アンラボ・セキュリティレター

Press Ahn

2019.8　Vol.68

ランサムウェアと採掘マルウェア、減少の意味

2019 年上半期ランサムウェアおよびマイナー統計

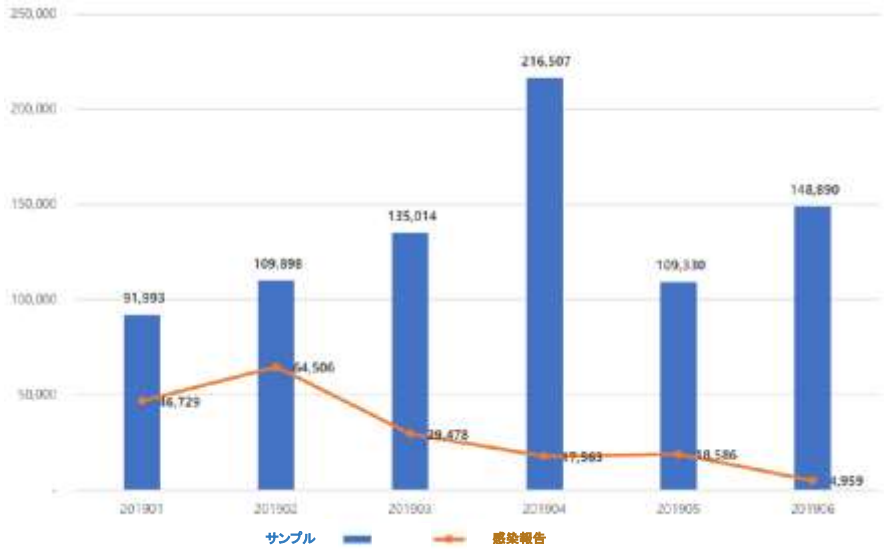
ランサムウェアと採掘マルウェア、減少の意味

2019年上半期のマルウェア統計によると韓国でもランサムウェアとマイナーマルウェア(Miner、仮想通貨の採掘マルウェア、以下マイナー)が激減する傾向を見せた。だがこれらの数値の内情を見ると、個人を対象にしたランサムウェアとマイナーの拡散は減少した一方で、企業を対象とした攻撃はむしろ増加したことが分かった。これは世界的に共通している現象であるが、実は韓国におけるランサムウェア推移の変化は他の国とは少し異なる点がある。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(AhnLab Security Emergency response Center、以下ASEC)が発表した 2019年上半期韓国におけるランサムウェアとマイナー統計の特徴を紹介した。

企業や機関に被害をもたらすマルウェアは多様だが、問題となるのはやはりランサムウェアとマイナーだろう。これらの悪意あるコードらは、システムを使用不可にしたり、パフォーマンスを低下させてビジネスの継続性と生産性に直接影響を与えることもある。組織のセキュリティ担当者が特にランサムウェアとマイナーに注意しなければならないのもこのためだ。

2019 年上半期脅威の減少、だが...

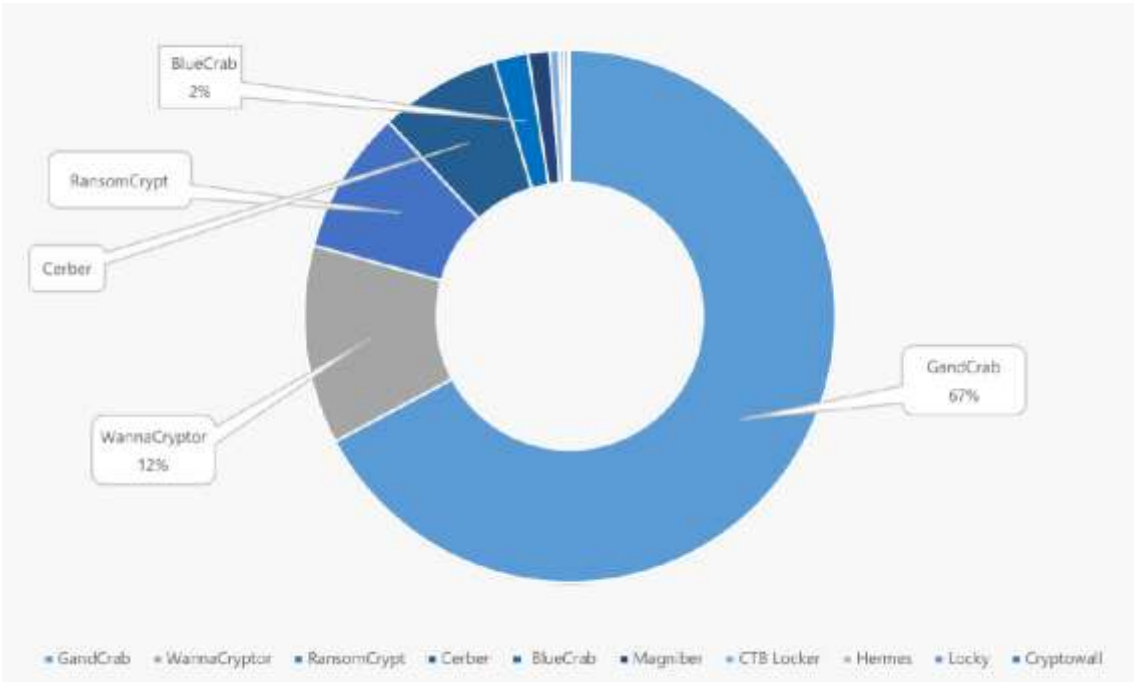
ASECの集計によると、今年第2四半期ランサムウェアサンプル数は 47万4千件で、第1四半期の 33万6千件に比べて 41.2%増加した。しかし第2四半期ランサムウェア感染報告件数は 4万1千件で、1四半期の 14万7百件に比べて 70.7%も減少したことが分かった。これは 2016年以来最も低い数値である。



