アンラボ・セキュリティレター

Press Ahn

2016.8　Vol.32

「ランサムウェア」「標的型攻撃」…次なるキーワードは？

2016 年上半期脅威動向及び下半期予測

「ランサムウェア」「標的型攻撃」…次なるキーワードは？

昨年度の予測通り2016年上半期はランサムウェアの種類や攻撃量が激増し、多くの被害を発生させた。中では標的型攻撃や敵対的な意図を持つ攻撃者の大規模施設へのピンポイント攻撃も多発した。またエクスプロイトキット(Exploit kit、以下EK)にマルバタイジング(Malvertising[1])手法が結合したことで不特定多数を対象にした大規模なマルウェア感染もどんどん広がっている。モバイルの場合は、前年下半期に比べてRoot権限を悪用する悪性アプリが400%も増加した。

引き続き2016年下半期もランサムウェアの猛威とインフラ施設を狙ったサイバーテロや標的型攻撃が続く見通しだ。またブラックマーケット発マルウェアサービス(Malware-as-a-Service)の活性化によって、今後サイバー攻撃の範囲や手法がますます多様化し、フィンテック(Fintech)サービスを狙ったモバイルセキュリティ脅威が登場すると予想される。

今回のコラムでは、アンラボのグローバルセキュリティ対応組織「ASEC(AhnLab Security Emergency response Center)」の専門家たちが選定した2016年上半期脅威動向 Top5の分析と、下半期脅威予測 Top5をそれぞれ紹介した。

2016 上半期脅威動向 Top5

01 ランサムウェア激増

上半期はランサムウェアの種類・量が爆発的に増加して多くの被害が発生した。固有の特徴を持つ様々なランサムウェアが発見されただけでなく、RaaS(Ransomware-as-a-Service)の浮上によってこれらの配布を助長する役割を果たしたようだ。また活発化していたTeslaCryptが突然活動を終了した途端、CryptXXXが韓国の某有名コミュニティサイトで配布され深刻な被害をもたらした。その他MBR(Master Boot Record)を暗号化するPETYA、医療機関を狙ったSamSam、人質に取ったファイルを一時間に一つずつ削除するJigSaw、音声でランサムウェア感染の事実を知らせるCERBER、迷惑メールで世界を驚愕させたLocky、USBを通じて感染するZCryptorなどが上半期を代表するマルウェアとなった。そしてFlash、Silverlightなどソフトウェアの脆弱性を悪用するエクスプロイトキットによる配布も増加しつつある。これはユーザーも知らないうちに感染させるDrive-by-download手法を使って感染率を高めるとともに最大限の収益を上げる効果がある。国と地域に関係なく世界で同時多発的に発見されていることからもそのような傾向を裏付けている。

韓国では TeslaCrypt、Locky、CERBER、CryptXXXの感染が顕著だった。アンラボを始めとするセキュリティ業界では、ランサムウェア遮断のための診断に力を入れて事前検知・遮断機能を追加しながら持続的に取り組んでいる。

[1] Malicious Advertising、またはMalware+Advertisingの略語。Web広告にマルウェアを挿入してユーザーを攻撃するタイプ

02 「絶えず」「こっそり」標的型攻撃

標的型攻撃は攻撃対象が限定されているうえ、こっそりと進行されるため事前に把握することが難しい。

今年初頭に朝鮮の第4回目の核実験の後、政府と国家機関を騙った偽装メールが発見された。まもなくしてからセキュリティ会社の証明書が流出され、DRM[2]ソリューションを改ざんしたマルウェアが配布された事件もあった。また韓国の航空会社と軍需企業がハッキングで情報が流出され、軍関連サイトもハッキングされてサービス中止になったケースもある。

また海外でも様々な標的型攻撃が発生した。ウクライナ停電は発電所を攻撃したマルウェア「Black Energy」によるものと判明され、主要国の金融・保険サービスを主な標的にした「LatentBot」攻撃も発見された。Pawn Storm、又はSofacyで知られた組織が米国の外交部や民主党などを攻撃したケースもあった。標的型攻撃は金銭目的以外にも、政治、軍事、経済、外交などのトラブル状況で優位を占めるために実行する場合もある。

標的型攻撃を成功させるためには、まず攻撃対象に関する情報を事前に把握しておく必要がある。Twitter、Tumblr、LinkedIn、MySpace、GitHubなどのアカウント情報が大量流出された事件があったが、このような情報漏えいは攻撃者にとって格好の情報収集の場になり得るので注意が必要だ。

