2017年
5大脅威予測

アンラボ・セキュリティレポート

AhnLab

CONTENTS

2017年
5大脅威予測

01. 金ある所にランサムウェアあり 3

02. 一般的な攻撃ツールの進化 4

03. 内部侵入とシステム掌握の試み 5

04. 止まないインフラ・サイバーテロ 6

05. Internet of Things vs. Threat of Things 7

情報セキュリティ提言 2017 8~10

AhnLab

01.
金ある所に
ランサムウェアあり

2016年に激増したランサムウェア(Ransomware)は比較的簡単に稼げる犯罪手段として位置づけられた。特に企業の場合、ビジネスへの影響や顧客情報などの重要なデーターを失う恐怖から身代金(ransom)を支払うケースが少なくなかった。そしてランサムウェア作成・配布サービス(Ransomware as a Service、以下RaaS)まで登場し、需要と供給が立派に成立する一つの市場を形成するのに至った。

2017年ランサムウェアはさらに高度化されて攻撃範囲も広がる見通しだ。金銭的利得が目的なら「お金」が集まる場所に集まることは必須で、これまでのサイバー金融犯罪は偽サイトを利用して使用者情報を奪取するフィッシングとファーミングが主導したが、今後はランサムウェアがその中心に台頭すると思われる。その他、スピアフィッシング等と結合した手法や企業間の貿易取引代金を狙う犯罪組織の活動にも要注意だ。

02.
一般的な攻撃ツールの進化

わずか数年前までもサイバー攻撃は専門的なIT知識を持つハッカーやハッキンググループの所業と思われていた。しかし最近は暗市場のほかにも、ネット上でRaaS(ランサムウェア作成サービス)をはじめとして多様なスパムメール送信サービスを利用することができる。専門的なIT知識がなくてもマルウェアを作成して、サイバー攻撃を仕掛けることが可能になったのだ。サイバー攻撃の一般化は犯罪増加に繋がり、対応はますます難しくなるはずだ。

攻撃者は、スパムメールの添付ファイルと Webサイト訪問の際に自動でインストールする Drive-by-download攻撃を試みたり、ソフトウェアのセキュリティパッチをその都度適用しないユーザーが多いことから、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(以下、EK)を積極的に活用するなど、攻撃手法をさらに強化してくる。持続的に増加するEK攻撃に備えるためには定期的にサイトの改ざん有無を把握し、特にWebSellには格別な注意が必要だ。

03.
内部侵入と システム掌握の試み

2010年前後に発生したハッキングは、企業機密や企業が保有する個人情報を奪取するものがほとんどであった。しかし最近は単なる情報流出ではなく、企業インフラを掌握するための攻撃に変化しつつある。

特に今年は組織の内部インフラに侵入するための多様な手法が登場するだろう。攻撃に成功して感染システムを拠点に内部インフラへ侵入し、情報収集及び検索を通じてまずシステムのアカウント情報を入手する。アカウント情報の収集・活用を繰り返して内部システムの運営に関する権限を奪取すると、最終的にインフラ全体を掌握する。内部システムが掌握されると、またここを攻撃拠点にして該当企業のサービス利用に必要な正常プログラムになりすまし多数のPCにマルウェアをインストールできる。一度感染PCに繋がるとネットワーク上の別のシステムからまた別の企業システムが掌握される危険性もある。

04.
止まないインフラ サイバーテロ

2017年は世界的に地政学的な対立がさらに深化する見込みだ。国家間の理念的葛藤により国家機関や組織、企業を狙うサイバーテロも多発するだろう。最近の攻撃傾向としては、ターゲットを設定する際に不特定多数が利用するオンラインサービスだけでなく、サービスの種類や規模に関係なくほとんどの領域で拡がっている。社会インフラ施設攻撃など大規模なサイバーテロの背後には、主にテロ団体や敵対関係にある国家が動いていると推定されている。攻撃の動機も、金銭的な利益よりは宗教、理念、政治的な思惑によるものが大きい。特に社会インフラ施設への攻撃が成功する場合、社会的な混乱を引き起こして宣伝効果を最大化することから、今後とも持続的に発生する見込みだ。

ほとんどの社会インフラ施設の内部システムは、外部網とダイレクトに接続しない分離環境で安全に運営される。しかしただ一つでも外部のインターネット網に接続するシステムが存在していると、外部と内部を繋ぐポイントが存在することになり脅威から完璧に安全とはいえない。そしてセキュリティホールとしてヒューマンエラーが最大のネックとなる。強固なセキュリティであるほど不便であるため、コンプライアンスを守らないスタッフは必ずでてくるものだ。攻撃者はこのような脆弱性をキャッチして多様な方法を動員して攻撃を試みるのだ。