[図1] 2019年上半期ランサムウェア統計(*サンプル数および感染報告件数)

2四半期にランサムウェアサンプル数が増加した要因は「GandCrab」ランサムウェアにある。5月末、攻撃者が製作中止を宣言するまでに様々な変形が配布され、上半期主要ランサムウェアの中でも最も多い 67%の割合を占めた。([図2] 参照)

上位ランクに含まれない小さいランサムウェアが全体的に増加したことも、第2四半期ランサムウェアサンプル数が増えた要因の一つであった。



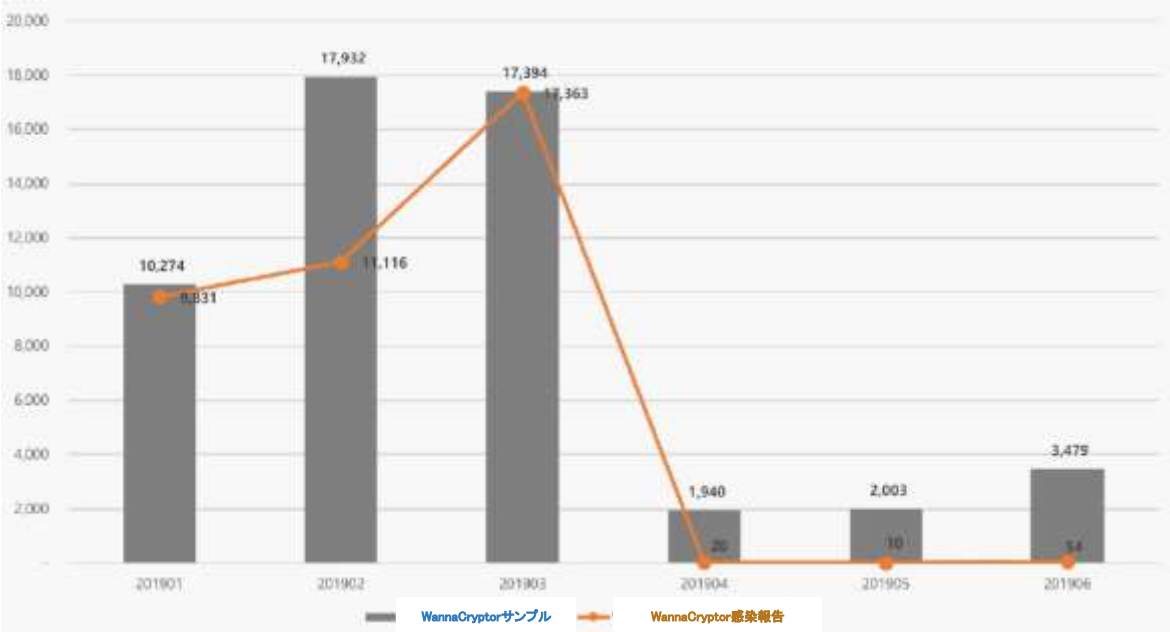
[図2] 2019年上半期ランサムウェアトップ10 (*サンプル数基準)