03 インフラ施設を対象にした多様な攻撃

2015年12月に発生したウクライナ停電と、2016年2月に起こったバングラデシュ中央銀行の1千億ウォン盗難事件はサイバー攻撃によるものだった。特にバングラデシュ中央銀行の件は国際銀行間通信協会(SWIFT)システムへの攻撃で、ベトナム、フィリピン、ウクライナでもSWIFTシステムに対する攻撃が見つかった。これらの大掛かりな攻撃と比較して今年初頭韓国で発生した交通案内システムのハッキング事件は子どものいたずら程度の件だったといえる。この他、鉄道システムのような交通施設と上水道、ダムを狙った攻撃の試みもあった。

通常大規模な国のインフラ施設はセキュリティが強固にできていると思われがちだが、前述の件やドイツ原子力発電所から旧型のマルウェアが今さら発見された点などを見ると、セキュリティの盲点はどこかしら存在しているようだ。社会インフラ施設は国民の安全とも密接な関連があるため利便性とセキュリティ性に対する適度なバランスを取ることが求められる。

04 Malvertising と Web エクスプロイトキット

エクスプロイトキット(以下、EK)がランサムウェア大量感染のために活用されてから多様なタイプが登場した。2016年上半期まで猛威を振るったAngler EKとNuclear EKの活動は終了したが、Magnitude EK、Neutrino EK、RIG EK、Sundown EKなど現在は色々なタイプのEKが活発に使用されている。またEKによるマルウェアの配布にMalvertising手法が結合したことから、アドウェア(Adware)のネットワーク又はサイトの広告バナーを利用してEKの多階層リダイレクション(Redirection)を悪用する。これにより不特定多数を対象に大量感染を引き起こし、配布源を特定できたとしても遮断が困難な状況が増えている。脆弱性を突いて配布されるマルウェアの多くは金銭目的のランサムウェアとファーミング(Pharming)に二分化されていたが、ランサムウェアの世界的な流行によりファーミングはたいして注目を集められなかった。ランサムウェアは仮想貨幣のビットコイン(Bitcoin)を狙ってヨーロッパを中心に活動し、ファーミングは東アジアを中心に口座情報を奪取して実際に貨幣を奪取する特徴を持っている。

[2] Digital Rights Management

05 ルーチング試みとRoot権限を悪用するアプリ増

2016年上半期はRoot権限を悪用する悪性アプリが多く発見された。悪性アプリがRoot権限を利用するのはユーザーがアプリのインストールを認知できないようにしてセキュリティプログラムの検知・駆除を難しくするためである。インストールされた悪性アプリはRoot権限を利用して個人情報の奪取、広告露出、ユーザーが望まないアプリをインストールするなどの悪性動作をする。2016年収集されたRoot権限奪取タイプの悪性アプリ数は、2015年下半期対比約400%も急増した。

最近発見された悪性アプリGodlessは、Android5.1バージョン(Lollipop)以下でRoot権限を奪取して複数の脆弱性を悪用することが判明した。このようなRoot権限奪取タイプの悪性アプリのほとんどは中国で作成され、インストールと広告から得る収益が目的であると推定されている。

2016 下半期の脅威予測 Top5

01 ブラックマーケット発マルウェアサービス(Malware-as-a-Service)

TORによる匿名化とダークWebの使用が楽になり、サイバーブラックマーケット発マルウェアサービス(Malware-as-a-Service、以下 MaaS)が活性化している。需要者のニーズに応じて提供者(Vendor)はサービス化(as-a-Service)を図り、MaaSからサイバー攻撃に必要なリソースを取り揃えることができる。MaaSが活気付いて提供者同士の競争も激化し、サイバー攻撃に必要なリソース単価がダウンしていく中、機能と種類は多様化している。MaaSを使えばマルウェアをオーダー・作成するだけでなく配布するために必要なゼロデイ脆弱性、難読化、エクスプロイトキット、spamネットワークに至るまで、サイバー攻撃を仕掛けるために必要な要素をお金さえ払えばすべて利用することができる。

MaaS形態のブラックマーケットでは、サイバー攻撃を企画・実行するために必要な専門知識をすべて「委託」という形で運用できる。これは誰でも攻撃者になれる環境が整ったということを意味する。これらの理由も相まって2016年上半期にはspamとエクスプロイトキットを使用したマルウェアの配布が急増した。MaaSを利用すれば攻撃に必要な様々なものを簡単に揃えることができるので今後発生するサイバー攻撃の範囲や様相はますます多様化すると見られ、DDos、ランサムウェア、金融マルウェアのようなオーソドックスな脅威に加えてインサイダーリスク、個人・企業の情報流出、標的型攻撃など幅広く悪用されると予想される。

