アンラボ・セキュリティレター
Press Ahn

2018.7　Vol.55

アンダリエルの攻撃パターン変化

2018 上半期脅威グループ詳細分析

アンダリエルの攻撃パターン変化

アンラボは 5月末にアメリカで開かれた第12回 CARO ワークショップ(12th international CARO Workshop)にて「アンダリエル(Andariel)」攻撃グループの詳細分析を発表し、大きな関心を集めた。アンダリエルは現在韓国で最も活発に活動している攻撃グループで、2015年から韓国の主要機関及び企業に対する持続的な攻撃を展開してきたが、最近は一般ユーザーにまで攻撃対象を拡げている。今回のプレスアンでは、アンラボセキュリティ対応センター(ASEC)が分析した「アンダリエル」攻撃グループの主要攻撃ケースと手法の変化を説明した。

アンダリエルは攻撃グループ「Lazarus」の下位グループで 2015年から活動が確認された。同グループは 2014年から 2015年にかけて発生したサイバー攻撃 Operation Black Mine と関連があり、同攻撃は、2008年韓国の軍事機関攻撃と 2013年 3.20 ネットワーク障害(DarkSeoul)にも関与が疑われていた。

アンダリエルは韓国で活動中の脅威グループの中で最も活動が盛んだ。初期は主に軍事関連情報を入手するために攻撃を展開したが、2016年末から金融、旅行会社、オンラインゲームユーザー、仮想通貨取引所の利用者など攻撃対象を多角化している。特に攻撃対象(target)が使用するソフトウェア脆弱性を利用した攻撃が多発する点からして韓国の IT環境をよほど知り尽くしていると見られ、格別な注意が求められている。

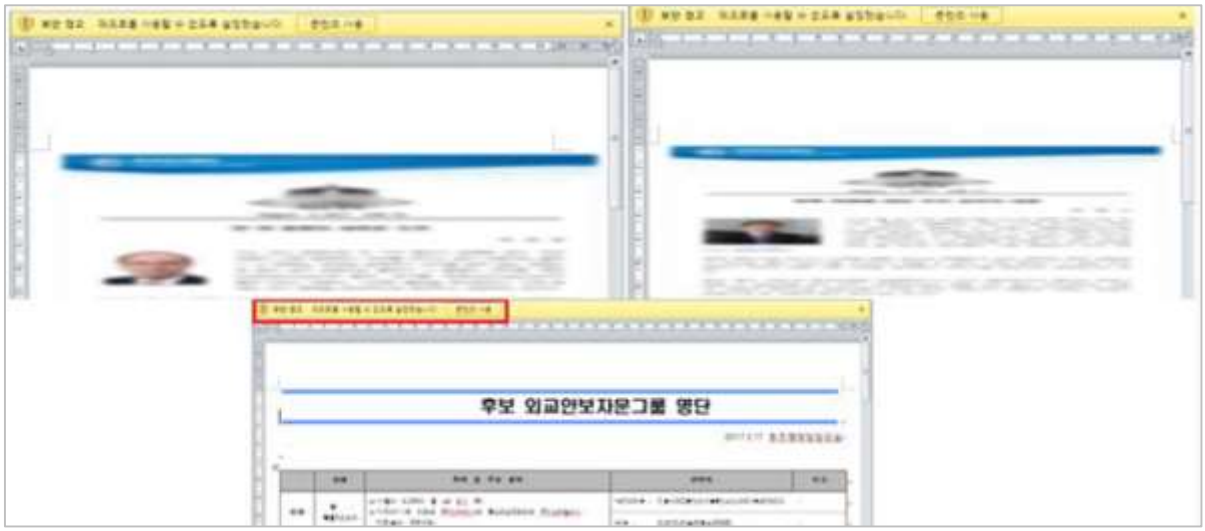
アンダリエルグループの攻撃手法

アンダリエルが主に使う攻撃手法は、▲スピアフィッシング(Spear Phishing)、▲ウォータリングホール(Watering-hole)、▲中央管理システムの脆弱性攻撃、▲サプライチェーン(Supply Chain)攻撃で区分する。

