アンラボ・セキュリティレター

Press Ahn

2015.5　Vol.17

悪の化身、ランサムウェア Top6

代表的なランサムウェアの特徴と悪性行為分析

悪の化身、ランサムウェア Top6

海外ではすでに数年前から登場していたランサムウェアだが、韓国ではこれまで目立った被害は発生していなかった。しかし最近ランサムウェアの一種である「CryptoLocker（身代金要求型不正プログラム）」のハングル版がWebで配布され、ランサムウェアへの懸念が高まっている。今回のPress Ahnでは主要ランサムウェアをカテゴライズし、それぞれの特徴をまとめた。カテゴライズおよび優先順位は、国内外の注目度（お問い合わせ、ニュース記事、投稿数など）と診断件数をベースにし、対象期間は2014年10月～2015年3月までとした。

ランサムウェア（Ransomware）はransom（身代金）とsoftware（ソフトウェア）の合成語で、ユーザーの文書ファイルを「人質」にして身代金を要求するとして付けられた名称だ。このマルウェアが一度システムにインストールされると、ファイルを暗号化して使用不可にし、正常化を条件にビットコインまたは追跡困難な電子マネーの支払いを要求することから非常に厄介だ。

ランサムウェアTop6

ランサムウェアの中でも、V3診断数で最大の比重を占めるとともに注目を集めているものを次の[表1]のようにまとめた。

これらのランサムウェアは、Nabucurとその他のランサムウェアに分けることができる。Nabucurはエンコードされたソースファイルに感染コードを追加して通常ファイルを変更する手法だが、アンラボV3は変更されたファイルを元のファイルに復元することが可能だ。一方でその他のランサムウェアはRSAやAESなどの暗号化技術を使用するため、元のファイルに復元するための復号化キーが必要になる。

注目のランサムウェアの特徴は次の[表2]の通りだ。NsbLockerとその他のマルウェアの特徴における最大の差は、暗号化技術を使用しないことと攻撃対象ファイルに「.exe」ファイルが存在することにある。そして共通点としては、すべてのランサムウェアは「ビットコイン」を利用して身代金の支払いを誘導していた。

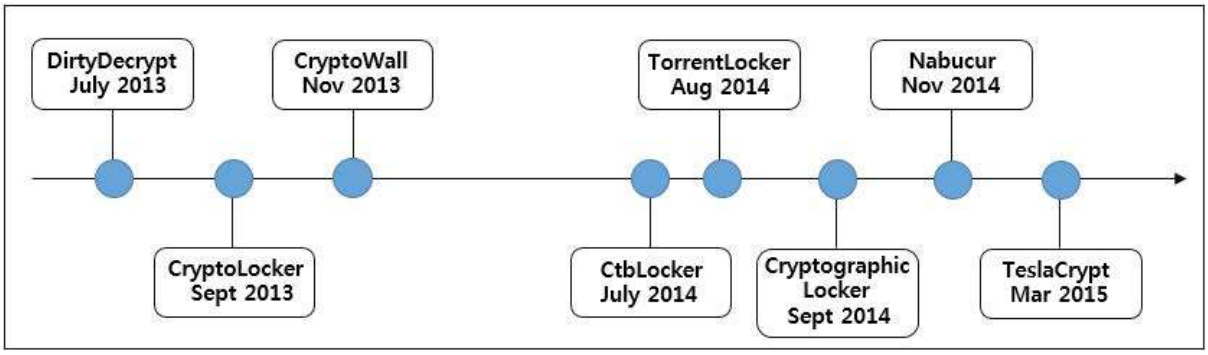
	FAMILY	MD5
1	NsbLocker / Nabucur	4DDE0233CD956FAA19FF21B3FB73FBBDED42954A5824A5DD1E57916848019 1B2 770D3BC32F7ACA8F94DD22209532A35219840868F8D20089BA4CE289F48A6A09 DC5BAD327EF50D2594F423A1DF7A6C03FF6CAFE7597BD6FF1521A1A1F817D9BF
2	CtbLocker / Critroni	vDEFB9614AFA1DA0D0057C80AACBCA7F0D0C3CE7B8B99D4B4278CE3E3CECE33E9 E89F09FDDED777CEBA6412D55CE9D3BCF420BDEB156FDB2F874A1E5D51E9D65F FEC68D340ED13292701404E438059FB714C0558C757C93465ECCBBD77D58BBF3
3	CryptoLocker	0204332754DA5975B6947294B2D64C926FE47DC2BDB86B0FC28017FC6A67B1F9v 0E1543914E129FF069D1079695115FE90DF492989EEA14562EE2E8C880EEDDB6 419ECEC2051479609ADED0C173619DF804FB36199787F2E3E2135611A38321EB
4	CryptoWall / CryptoDefense	31C2D25D7D0D0A175D4E59D0B3B2EC940650C9045814C652C2889D291F85C3AE B6C7943C056ACE5911B95D36FF06E0E4A9927372ADB1BBAB4D9FEDA4973B99BB 73A9AB2EA9EC4EAF45BCE88AFC7EE87E
5	TorrentLocker	7D1D5E27C1C0CB4ABCC56FA5A4A16744253491AD824E156971C957CD15254844 4A96F22E4FFDBCF271FF4EB70B1320ED86296FB3DDD46431DDFE8A48D6FB165C 6694617DAB8CD78630AA0A3E002E519771C066D831A5749685747B33CB9588A8
6	TeslaCrypt	01ADE9C90D49AF3204C55D201B466C1B0FF2BE71B46C129EF8905B41E60C2AB0 03C1A14C715E3A41F36B026A11A1BCB40C64ADDB8FE2ED5B029D9337E0E2FBA0 0AFBAEE4802BB74F9AC366579921F2B40C27082138728BC2AACE00263396ADDA

