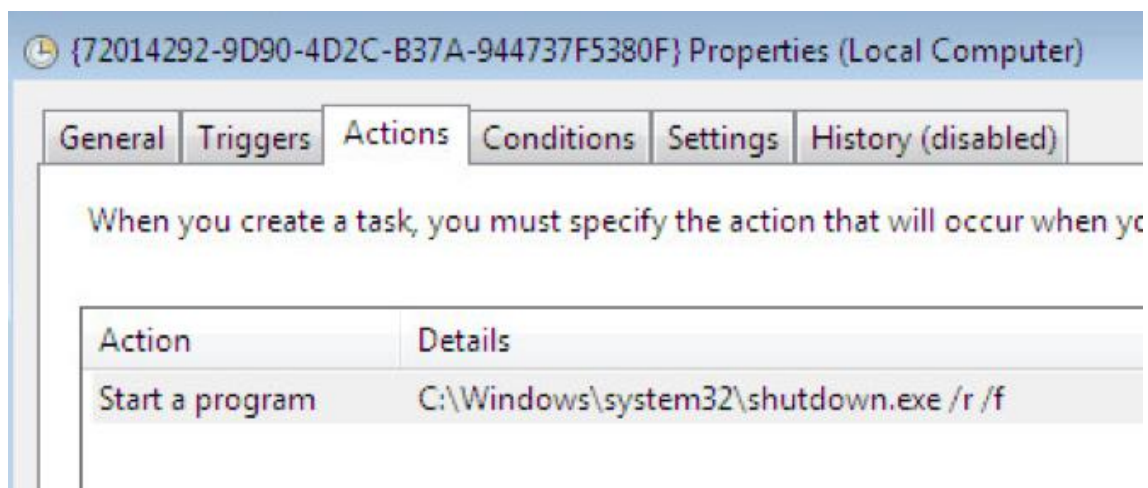
New Petya ランサムウェア攻撃を防御 2017年6月27日 Minerva のブログから

これまでにない獐猛な攻撃性を備え最も破壊的な新種ランサムウェアが登場しました。

このランサムウェアは1年前(2016年)に登場した Petya/Petwrap ファミリーに関連している亜種で、フィッシングメールなどに仕掛けられています。WannaCry と同じく、SMB プロトコルのネットワーク内に NSA ETERNALBLUE エクスプロイトをリークさせ感染が拡大していきます。

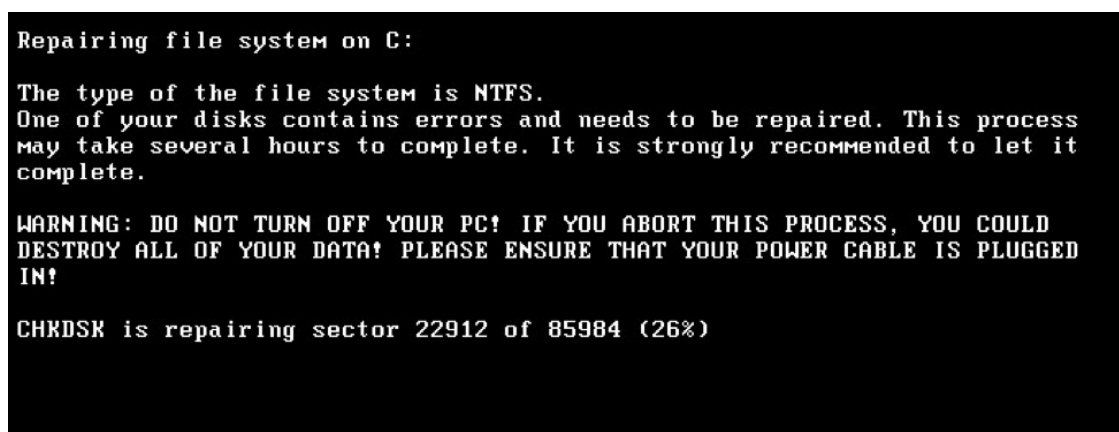
Prot...	Local ...	Remote Address	State
TCP	192.168...	192.168. [REDACTED]	96:139 SYN_SENT
TCP	192.168...	192.168. [REDACTED]	97:445 SYN_SENT
TCP	192.168...	192.168. [REDACTED]	97:139 SYN_SENT
TCP	192.168...	192.168. [REDACTED]	98:445 SYN_SENT
TCP	192.168...	192.168. [REDACTED]	98:139 SYN_SENT
TCP	192.168...	192.168. [REDACTED]	99:445 SYN_SENT

マシン感染後、ハードドライブセクターのスケジュールタスクが上書きされてしまい、1 時間以内に強制再起動してしまいます。



他の攻撃方法としては、Windows API の NtRaiseHardError を利用し、再起動を強制された後、ブルースクリーン停止状態(BSoD)に陥ります。

マシンが再起動後、偽の CHKDSK 画面が表示されます。



それからランサムノートへ画面遷移します。

```
Doops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

    1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
    wowsmith123456@posteo.net. Your personal installation key:

    hYH [REDACTED] BApN-ESERuN

If you already purchased your key, please enter it below.
Key: _
```

他のランサムウェアは被害者のファイルデータを暗号化するのとは異なり、このランサムウェアは被害者の OS レベル全てのマシンをハイジャックしてしまうので、デバイス自体が全く機能しなくなります。

今までの攻撃で 1.8 ビットコイン(当時の時価で 5000 米ドル以下)がすでにこの攻撃で 18 回のトランザクションが行われており、今後増加していくと思われます。

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX	No. Transactions	18
Hash 160	e62f3c2c154063f3e230d293701c7583f5489556	Total Received	1.88151928 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	1.88151928 BTC
		Request Payment	Donation Button



Minerva は New Petya 攻撃を防御

Minerva 製品は Petya の悪意のあるインジェクション攻撃の段階で先制防御するので、全体の攻撃から防御することが可能です。Minerva のテクノロジーはマルウェアが検知を回避しようとする段階で、実行をストップさせます。今回の Petya 攻撃のみならず、多種多様なメモリーインジェクション攻撃やファイルレス攻撃においても Minerva は先制防御できる製品です。

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。