1. マクロを利用するスピアフィッシング

アンダリエルは、ターゲットに関連する偽装文書を添付してメールを送りつける「スピアフィッシング手法」を利用した。添付された文書ファイルにはマクロ(Macro)が含まれ、受信者にマクロ機能を活性化するように誘導した。マクロ機能を悪用した手法は活動初期の 2015年に比べてどんどん発展した。[図1]は 2017年に発見された文書ファイルだが、本文をぼやけて表示するように処理することで受信者にマクロ機能活性化を促した。

アンダリエルは韓国産ソフトウェアの脆弱性を利用したが、意外なことに 2018年 5月現在までアンダリエルがハングル形式ファイル(HWP)を攻撃に利用したケースは確認されなかった。



[図1] 攻撃に使用された文書(2017年)

2. ActiveX 脆弱性を利用したウォータリングホール

アンダリエルは、ターゲットが接続しそうなサイトをハッキングして脆弱性攻撃コードを潜ませ、同サイトにアクセスするとマルウェアに感染するウォータリングホール手法を使った。特定の IP アドレスから接続してこそマルウェアに感染する標的型攻撃を思わせるケースもあった。アンダリエルは ActiveX 脆弱性攻撃コードをサイトに潜ませて、ユーザーが特定の ActiveX がインストールされた IEブラウザで該当のサイトに接続すれば攻撃が動作する手法を使った。

3. 中央管理ソリューションの脆弱性を攻撃

アンダリエルは攻撃対象が導入した中央管理ソリューションを把握して脆弱性を探り、攻撃に利用する。同攻撃は管理サーバーアカウントを利用する攻撃と、クライアントエージェント脆弱性を利用した攻撃に区分される。

管理サーバーを利用した攻撃は、管理者アカウントを奪取して正常ファイルの代わりにマルウェアを配布する。管理者アカウントが一度でも悪用されると大変なことになるのはこのためだ。また管理サーバーは常用ソフトウェアのアップデートファイルを外部(ソフトウェア開発元)からもらって内部に配布するため、外部アップデートサーバーのファイルが悪意あるファイルに改ざんされた場合、マルウェアが含まれたアップデートファイルが中央管理サーバーを通じて内部のネットワークに配布されてしまう。

クライアントエージェントを利用した攻撃は、中央管理サーバーからのコマンドやファイルの適合性をスキャンするエージェント機能を回避するなどの手法で、管理サーバーのように偽装してエージェントにコマンドを送信する手法だ。

4. サプライチェーン攻撃

アンダリエルは多様なサプライチェーン(Supply Chain)を利用して攻撃を試みた。ソフトウェアのセットアップファイルにマルウェアを潜ませて同ソフトウェアの公式サイトから配布する手法と、ソフトウェアアップデートプロセスからマルウェアを感染させる手法を利用した。一部攻撃は同ソフトウェアを使用するすべてのユーザーを感染させるのではなく、接続 IP アドレスを確認してターゲットのみ感染させていた。ほかにも特定の産業分野で使用されるシステムに関するソフトウェアの脆弱性を利用した攻撃を実行した。

攻撃パターンと対象の変化

アンダリエルの 初期ターゲットは軍事機関と防衛産業だった。2015年には韓国で開催された国際防衛産業展示会(Seoul International Aerospace & Defense Exhibition, ADEX)に参加した企業への攻撃があった。イベント関連内容に偽装した文書をメールに添付して参加者に送信し、マクロ機能を利用して変種の Rifdoor マルウェアのダウンロードを誘導した。

[図2] マルウェア変種のリーフドア(Rifdoor) PDB 情報

以後アンダリエルは防衛産業への攻撃を持続的に展開した。代表的なものとしては 2016年2月韓国のセキュリティ会社がハッキングされ、デジタル証明書が流出された件がある。2016年4月には防衛産業、海洋サービス会社、ICT企業などで中央管理ソリューションの脆弱性を利用したマルウェア「Ghostrat」に感染された。Ghostrat は中国で製作されたバックドアタイプのマルウェアで、アンダリエルは同マルウェアを 2015年から 2016年にかけて攻撃で使用した。

