アンラボ・セキュリティレター

Press Ahn

2019.4　Vol.64

Tick グループの最新攻撃事例分析

韓日で展開されてるターゲット攻撃

Tick グループの最新攻撃事例分析

10年もの間、韓国と日本を中心に攻撃を展開してきた脅威グループが存在する。その名もティック(Tick)だ。2013年に海外のセキュリティベンダーによって初めて知られたが、実は2008年頃から韓国で活動してきたとされる。しかし主に日本で攻撃ケースが知られており、韓国の攻撃ケースは多く知られていなかった。

そんな中、アンラボセキュリティ対応センター(AhnLab Security Emergency response Center、ASEC)では「Tick攻撃動向レポート」を発表し、主要攻撃対象とその手法について詳細に分析した。

Tick グループは、Bald Knight、Bronze Butler、Nian、RedBaldknight など様々な名前で呼ばれ、2013年海外セキュリティベンダーによって初めてその存在が知られた。同ベンダーがグループ名を『Tick(ティック)』と命名した 2014年から本格的な活動が検知されたが、この時から主に韓国と日本企業への攻撃を試みたとされる。しかし韓国ではこれより何年も前の 2008年に、同グループに関するマルウェアが発見されていた。このことから、Tickは 10年以上も韓国を対象に攻撃を仕掛けてきたと推測できる。

同グループは韓国と日本のインフラ環境に精通していると見られている。日本の攻撃ケースでは主に日本で使用される製品の脆弱性を利用し、韓国では脆弱性攻撃に加えて韓国産アンチウィルスやセキュア USB 製品を攻撃したからだ。

今回のコラムでは、韓国の事例を中心に Tick の攻撃手法とマルウェアに探る。

主要攻撃ケース

韓国の場合、Tick は防衛産業をはじめ政治機関、エネルギー、電子、製造、セキュリティ、Web ホスティング、IT サービス会社など多様な産業分野を攻撃対象にしている。主にスピアフィッシング、Adobe Flash や MS Office の脆弱性攻撃、ウォーターリンホルなどの攻撃手法を駆使する。マルウェアに Garbage データーを追加して分析を妨害したり、不正ファイルを作成する際に数十から数百メガバイトの長さを持つファイルを作成してセキュリティプログラムの迂回を試みている。

時期	対象	攻撃手法
2013年2月	不明	Flash 脆弱性(CVE-2013-0633、CVE-2013-0634)を利用した攻撃
2014年3月	韓国 - 防衛産業	Netboy 変形で攻撃。韓国で多数の感染報告
2015年1月	韓国 - 大企業 A	Bisodown 変形で攻撃
2015年5月	韓国 - 大企業 B	Netboy 変形で攻撃
2015年6月	アジア - 金融機関	確認不可
2016年2月	韓国 - 海洋産業	Daserf 変形で攻撃。2016年6月、韓国のキャリアで発見された Daserfマルウェアと同じ
2016年6月	日本 - 旅行会社	LAC レポートによる
2016年6月	韓国 - キャリア	Daserf 変形で攻撃
2016年9月	韓国 - エネルギー	Datper 変形で攻撃
2016年12月	日本 - 企業	日本の資産管理ソフトウェアの脆弱性(CVE-2016-7836)を攻撃して感染
2017年4月	韓国 - 未確認	2018年パロアルトユニット42を通じて韓国のセキュアUSBへの攻撃が知られた
2018年5月	韓国 - 国防分野推定	Bisodown 変形で攻撃。軍事関連内容に偽装したファイル(decoy)などからみて国防分野の関係者がターゲットと推定される
2018年5月	韓国 - 政治機関	Bisodown 利用攻撃
2018年8月	韓国 - 国防分野	Bisodown 変形で攻撃。感染システムで Linkinfo.dllファイル名を持つ Keyloggerと一緒に発見
2018年9月	韓国 - 政治機関	Datper 変形で攻撃
2019年1月	韓国 - 情報セキュリティ	JPCERT で 2019年2月に公開した Datper 変形で攻撃
2019年1月	韓国 - Webホスティング	2019年1月、韓国のセキュリティベンダーで発見されたマルウェアと同じ
2019年2月	韓国 - 電子部品	JPCERTで2019年2月に公開した Datper 変形で攻撃
2019年2月	韓国-ITサービス	2019年2月、韓国の電子部品の攻撃マルウェアと同じ Datper 変形で攻撃

