アンラボ・セキュリティレター

Press Ahn

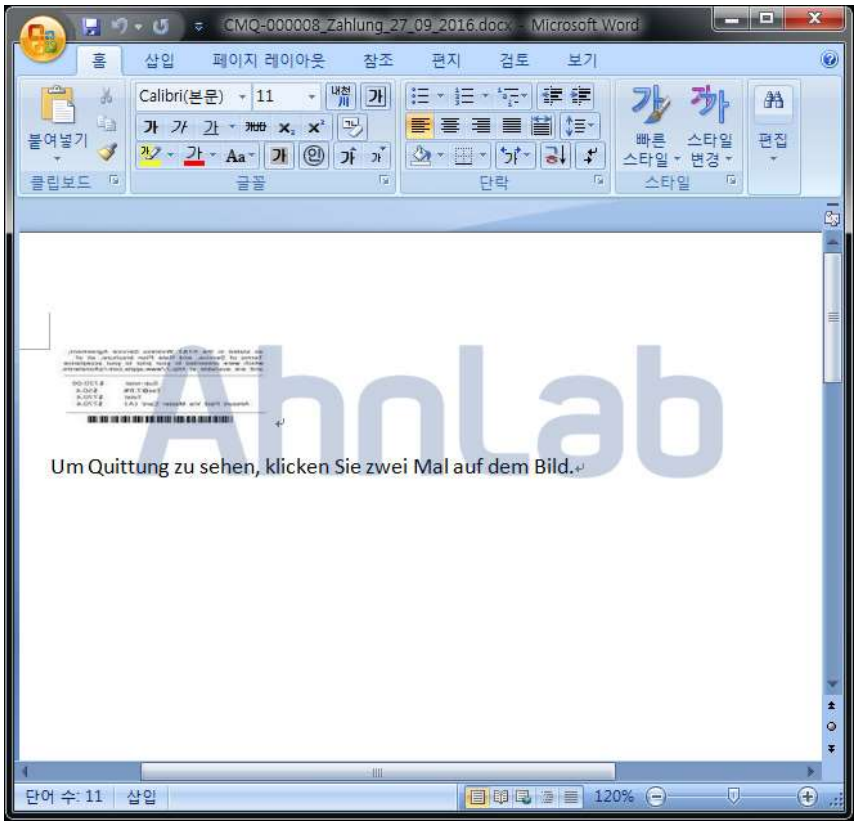
2016.11　Vol.35

Tor ネットワークを悪用するマルウェア

Tor ネットワークを悪用するマルウェア

Tor(トーア) Network は、ホストとサーバー間の通信時に仮想回線接続を数回に渡って経由するため、使用者の痕跡をトレースしにくい。おかげで匿名性が保証され、身元を明らかにしなくてもサーバーを運用できることから悪意ある行為にたびたび利用されている。今回のコラムでは Torネットワークの特性を悪用して使用者情報を奪取するマルウェアの実体について紹介する。

Torネットワークを悪用するマルウェアは、スパムメールに悪性ファイルを添付して配布される。まず添付された悪性ファイルを実行すると [図1]のように『イメージをダブルクリックして参照してください。』というドイツ語のメッセージが表示され、悪意あるスクリプト実行を誘導する。



[図1] 悪性ファイルの誘導内容

メッセージの誘導に従ってイメージをダブルクリックすると、文書 OLE(Object Linking & Embedding)領域に含まれた悪性 JavaScriptが実行される。JavaScriptは難読化されており、これを解除すると [図2]のように Windows PowerShellスクリプトで作成されていることが分かる。