アンダリエルの攻撃パターンに変化が起こったのは 2016年だった。2016年8月、アンチウィルス管理プログラムの脆弱性を利用して軍事関連機関を攻撃して軍事情報を流出した。また 2016年末からは金銭的な収益目的へと攻撃の様相が変化している。10月には某ソフトウェア製作社サイトをハッキングし、正常なインストールファイルをマルウェアが挿入されたファイルにすり替えてオンラインギャンブルゲームで相手の手をのぞき見するマルウェアを配布した。2017年にはネットカフェのマネジメントプログラムを利用して、不特定多数を対象にマルウェアを配布している。2017年3月には韓国の ATM がハッキングされ、クレジットカード情報が流出される事件が発生した。この件では 2016年11月から攻撃を試みたようで、攻撃に使用されたマルウェアは 2016年軍事関連機関の資料流出に悪用されたマルウェアと似ていた。また 2017年5月から 7月まで金融業界を集中攻撃している。金融労組のサイトでマルウェアを配布したり、金融機関で使われるシステム脆弱性を利用して攻撃を試みた。

2017年10月には韓国の有名旅行会社がハッキングされて個人情報が流出されたが、続いて12月にも別の旅行会社がハッキングがされたことが分かった。2017年12月、アンダリエルは ERPソリューションアップデートファイルを改ざんしてマルウェアを配布した。しかし該当の ERPソリューションを使用するすべての企業ではなく、特定企業のみマルウェアが侵入していた。

アンダリエルは 2017年12月から仮想通貨取引所ユーザーを対象に攻撃を展開した。また 2018年1月にはマルウェアが含まれたリモートサポートプログラムを配布し、今年2月には国会議員室を騙ったメール攻撃を試みるなど、多様な攻撃様相を見せた。国会議員室を装ったメールに含まれたマルウェアは、2017年 ATMハッキングに使用されたマルウェアの変形であり、また別の変形も 6月に金融会社の攻撃で使用された。

企業を狙う中央管理ソリューション攻撃

アンダリエルは韓国で使用率の高い中央管理ソリューションを悪用し、多数の攻撃を展開した。一定規模以上の企業では PC など多数のシステムを中央管理ソリューションに繋いで管理している。攻撃者らが中央管理ソリューションを狙う理由は、中央管理ソリューションを掌握すれば、そこに繋がれるすべての内部システムのリモートコントロールが可能になるからだ。

次にアンダリエルが中央管理ソリューションのクライアントエージェント脆弱性を利用して、悪意あるファイルを侵入させた 3つのケースを紹介した。

1. 中央管理ソリューション攻撃 A

2015年中央管理ソリューション Aの脆弱性を攻撃するマルウェアが発見された。同マルウェアが実行されると、指定された IP アドレスを通じて中央管理ソリューション A の管理サーバーに接続したエージェントに、マルウェアが挿入された実行ファイル v3pscan.exe が送信・実行された。

2. 中央管理ソリューション攻撃 B

中央管理ソリューション B の脆弱性を悪用した攻撃は 2015年から 2017年まで確認された。nc.exe、nt.exe、n5lic.exe、nc5rt2.exe、Bin.exe など多様なマルウェアが使われたが、vs1.vbs、winrm.vbs などの VB スクリプトファイルを作成して悪意あるファイルもダウンロードさせた。2015年から 2017年までに発見された変形は、サーバー IP、ターゲットシステム IP、ダウンロードアドレス、リモート実行ファイルパスなどを因子として、脆弱性攻撃に成功したシステム上にマルウェアをダウンロードするスクリプトファイルを生成する。このスクリプトは因子に入力されたアドレスからファイルをダウンロードした後、5バイトを復元した。

```
c:\work>nc
Usage:main.exe ServerIP, TargetIP, DownloadUrl, RemoteFilePath, [vbScriptPath=c:
\windows\temp\winrm.vbsInvalid License.Try Again

c:\work>nc5rt2
Usage:main.exe LICENSE TargetIP, PORT, DownloadUrl, RemoteFilePath, [vbScriptPat
h=c:\windows\temp\winrm.vbs
c:\work>bin
Usage:main.exe License TargetIP, DownloadUrl, RemoteFilePath, [vbScriptPath=c:\w
indows\temp\vs1.vbs
c:\work>
```