[表1] Tick の主要攻撃事例（2013-2019）

[表1]は同グループの活動が最初に確認された 2013年から 2019年 2月現在までに知られている攻撃ケースをまとめたものだ。

主要マルウェアの詳細分析

Tick グループが使用したマルウェアタイプは、ダウンローダの役割をする Bisodown(別名 Cpycat 又は HomamDownloader）と Gofarer、バックドアの Daserf、Datper、Hdoor、Ghostrat、Netboy(別名 Domino 又は Invader)、Ninezero(9002)、Xxmm など多様だった。使用されたマルウェアを機能別に見てみると以下の通りである。

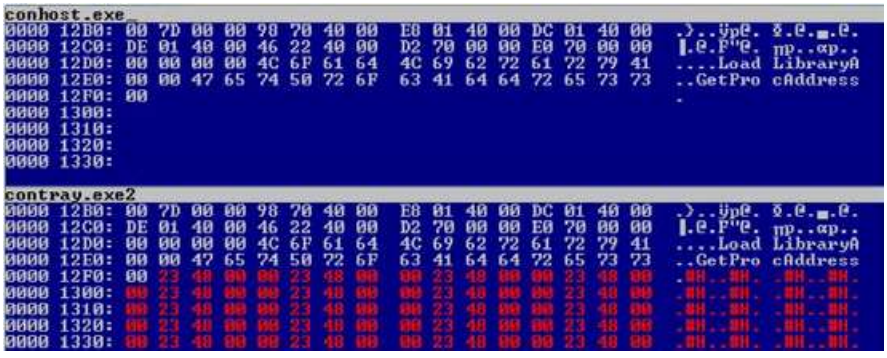
1. ダウンローダ (Downloader)

攻撃者はターゲットに業務に関連した偽装メールを送る。メールには PDF や Word ファイルに偽装した実行ファイルを添付していた。ユーザーが文書ファイルになりすました添付ファイルを開くと、実行ファイルが動作してダウンローダによって追加マルウェアをダウンロードする。

Tick が使用したダウンローダマルウェアは 2014年4月に初めて発見された Bisodown と 2015年に発見された Gofarer だった。 Bisodown は 2019年現在まで韓国企業へのターゲット攻撃で数回使用された。