第2四半期に入り、ランサムウェア感染報告件数が激減した原因も GandCrabにある。[図3]のように今年3月から GandCrab感染件数が減少し始め、攻撃者が製作中断を宣言した 5~6月には激減している。結果的に上半期韓国のランサムウェアサンプル数の増加と感染報告件数の減少は、すべて GandCrabによるものだったといえる。GandCrabは 2018年1月に初めて報告された後、2019年6月まで最悪のランサムウェアとして名を馳せていた。約 15ヶ月間、韓国で発見されたサンプル数だけで 56万9千件、感染報告件数は 50万2千件に達した。月平均 3万3500件ほどの被害が発生しており、韓国における GandCrabの被害は甚大なものとなった。

[図3] 2019年上半期 GandCrabランサムウェア推移(*サンプル数と感染報告件数)

GandCrabと共に WannaCryptor(別名ワーナークライ)ランサムウェアの感染件数もまた大幅に減少し、今年上半期ランサムウェア感染件数は全体的に減少している。2017年5月世界に衝撃を与えた WannaCryptorランサムウェアは、SMB脆弱性(MS17-010、別名 EtenalBlue)を通じて被害が拡散した。今年の初めにも韓国では WannaCryptorサンプル数と感染件数が増加したことが確認された。([図4]参照)

企業では管理プロセスの都合により関連するセキュリティパッチを適用しないところも多く、WannaCryptorの被害が続いた要因となった。第2四半期に入り WannaCryptorランサムウェアの感染は収まりつつあるが、SMB脆弱性を利用する多様なマルウェアが配布され続けているだけに企業のセキュリティ担当者は SMB脆弱性管理の優先順位を上げて対処すべきだろう。



[図4] 2019年上半期 WannaCryptorランサムウェア推移(*サンプル数と感染報告件数)

2019 年上半期「Clop」と「BlueCrab」に注目

第1四半期には意外な伏兵の登場によってセキュリティ業界を緊張させた。「Clop」ランサムウェアだった。[図5]のように第1四半期 Clopランサムウェアの感染件数は急増したが、第2四半期には著しく減少している。だが 7月初め、一部の企業を中心に同ランサムウェアの被害が報告された。[図5]でもう一つ目を引くのは Clopランサムウェアがサンプル数に比べて感染報告件数が非常に多いということだ。同ランサムウェアは、サンプル数を基準に上半期ランサムウェアトップ 10にランク入りしないほど少ない割合にも関わらず、感染件数が高かった。その理由は何か。

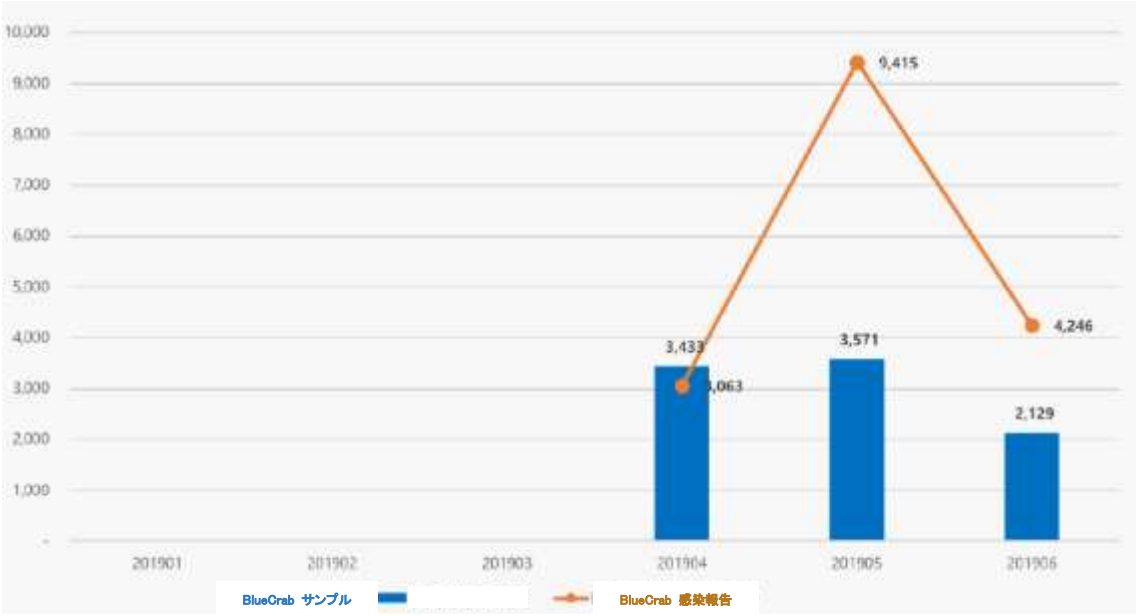
Clopランサムウェアは今年の初めから特定の組織を詐称して、悪意ある実行ファイルやワード、エクセルなどの不正な文書ファイルを添付したメールを企業や機関に送信した。5月末には国税庁を詐称して htmlファイルを添付するなど攻撃方法を変更したこともある。