[図3] 中央管理ソリューション B 攻撃ツール

3. 中央管理ソリューション攻撃 C

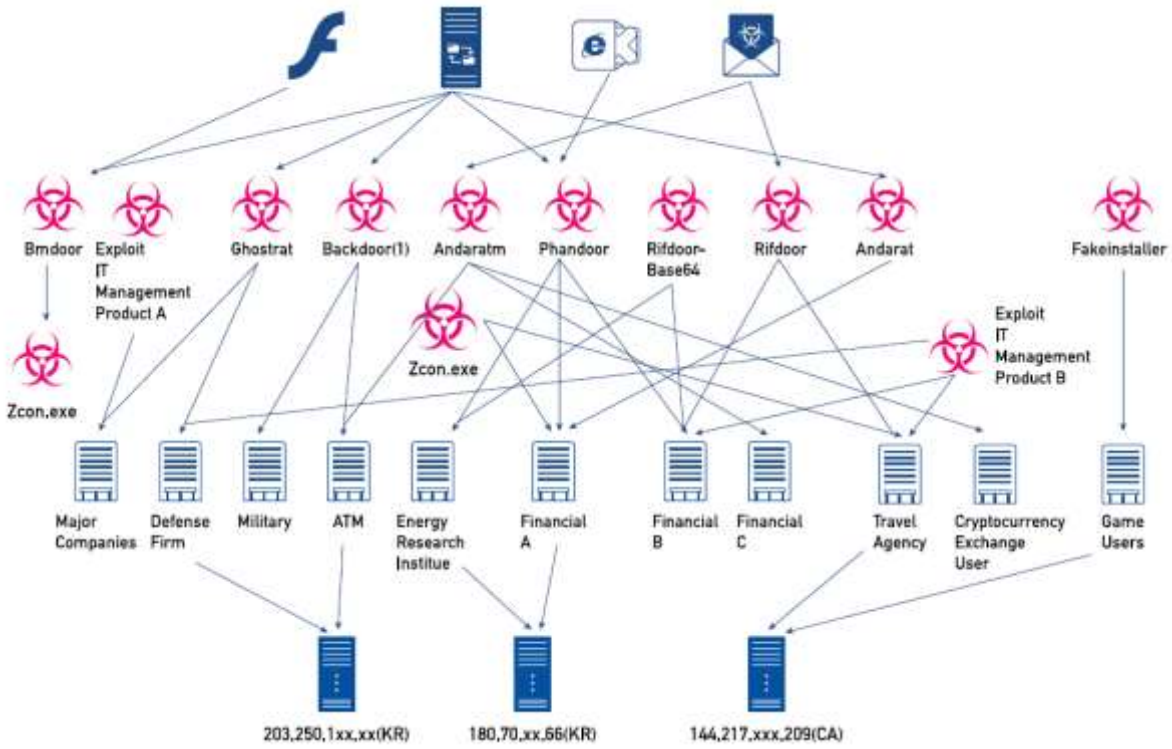
中央管理ソリューション C の脆弱性を利用したマルウェアは 2016年 9月に初めて発見され、ファイル送信及び実行などを遂行した。

```
c:\work>x
+++  TargetIP TargetPort commandType arg1 arg2 arg3
+++      SendFile calc.exe /tmp/calc.tmp
+++      GetFile /tmp/calc.tmp c:\temp\calc.exe
+++      Scan
+++      Update
+++      Run c:\windows\notepad.exe 1.txt system(administrator)
+++      Restart
+++      ServerUpdate
```