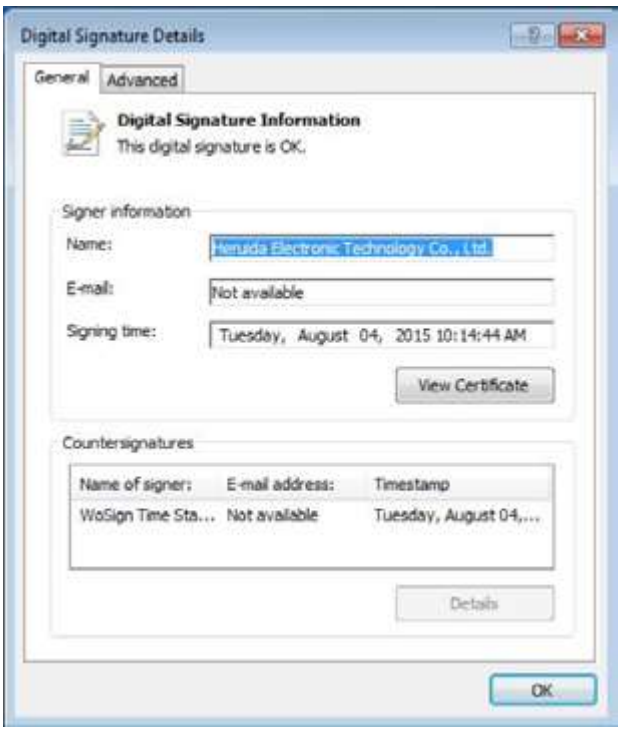
[図1] Bisodownマルウェア文字列

2015年以降に発見されたダウンローダ変形はファイル作成時、ファイルの最後に Garbage データーを追加してファイルサイズを数十~数百メガバイトまで大きくする。



[図2] ファイル作成時に追加された Garbage データー

Gofarer ダウンローダのデジタル署名を確認した結果、[図3]のように Heruida Electronic というメーカーの証明書を持っていることが分かった。だがメーカーが実在する会社かは確認されていない。



[図3] マルウェアのデジタル署名

ところが同じ証明書で署名された別の 4つのマルウェアが発見された。このうち 2015年7月に発見された変形と、証明書がない変形はすべて日本で発見された。まだ韓国で Gofarer の変形は確認されていない。

2. バックドア（Backdoor）

バックドア機能を持つマルウェアは、Daserf(別名 Muirim、Nioupale、Postbot)、Netboy(別名 Domino、Invader、Kickesgo)、Ninezero(9002)、Xxmm(別名 KVNDM、Minzen、Murim、ShadowWali、Wali、Wrim)、Datper などがある。Daserf は主にファイルリスト表示、cmd.exe でコマンド実行、ファイルのアップロード/ダウンロード/削除/実行などの機能を実行する。

2009年に初めて発見されたが、韓国で確認されたのは 2011年4月が初めてだった。初期は C言語で制作されたが 2013年以降 Delphi で製作された変形も登場した。サイズはほとんど約 30~40キロバイト程度だが、いくつかの変形は 100キロバイト以上の場合もあった。

Daserf 変形はバージョン情報などの特徴的な文字列と、ファイルの末尾に暗号化された C&C 情報を持つ。またバージョン情報も含むが [図4] のサンプルバージョンは 1.3G だった。ファイルの末尾には暗号化された C&C 情報が存在する。

[図4] のバージョン情報を含む Daserf マルウェアの文字列

韓国の攻撃事例のうち 2011年4月 Daserf マルウェアに感染されたシステムの中で、keyll.exe というファイル名のキーロガーが確認された。Daserf に感染した別のシステムでも同様のキーロガーが発見されたが、これは Daserf がキーロガーをダウンロードしたものと見られる。

Netboy は Delphi で作成されたマルウェアで、ほとんどの変形は主な文字列が 0x7C で XOR 暗号化されている。韓国では 2008年に初期バージョンが発見され、他の変形と同様に主要文字列が 0xC7 で XOR 暗号化されていたが、DLLファイル形式だった。また同変形はその後の 2010年に発見されたサンプルとはコードもかなり異なっていた。国内で Netboy 変形が最も多く発見された 2010年以降、本格的に活動を開始したとされる。

```
1318FE94 xor0x7C_1318FE94 proc near               ; CODE XREF: MalwareMain_13190EE8+5A↑p
1318FE94                                          ; MalwareMain_13190EE8+84↑p ...
1318FE94
1318FE94 var_4           = dword ptr -4
1318FE94
1318FE94                 push    ecx
1318FE95                 mov     [esp+4+var_4], eax
1318FE98                 mov     cl, 7Ch ; '|'
1318FE9A                 mov     eax, edx
1318FE9C                 dec     eax
1318FE9D                 test    eax, eax
1318FE9F                 jl      short loc_1318FEAD
1318FEA1                 inc     eax
1318FEA2
1318FEA2 loc_1318FEA2:                            ; CODE XREF: xor0x7C_1318FE94+17↓j
1318FEA2                 mov     edx, [esp+4+var_4]
1318FEA5                 xor     [edx], cl
1318FEA7                 inc     [esp+4+var_4]
1318FEAA                 dec     eax
1318FEAB                 jnz     short loc_1318FEA2
1318FEAD
1318FEAD loc_1318FEAD:                            ; CODE XREF: xor0x7C_1318FE94+8↑j
1318FEAD                 pop     edx
1318FEAE                 retn
1318FEAE xor0x7C_1318FE94 endp
1318FEAE
```

