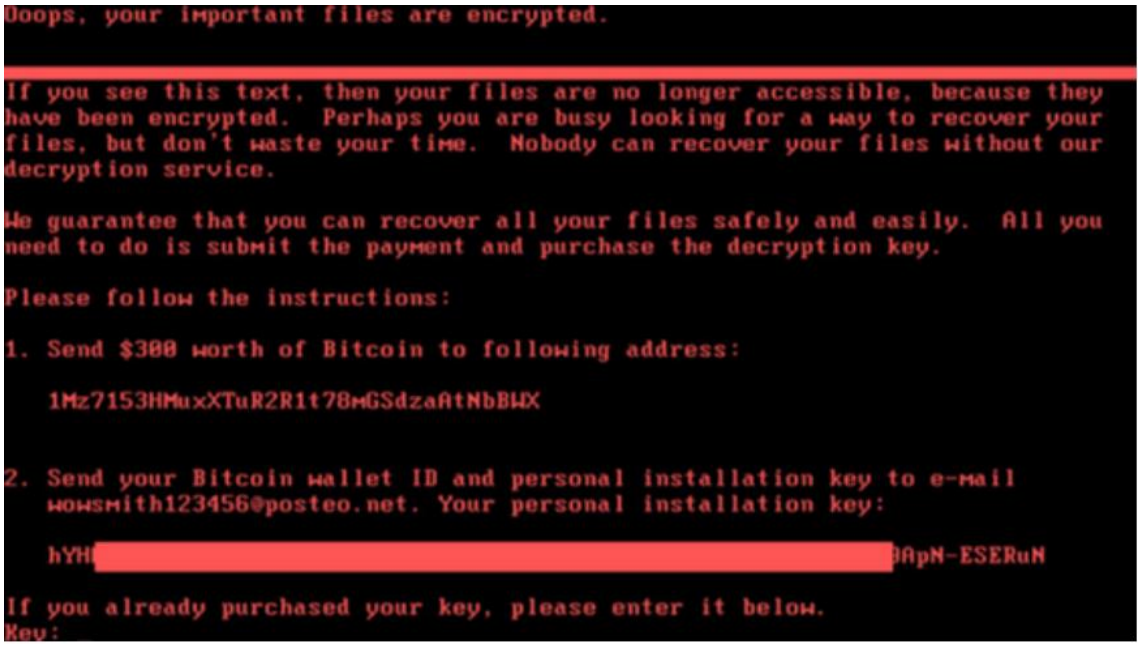
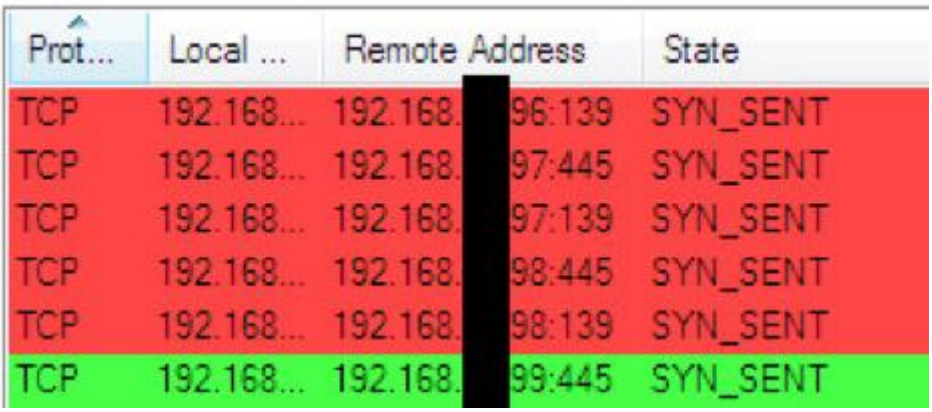


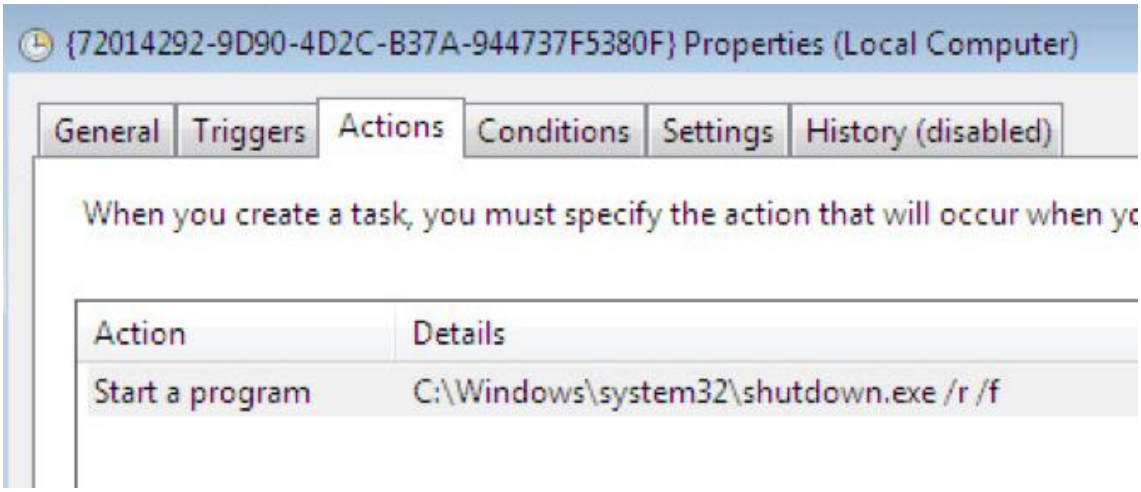
New Petya ランサムウェア攻撃を防御
2017 年 6 月 27 日 Minerva のブログから