[図4] 管理ソフトウェア C 攻撃ツール

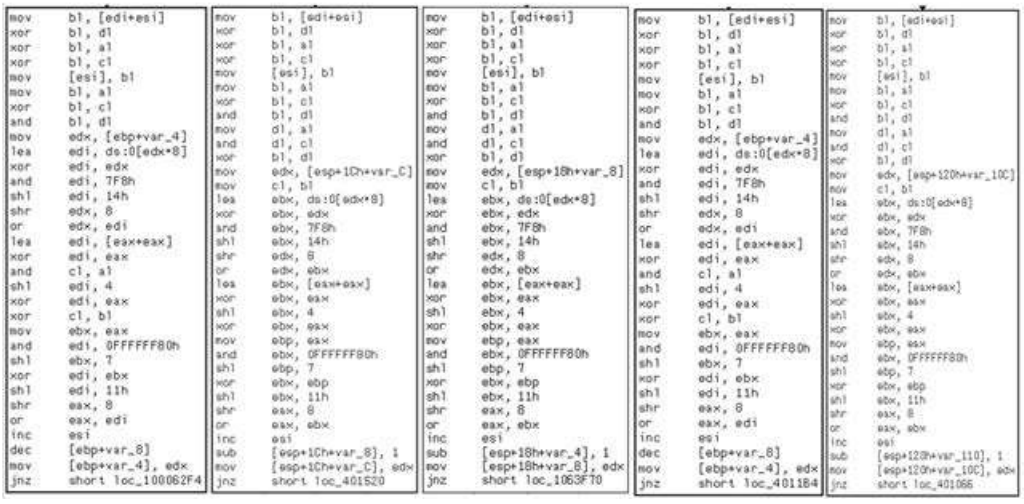
アンダリエル関連攻撃ケース

アンダリエルは多様なマルウェアを駆使して攻撃を展開した。アンラボの分析によると多数の攻撃ケースからアンダリエルとの関連性が発見された。
アンダリエルと Operation Black Mine の攻撃パターンは似ているが、特に zcon.exe ファイルを共通的に使用したことが確認された。
二つの攻撃グループの関連性が疑われる理由がここにある。類似マルウェアで多様な目標を攻撃し、一部マルウェアは同じ C2を使用した。マクロを利用した攻撃の場合も 2015年と2017年のマクロのコードに大きな差がなかった。



[図5] アンダリエルと多数の攻撃の連関関係

またアンダリエルが製作したマルウェアは、[図6]のように似たような暗号化方式を使っていた。



[図6] アンダリエルのマルウェア暗号化方式

最新の攻撃に備えて内部へのモニタリング強化を

アンダリエルの攻撃ケースからわかるように、企業の中央管理ソリューションもまたいつでも攻撃の経路になりえる。中央管理ソリューションを利用した攻撃は組織全体にかけて莫大な被害を与えかねないので、格別なセキュリティ管理が求められる。

まず中央管理ソリューションの管理サーバーに対するセキュリティポリシーが重要だ。許可されたシステムのみ管理サーバーにアクセスできるように制限し、管理サーバーのログイン情報(管理者アカウント)を随時変更して、システムに保存しないなど基本的なポリシーが守られるように適切な管理が重要だ。

また周期的にログを確認して、異常なファイルが管理サーバーから配布されてないか確認しなければならない。管理サーバーを通さずにクライアントにインストールされたエージェント脆弱性を悪用する攻撃ケースもあるため、中央管理ソリューションが使用するポート番号に対する動きなどが発生していないかモニタリングが必要だ。

攻撃者は多様な方法で内部への侵入を試みることから、外部とのアクセスポイントにセキュリティが集中しやすいが、中央管理ソリューションを悪用する攻撃のように内部インフラで発生するイベントもまたしっかりとモニタリングする必要がある。

アンダリエル攻撃グループに関する詳細な分析レポートは、下のリンクからダウンロードできる。

◆ **アンダリエル攻撃グループ分析報告書をダウンロード** (現在韓国版のみ。10月に英語版公開予定)

http://download.ahnlab.com/kr/site/library/[Report]Andariel_Threat_Group.pdf

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)