[図5] Netboy マルウェアの XOR 暗号コード

Netboy マルウェアは explorer.exe など通常のプロセスに悪質なコードを挿入して、キーロギング、画面キャプチャ、プロセスリスト、プログラム実行などの機能を実行する。2013年に発見された変形から、コードの中間に Garbage データーを追加するなど分析を妨害した。

Ninezero は Tick が 2012年から 2013年の間に使用したマルウェアであり、通信する際に『9002』の文字列を送信することから「9002バックドア」とも呼ばれる。韓国で同マルウェアが確認されたのは 2012年だった。約 70キロバイト程度の長さで、実行されると DLL形式のバックドアを作成し、サービスとして動作する。アンラボの分析によると一部のシステムは Netboy 感染後に Ninezero に感染した痕跡が確認された。

2015年に初めて発見された別のバックドアマルウェアとしては、[図6]のようにコードに Xxmm という文字列が存在し、『Xxmm』という名前がついた。Tick が同マルウェアを本格的に使用したのは2016年からだった。

[図6] Xxmmの特徴的な文字列

Xxmm はドロッパー、ローダー(Loader)、バックドアモジュールで区分される。ドロッパーが実行されると OS を確認して 32ビットのマルウェアか 64ビットのローダーマルウェアを作成する。ローダーが実行されると、暗号化されたバックドアマルウェアをメモリにインジェクションして実行する。Xxmm も Garbage データーを追加して、ファイルの長さを 50メ～100メガバイトにまで増やす。

Datper は 2015年から 2019年3月の現在までに発見されており、Delphiで作成された。Tick が使用した他のマルウェア同様にコードの中間に Garbage データーが含まれている。Datper 変形に感染した一部のシステムでは、キーロガーや Mimikatz マルウェアが発見された。

3. キーロガー(Keylogger)

前述したように 2011年4～5月、Daserf マルウェアに感染された一部システムにおいて keyll.exe というキーロガーが発見された。このキーロガーが実行されると、ユーザーが入力したキーの内容が c : ¥ windows ¥ log.txt ファイルに保存される。

[図7] 2011年キーロガー文字列

2017年と 2018年に Bisodown マルウェアや Datper マルウェアに感染したシステムから別のキーロガーが発見された。このキーロガーのファイル名は、apphelp.dll、k6.dll、linkinfo.dll など約 40～50キロバイトの長さを持っていた。

[図8] 2017年キーロガー文字列

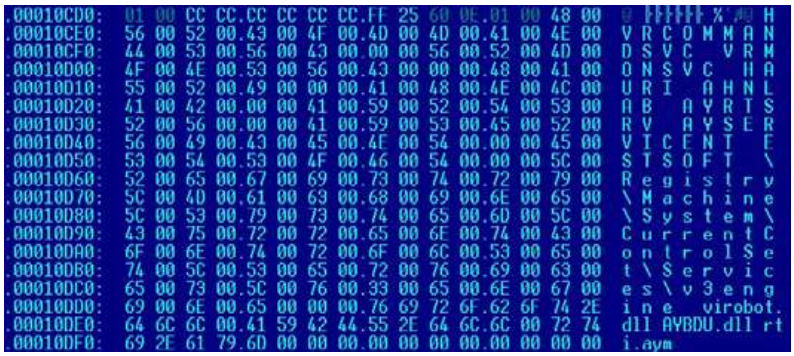
主な攻撃ツールの分析

アンラボでは Tick の活動を追跡することで攻撃者が保有している多様な攻撃ツールを確認できた。

1. アンチウィルス回避(Anti-AV)