[表1] 代表的なランサムウェア

	区分	プロトコル	暗号化	ターゲット	手法	支払い	要求額
1	NsbLocker / Nabucur	TCP	Polymorphic	Doc/EXE/Image /Media	Polymorphic	Bitcoin	250 USD
2	CtbLocker / Critroni	HTTPS/TOR	AES, ECDH	Doc/Image	OpenSSL	Bitcoin	0.5 USD
3	CryptoLocker	HTTP	AES, RSA	Doc/Image	MS Crypto API	Bitcoin	300 USD
4	CryptoWall / CryptoDefense	HTTP/TOR	RSA	Doc/Image	MS Crypto API	Bitcoin	500 ~ 1000 USD
5	TorrentLocker	HTTPS	AES	Doc/Image	OpenSSL	Bitcoin	0.8 BTC
6	TeslaCrypt	HTTPS/TOR	AES, ECC	Game/Doc/ Image	OpenSSL	Bitcoin	500~1000 USD

[表2] 代表的なランサムウェアの特徴

これらのランサムウェアのタイムラインは、[図1]の通り。最近発見されたTeslaCryptは、攻撃対象となる文書や画像だけでなく、ゲームに関するファイルもターゲットにすることが特徴的で、電子メールで広まっている「CtbLocker」の類は最近再び拡散傾向にある。