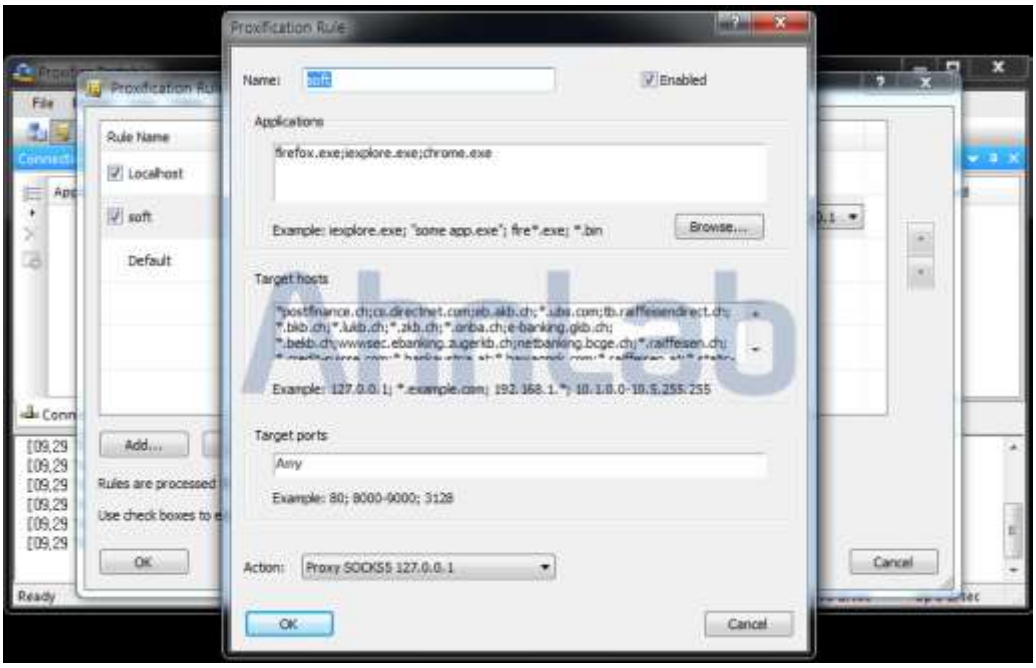
[図2] JavaScriptで難読化が解除されたPowerShellスクリプト

PowerShellはシステム管理用に設計された Windowsスクリプト言語であり、命令語を使用してシステムをハンドリングできる。Windows XPから Windows 8まですべてサポートし PowerShellで作成されたマルウェアの場合はほとんどの Windowsプラットホームを攻撃することができるのだ。攻撃者は攻撃を仕掛ける際に自分が必要な URLを入手するため、予めインストールされた Proxifierを利用する。

Proxifierはプログラムで発生するネットワーク要請を途中で横取りし、指定されたルールに従って外部に伝達するソフトウェアである。攻撃者はルールを操作して主なブラウザである IE、Chrome、Firefox等で攻撃者が指定した URLを要請した後、プロキシを通じて伝達する仕組みになっている。