Clopランサムウェア攻撃者は特定のハッキングツールを利用して企業の PCとサーバシステムの掌握を試みるが、まず感染したシステムがターゲット企業のアクティブディレクトリ(AD)サーバーに接続されたシステムであることを確認する。内部への拡散を展開し、最終的に ADサーバの管理者権限を奪取して ADサーバに接続された PCやサーバシステムを感染させる。同ランサムウェアが ADサーバの権限を奪取すると感染が広がるだけでなく、ADサーバに接続された PCとサーバをリモートコントロールして情報流出も可能になるためより注意が必要だ。

[図5] 2019年上半期 Clopランサムウェア推移(*サンプル数と感染報告件数)

企業をターゲットにするランサムウェア攻撃はすでに国内外で頻繁に発生している。代表的なケースとして、今年の上半期ノルウェーにある世界最大規模のアルミニウムメーカーとベルギーの飛行機部品メーカーがランサムウェアに感染して大騒ぎになった。また米国では交通施設や銀行、地方自治団体がランサムウェアに感染して業務が麻痺したこともあった。数年前、韓国でも有名なホスティング会社を狙った標的型ランサムウェア攻撃によって莫大な被害が発生したことがある。しかし Clopランサムウェアは特定の産業群を対象にするよりは一般企業の環境を考慮したランサムウェアと推定されている。

そして今年上半期に登場したニューフェイスの代表格に、「BlueCrab(別名Sodinokibi)」がある。これは今年4月初めて報告されたランサムウェアだが、上半期ランサムウェアトップ10にランクインするほど急増した。



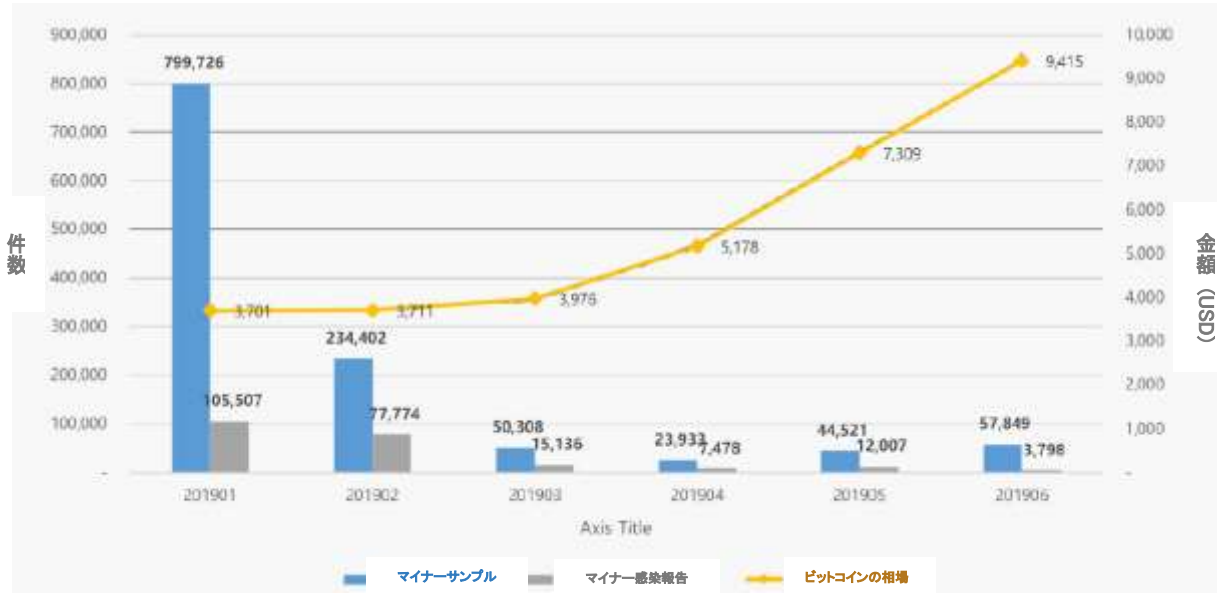
[図6] 2019年上半期 BlueCrabランサムウェア推移(*サンプル数と感染報告件数)