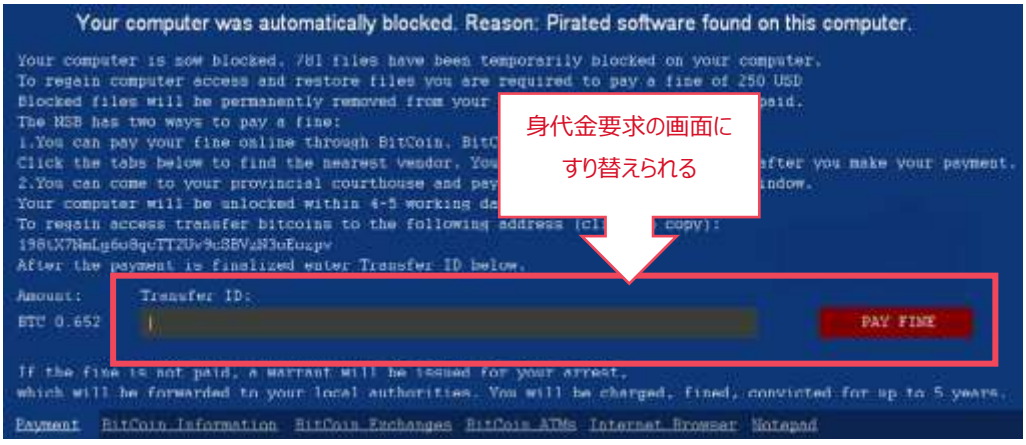
[図1] 主なランサムウェアの発生時期

ランサムウェアの機能解析

NsbLocker /Nabucur

Nabucurについては、2015年2月11日付けのアンラボASECブログ（http://asec.ahnlab.com/1025）「元のファイルに復元可能なランサムウェア（NSB : National Security Bureau）」で紹介している。このマルウェアに感染すると、システム上の画像（* .bmp、* .gif、* .jpg、*。png）ファイル、文書（* .doc、* .ppt、* .xls）ファイル、メディア（*。 mp3、* .wma）ファイルだけでなく、実行ファイル（* .exe）と圧縮ファイル（* .rar、* .zip）も攻撃対象になる。これらのファイルは、元のファイルをまずエンコードした形でバックアップしてから実行ファイルに変更する。この場合は元のファイルを「AES」、「RSA」のような暗号化手法で変更したものではないため、ワクチンでも復元できる。だが変更された実行ファイルにはバックアップされた元のファイルだけでなく、Nabucur感染コードも含まれている。これこそは、再び別のファイルを感染させるNabucurランサムウェア型のマルウェアなのだ。

Nabucurに感染したファイルが実行されると、2つの実行ファイルを「%User%」と「%ALLUser%」フォルダに作成する。これらのファイルは、スレッド形態で機能を実行しながら、C&C接続とシステム内の特定の拡張子を持つファイルを感染させる。そして最後にシステム画面を身代金要求の画面にすり変えるのだ。



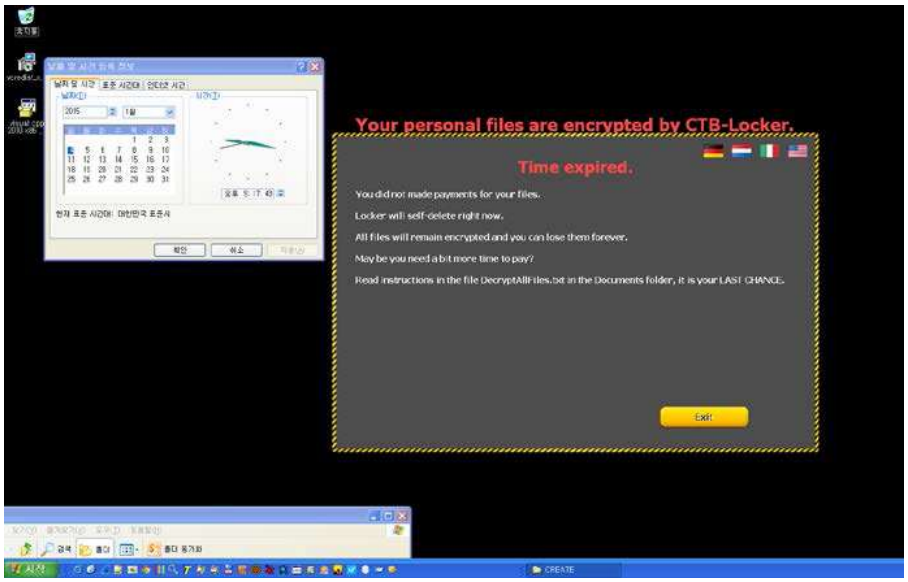
[図2] NsbLocker /Nabucur感染画面

CtbLocker /Critroni

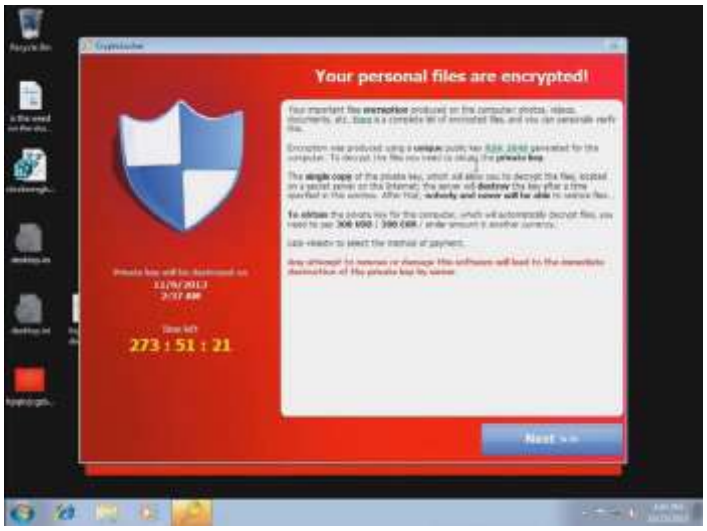
2014年7月に公開されたランサムウェア「CtbLocker」は「Critroni」という名でも知られ、スパムメールで配布されるダウンローダによって作成および実行される。添付ファイルに含まれたダウンローダは「.zip」または「.cab」形式に圧縮・配布される。解凍ファイルの拡張子は「.scr」で、実行すると「%TEMP%」フォルダに正常な「.rtf」ファイルを作成・実行し、まるで文書ファイルのように偽装するが、バックグラウンドではこっそりマルウェアをダウンロードする。このダウンロードファイルはランサムウェアであり、Officeなどの文書ファイルだけでなく画像やソースファイル、その他のファイルも暗号化対象とする。完了後はCtbLockerのメッセージとともに、ビットコインを要求するページが表示される。