これまでにない獰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 プロトコー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。

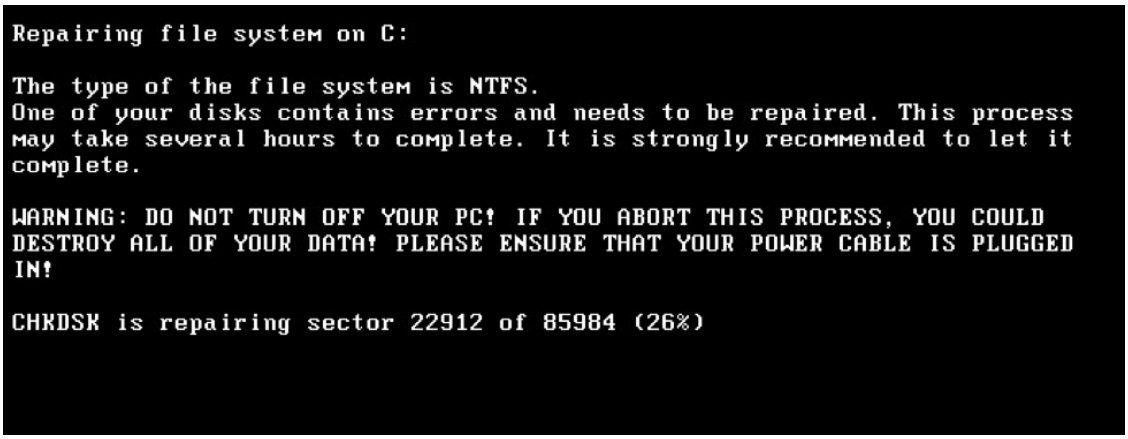


マシン感染後、ハードドライブセクターのスケジュールタスクが上書きされてしまい、1 時間以内に強制再起動してしまいます。

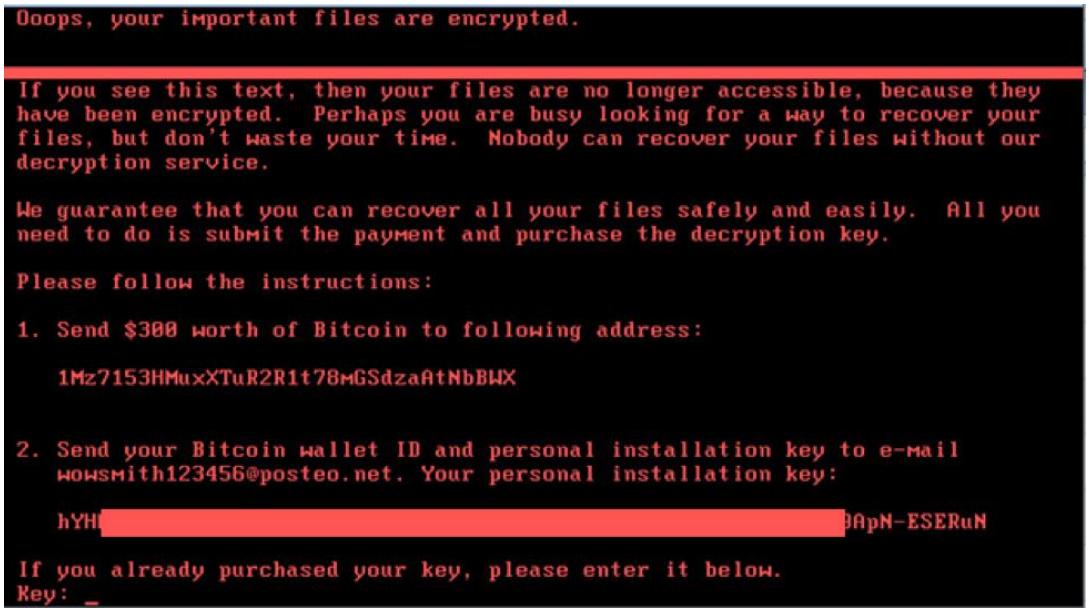


他の攻撃方法としては、Windows API の NtRaiseHardError を利用し、再起動を強制された後、ブルースクリーン停止状態（BSoD）に陥ります。

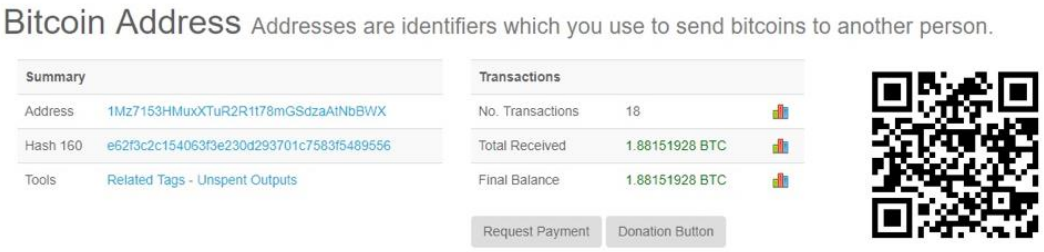
マシンが再起動後、偽の CHKDSK 画面が表示されます。



それからランサムノートへ画面遷移します。



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。



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。