02 社会インフラ施設向けサイバーテロは続く

社会インフラ施設に対する攻撃の成功率は一般的なハッキングより低いうえ、金融機関を対象にしたハッキングのような金銭的利益も発生しにくい。しかし一度成功すれば社会的混乱を巻き起こしたり、その宣伝効果は絶大なものがある。特に社会インフラ施設へのサイバーテロは通常のテロや軍事的攻撃に比べて追跡やリベンジが難しい。主に団体によるテロ行為や国レベルの攻撃に多く発生するが、金銭目的よりは宗教、政治的な動機が多く簡単に解決することはできない。

社会インフラ施設はネットワーク網が分離された状態で運用されているものが多いが、やはりインターネットに繋がるシステムは必ず存在し、使用者の立場では不便であることを理由にセキュリティを遵守しない者も多くいる。攻撃者はシステムの脆弱性を見つけ出すために様々な攻撃方法を駆使してくるだろう。不十分な対応は被害を拡大させる可能性があるため、しっかりと事前予防と対応をしなければならない。

03 ランサムウェア増加による被害増大

ランサムウェアのTeslaCrypt、Nuclear EK、Angler EKが上半期に活動を終了し、Lockyを拡散させるNercus Botnetがしばらくなりを潜めていたが最近またNercus Botnetが LockyとCERBERの拡散を再開し、活動を終了したAngler EKの空席はNeutrino EKが埋めつつある。RaaS(Ransomware-as-a-Service)が活性化されてランサムウェアが巨大な市場を形成し、今よりさらに多くのランサムウェアが出現すると見られる。MBRのみならずシステムの他領域まで暗号化対象を拡大する可能性や医療機関を狙うSamSamのように他分野に攻撃対象を拡大する可能性もある。最近はゼロデイ脆弱性を突いたMalvertising手法のせいで大規模な感染が起きているだけに、既知のランサムウェアがさらに領域を広げて被害を発生させる可能性が考えられる。

6月のBrexitの影響からビットコインの価格が急騰し、ビットコインを要求するランサムウェアの活動はさらに活発になる恐れがある。特にセキュリティ企業等の対応を迂回するため、多様な機能で武装した形態になるかもしれない。

04 信頼する共用ソフトウェアを利用した標的型攻撃

韓国で発見された標的型攻撃を見ると攻撃に使用されたマルウェアは主に中央管理ソリューションとWeb、メールを通じて拡散されていた。だが今後はこれに加えて内部で使用する共用ソフトウェアから感染するケースも加わる可能性がある。2016年初頭に発生したセキュリティ会社と全社資源管理(ERP)会社のデジタル署名盗用事件は、攻撃者が奪取した証明書で署名された悪性プログラムを作成してセキュリティ会社のDRM(Digital Rights Management)ソリューションを改ざんした件だった。これは内部で使用するセキュリティプログラムを悪用した攻撃手法で、共用ソフトウェアと運営サーバーに攻撃範囲を限定して配布したため長期間潜入が可能だった。

通常内部の配布サーバーを利用する共用ソフトウェアは内部ネットワークを通じて管理されるため、ユーザーはこれといって疑うことなく信頼して使用する。そのため流出された証明書によって改ざんされた共用ソフトウェアを内部の配布サーバーから配布しても、管理者と使用者に疑われることなく多数のシステムを掌握できる。こうなると発見すること自体大変で、その被害も拡大するしかない構造だ。

今後はこのような共用ソフトウェアの信頼区間を利用した攻撃方法がどんどん増加すると予想されるため注意が必要だ。

05 モバイル向けFintechサービスの脅威登場

Fintechサービスの増加によって金融情報を狙う悪意あるアプリが登場すると予想される。2014年末、Fintechがブームを起こし多様なモバイル簡単決済サービスが紹介された。最近は端末メーカーで直にサービスするモバイル簡単決済や、アプリを利用した決済サービスが幅広く使われている。このような決済サービスを悪用して金銭的収益を上げる悪質なアプリが登場する可能性がある。モバイル少額決済の脆弱性を狙った悪意あるアプリから、モバイルバンキングアプリに偽装して個人金融情報を奪取するアプリなど悪意あるアプリは続々出現している。

Fintechサービスが社会全般に普及していくとともに関連する脅威は持続的に登場するはずだ。

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)