[図3] CtbLocker感染画面

96時間以内に身代金を支払わない場合、データを回復できないというメッセージを表示し、期限が過ぎるかPCの時間を任意に操作すると有効期限終了の（expire）画面が現れる。



[図4] CtbLocker感染画面



[図5] CryptoLocker感染画面

CryptoLocker

2013年9月に初めて発見された「CryptoLocker」は、CtbLocker同様スパムメールの添付ファイルやP2P方式の「Gameover Zeus」ボットネットを通じて広まり、文書や画像ファイルを暗号化した。

正常化したければマネーパック（MoneyPak）やビットコインの身代金を支払うしかない。

このランサムウェアは、自動実行するようレジストリに自身を登録するのだが、登録名が「CryptoLocker」になっているのが特徴だ。C&Cサーバーに接続して公開鍵（Public Key）を受信し、システムファイルを暗号化する。現在はそのサーバーがダウン状態なので、ランサムウェアの機能は動作しない。

2014年8月、世界のセキュリティ専門家が「Tovar」オペレーションを通じてこのマルウェア作成者のC&Cサーバーをダウンさせ、サーバーに保存された復号化キーを多数獲得することにより、現在は暗号化されたファイルの多くを元の状態に復元した。

その間、全世界で約50万台のシステムがCryptoLockerに感染したことが報告された。

CryptoWall/CryptoDefense

CryptoWallの 動作もまた前述したCryptoLockerに似ている。両方の下位プロセスを作成後、PEイメージをインジェクションさせて動作し、C&Cサーバーから公開鍵を受信してからランサムウェアの機能を実行する仕組みだ。

[図6] CryptoWall感染画面

TorrentLocker

TorrentLockerもCryptoLocker、CryptoWallと同じような動作をするためコード部分が非常に似ている。このランサムウェアはレジストリ「HKCU¥ Software¥ Bit Torrent Application¥ configuration」に暗号化されたファイルリストを登録するため「TorrentLocker」と命名された。

[図7] TorrentLocker感染画面

TeslaCrypt

「TeslaCrypt」はゲーム機能と保存データを攻撃するランサムウェアであり、iframeの代わりにタグ（div）を使用したFlash Playerの脆弱性を突いてPCにインストールされる。構造はCryptoLockerと似ているが、文書ファイルだけでなくゲームに関するファイル（プロファイル、セーブ、データ、地図、モードなど）も暗号化するという点に違いがある。

TeslaCryptはCryptoLockerとは異なり、ビットコイン接続のアドレスを提供するためにネットワークが使用され、%AppData%フォルダには暗号化されたファイルリストを持つ「log.html」ファイルと、復号化する際に使用する「key.dat」ファイルが格納される。

そしてデスクトップに作成された「HELP_RESTORE_FILES.txt」には、暗号化されたファイルを解除するためにビットコインを決済する過程が説明されている。

[図8] TeslaCrypt感染画面

PCがランサムウェアに感染すると画面に警告メッセージが表示され、これを正常化するにはお金を振り込むよう求められる。感染すればPCを使用できないだけでなく重要なファイルが保存されている場合、ユーザーに選択肢はないに等しい。だが、ユーザーがお金を振り込んだとしてもシステムが100%元に戻るという確証もない。このように厄介なランサムウェアの被害を防ぐためには、もちろん感染しないように予防することが最も望ましい。何よりも発信先不明の電子メールに添付された疑わしいファイルを実行しないことと、使用中のセキュリティソフトを常に最新の状態に更新し、OSとアプリケーションの発行元から提供されるパッチを最新の状態に保つことが重要だ。

http://jp.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒105-0014 東京都港区芝4丁目13-2 田町フロントビル3階 | TEL: 03-6453-8315 (代)