Anti1.0 は、韓国で広く使用される韓国産アンチウィルスプログラムを攻撃するマルウェア作成ツールだ。2011年5月~7月まで、多数の変形が作られた。

[図9] 韓国産アンチウィルスプログラム攻撃用のマルウェアジェネレータ



[図10] 韓国産アンチウィルスプログラムの攻撃コード文字列

2. ビルダー (Builder)

2011年に製作された NForce は脆弱性を攻撃する悪意ある PDF を生成(build)するプログラムだ。

[図11] 悪意ある PDF ジェネレータ NForce

ShadowDawn は 2016年に発見されたビルダーで、Xxmmビルダー([図13]参照)と UI が類似している。

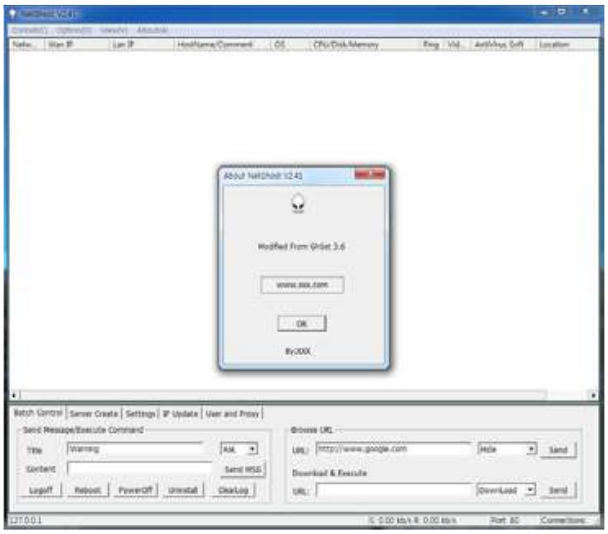
[図12] ShadowDawn ジェネレータ

3. コントローラ(Controller)

Tick は複数のコントローラ・プログラムを利用して、Netboy や Xxmm マルウェアを作成した。

[図13] Xxmmジェネレータ

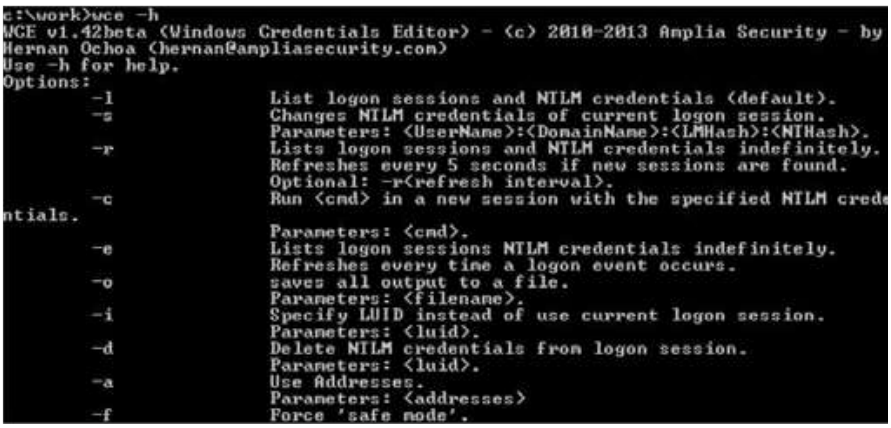
中でも NetGhost は、2014年から 2017年まで発見されたマルウェア作成及びコントローラだ。『Modified From Gh0st3.6』のような文字列が含まれていることから、Gh0st をベースに製作された可能性がある。



[図14] NetGhost コントローラ

4. WCE(Windows Credentials Editor)

WCE(Windows Credentials Editor)は Windows のシステムアカウント情報が分かるプログラムだ。攻撃者は 2013年に WCE.exe を使用した。