BlueCrabは名前だけでなく、その拡散方法も GandCrabに似ている。主にメールの添付ファイルとエクスプロイトキット(Exploit Kit)を利用した Malvertising手法を使用した。また WordPress脆弱性を利用して有名ポータルサイトの検索結果ページの上部に表示された Webサイトを通じて配布された点も GandCrabと同じだった。BlueCrabランサムウェアの暗号化された設定ファイルの中には、特定のフィールド値が含まれていたが GandCrab同様「サービス型ランサムウェア(Ransomware-as-a-Service、RaaS)」で作成されたためと推測される。今年上半期は BlueCrabの サンプル数や感染件数が GandCrabレベルには至らなかったが BlueCrabに関する RaaSが持続的に悪用される場合、下半期最悪のランサムウェアとして定着する可能性もある。

その他新たな登場には「Maze」ランサムウェアがある。同ランサムウェアは CVE-2018-8174と CVE-2018-15982の脆弱性を利用する Fallout エクスプロイトキットを介して拡散され、韓国の有名なセキュリティ企業の製品がインストールされたフォルダーを暗号化対象から除外するなど韓国ユーザーを対象に配布された件があった。

2019 年上半期韓国のマイナー(採掘マルウェア)統計

コインマイナー(Miner)はランサムウェア同様サンプル数と感染報告件数が昨年より減少した。2019年上半期マイナーサンプル数は 121万8千件で、前年同期 186万8千件に比べ 34.7%減となった。感染報告件数も 22万1千件で、前年同期 220万5千件より約 89.9%も減少した。



[図8] 2019年上半期マイナー統計(*サンプル数と感染報告件数)

2017年末、ビットコインなどの主な仮想通貨の価値が急騰し、マイナーのサンプル数と感染件数が共に上昇した。しかし2018年以降は仮想通貨の相場とマイナーマルウェアの推移が必ずしも同じ動きを見せていない。この傾向は今年上半期からより強くなっている。[図8]のように、今年 3月からビットコインの価値が着実に上昇しているにも関わらず、マイナーサンプル数と感染件数はむしろ減少している。

今年の上半期に広まったマイナーが主に採掘した仮想通貨は Moneroだった。韓国に配布されたマイナーのほとんどはどんな仮想通貨を採掘するにしてもビットコインで補償してくれるナイスハッシュ(Nicehash)アルゴリズムを採用していた。2019年上半期にビットコインの価値が再上昇したことで、一部攻撃者が採掘アルゴリズムにいち早く対応して変化させたものと思われる。仮想通貨の相場が以前ほどでないとしてもマイナーが完全に収束すると即断はできない。景気判断指数のように仮想通貨の価値が先行指数の指標になるとすれば、下半期にはマイナーサンプル数と感染報告件数が増加する可能性もあるのだ。

攻撃者の狙いは、安定的な収益源？

上半期ランサムウェアとマイナーが全体的に減少傾向を見せたのは確かに喜ばしい現象であり、そのマルウェアの変種について配布段階からタイムリーに対応できた証と評価できる。だが前述したように、全体的に減っているものの企業をターゲットにする標的型ランサムウェア攻撃に変化した部分に注目しなければならない。

一時は直接仮想通貨を採掘するマイナーが増加したことからランサムウェアが消滅するという予測もあった。だが現在、韓国だけでなく世界的にもマイナーよりランサムウェアのほうが企業のセキュリティに深刻な脅威となっている。

これは仮想通貨の相場が乱高下を繰り返し、攻撃者にとって安定的な収益源になれなかった点が増加にストップをかけた原因と予測されている。また仮想通貨の種類が多様化し、ビットコインなどのメジャーな通貨価値が攻撃者の期待値ほど上がらなかった点もある。攻撃者は収益性が下がったマイナーの代わりに、直接利益に繋がる企業をターゲットにしたランサムウェアに力を入れていると思われる。

さらに、ランサムウェアのターゲットが企業に移り、APT攻撃タイプに発展するという観測もある。

企業側はランサムウェア侵入経路から拡散や最初の感染ポイントに対する全体的な対策を用意しなければならない。特に WannaCryptorと Clop ランサムウェアのケースからわかるように、脆弱性へのセキュリティパッチ適用と共有フォルダーおよび重要システムの管理者アカウントの管理をしっかりと強化することが必要だ。

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)