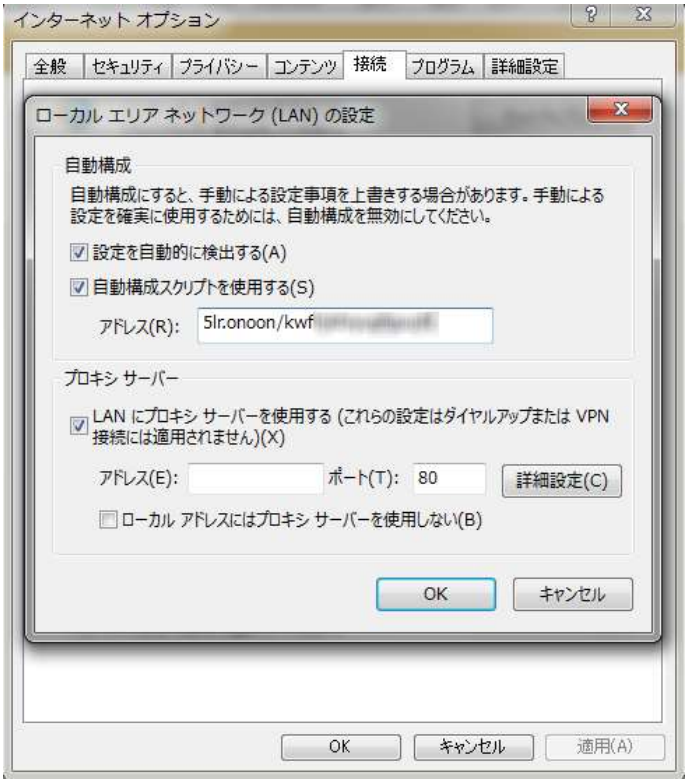
*postfinance.ch ; cs.directnet.com ; eb.akb.ch ; *.ubs.com ; tb.raiffeisendirect.ch ; *.bkb.ch ; *.lukb.ch ; *.zkb.ch ; *.onba.ch ; e-banking.gkb.ch ; *.bekb.ch ; wwwsec.ebanking.zugerkb.ch ; netbanking.bcge.ch ; *.raiffeisen.ch ; *.credit-suisse.com ; *.bankaustria.at ; *.bawagpsk.com ; *.raiffeisen.at ; *.staticubs.com ; *.bawag.com ; *.dientis.ch ; dientis.ch ; *bcvs.ch ; *cic.ch ; www.banking.co.at ; *oberbank.at ; www.oberbankbanking.at ; *baloise.ch ; *.ukb.ch ; urkb.ch ; *.urkb.ch ; *.eek.ch ; *szkb.ch ; *shkb.ch ; *glkb.ch ; *nkb.ch ; *owkb.ch ; *cash.ch ; *bcf.ch ; *.easybank.at ; ebanking.raiffeisen.ch ; *.onion ; *bcv.ch ; *juliusbaer.com ; *abs.ch ; *bcn.ch ; *blkb.ch ; *bcj.ch ; *zuercherlandbank.ch ; *valiant.ch ; *wir.ch

[表1] 攻撃者がターゲットとする URL



[図3] Proxifierを利用した悪意あるポリシー

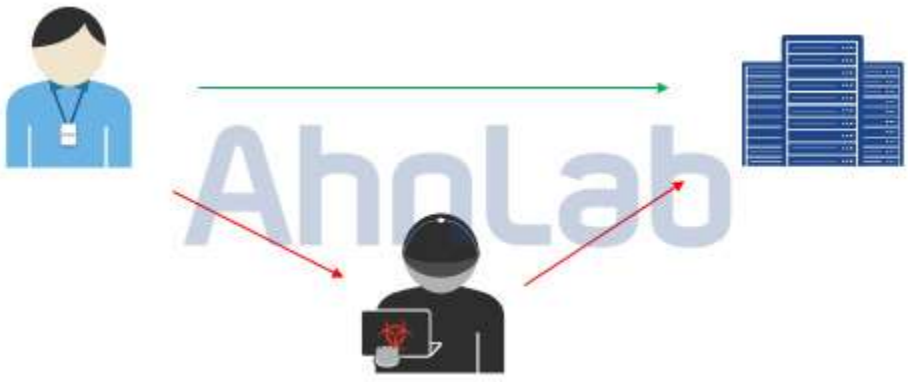
ホストでプロキシを設定しておくと、外部に出るデータは設定されたプロキシを通って出ることになる。攻撃者は[図4]のように、プロキシサーバーアドレスを自身の Torネットワークアドレスに設定することで Proxifierを通じて伝達されたパッケージが自分に送信されるようにしていた。



[図4] プロキシ設定の操作

ここまでの攻撃過程を簡単に図で現わすと、[図5]のようになる。このような攻撃タイプを中間者攻撃(man in the middle attack)と言う。

プロキシを操作されて攻撃者を通じて伝達される場合、行き交う過程で情報が操作されたり流出される可能性があるのだ。



[図5] 中間者攻撃

このように正常なメールに偽装してマルウェアを配布するケースが持続的に発生し、依然として大きなセキュリティ脅威になっている。上記のような事例の疑わしいメールを確認した場合、使用者たちの格別な注意が必要だ。

アンラボの V3製品では該当するマルウェアを次のような診断名で検知している。

<V3 製品群の診断名>

W97M/Dropper (2016.09.29.00)

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

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

〒108-0014 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)