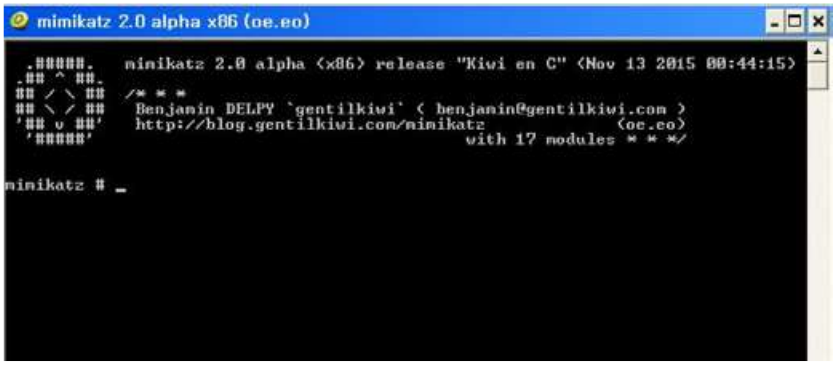


[図15] WCE 実行画面

2014年には 64ビットの WCE が初めて発見され、2016年6月に発見された 64ビット WCE は、前述した Gofarer マルウェアのデジタル署名のように Heruida Electronic という会社の証明書を持つ。

5. Mimikatz

Tick は 2015年から WCE の代わりに Mimikatz を利用してアカウント情報奪取を試みた。また Datper マルウェアに感染したシステムから mi.exe、m3.exe などの Mimikatz 変形が発見された。



[図16] Mimikatz マルウェア実行画面

アンラボの V3 シリーズでは Tick グループに関するマルウェアを、次の診断名で検知している。

<V3シリーズ診断名>

Dropper/Win32.Homam	Trojan/Win32.Homamdown
Trojan/Win32.Daserf	Trojan/Win32.MalCrypted
Trojan/Win32.Datper	Trojan/Win32.Netboy
Trojan/Win32.Domino	Trojan/Win32.Xxmm
Trojan/Win32.Gofarer	Win-Trojan/Injector.37100

マルウェアの動きを把握する

マルウェアだけで攻撃の背後まで特定するには限界がある。しかし Tick の場合は、いくつかのマルウェア証明書の署名が同じだったり、Daserf に感染したシステムから Netboy が発見されたり、Ninezero に感染したシステムで Netboy も一緒に発見されるなど明確な関連性が見えていた。
またほとんどのマルウェアが Garbage データーを追加し、ファイルサイズを増やす方法を取る点も似ている。これは多くのセキュリティ製品が異常に大きいサイズのファイルは収集しない点を狙ったものである。
もちろん一部のマルウェアでは関連性を把握しづらい面もあり、他のグループのマルウェアと知られる Bisonal 系のマルウェアをダウンロードするケースもあった。

結局 Tick による攻撃の関連性をより明確にするには、マルウェアだけでなく C&C サーバーなどの特徴を確認しなければならない。特に対象の内部でマルウェアが移動したプロセス、つまり Lateral movement を把握するなどの作業が必要だ。
Tick の攻撃対象企業では、エンドポイントを中心に不正ファイルが侵入したポイントからファイルの移動経路・行為・他のファイルとの相関関係を詳細に把握し、追跡する方策が必要となる。これと共にセキュリティベンダーとの積極的な情報共有が求められるだろう。
また、同グループが韓国と日本を対象に攻撃を展開しているだけに、もちろん 国家間の協力も重要課題である。

アンラボセキュリティ対応センター(ASEC)が発表した「Tick グループ攻撃動向レポート」の全文はアンラボサイトから確認できる。

▶「Tick攻撃動向レポート」のダウンロードはこちらへ（現在は韓国語版のみ）

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)

© 2019 AhnLab, Inc. All rights reserved.