05.
Internet of Things vs. Threat of Things

モノのインターネット(Internet of Things, IoT)の発展はさらに加速化するだろう。だがIoT分野は未だセキュリティに関しては認識不足で、脆弱な製品のまま販売される恐れがある。この点を逃さずIoTマルウェアも増加していくはずだ。

昨年米国ではマルウェア「Mirai」に感染されたIoT製品を利用して大規模なDDoS攻撃が発生した。IoTは消費者のもとに送り出された後は管理することが容易ではなく、数年は初期状態のまま使用されることが多い。ユーザー側はメーカーがサポートするセキュリティパッチを適用すること以外これといった対応手段がない。第一線のメーカーでは、セキュリティの課題を悩むほどの余裕がなかったり、技術力不足を理由に未対応のままにしておくことも。ユーザビリティの面から節電と低コストが売りのIoTであるため、セキュリティ強化機能を追加したり値段を引き上げることが難しいのだ。

よって普及しつつあるIoT製品のセキュリティを強化するためには、メーカーだけでなくセキュリティ企業と政府レベルの有機的な協力が必要だ。競争が激化するIoT分野の規制を個別単位の国で対応するのではなく、企業や各国の政府が協力してチェックシステムの構築とセキュリティ強化ガイドラインをまとめることが急がれる。

2017年
セキュリティトレンドは
ここを注目せよ

サイバー闇市場にはマルウェアの作成・配布サービス(Ransomware as a Service、以下RaaS)が定着し、これをベースに新しい犯罪生態系が形成された。一度生態系が造成されたからにはさらに多様なマルウェアが生産されるはず。またマルウェア同士の競争によってRaaSはさらに発展し、セキュリティ脅威は高度化されるだろう。

これを受けて、守り手はインシデントが発生したり必要性があった際にやっと導入していたソリューション情報を一つにまとめて管理しようとするニーズが生まれる。セキュリティ業界では、収集した情報を効果的に処理して最新の脅威に対応するための「自動化」、「マシンラーンニング」など多様な技術的アプローチを試みる一年になりそうだ。

AhnLab

Trend 1. 機械学習（マシンラーニング）登場

新しい技術研究の中で膨大なデータを分析するために登場したデータマイニングや機械学習などの技術がセキュリティ分野でも定着する年になるだろう。高度化する脅威に対応するために複数のセキュリティソリューションを導入したものの、これらを管理する人手不足や質的な限界は常に存在する。人の知識で実現したことを技術で紐解く過程を通じて、その間人海戦術で運営してきたセキュリティを技術ベースにシフトする動きは進むはずだ。オーソドックスなセキュリティシステムでは意味をなさなかった領域から、新しい情報を見つけるケースも出てくるに違いない。機械学習など技術との接点を通じて、専門的なアナリストに引けをとらない結果を打ち出すと思われ、ここから生じるリソースの余分は新しい分野やビジネスに投入されるポジティブな循環作用を形成する。

Trend 2. セキュリティ領域の細分化と統合管理へのニーズ

IoTとクラウドに代表されるIT環境の変化の時代、プラットホームとサービス領域のセキュリティニーズが増加するだろう。多様な体験の場を通じて最新技術への一定の理解を身に付けた企業は、各産業分野に適した技術とサービスを業務に適用していく。当然セキュリティ要素の配慮も同時に行われ、それぞれの環境に相応しいセキュリティ技術とソリューションを選択することになる。現在細分化されているセキュリティ領域を全体的に管理しながら、効果的な対応を可能にする統合セキュリティに対する具体的なニーズが浮上してくるはずだ。脅威情報を読み解く可視化は必須で、発見した問題点を解決する効果的な対策が求められるだろう。

Trend 03. 攻撃ツールの普及と悪の境界線

わずか数年前までもサイバー攻撃は専門的なIT知識を持つハッカーの領域であった。しかし現代ではサイバー闇市場だけでなく、ネットでも普通にスパムメール送信サービスや RaaSまでもそう手間をかけずに見つけることができる。

IT知識がない人でもサイバー攻撃を仕掛けることができるようになったのだ。主要プログラムの脆弱性を狙うEKの攻撃技法がアップグレードして、サイバー攻撃がさらに横行する可能性が高い。

RaaSによるサイバー攻撃の大衆化によって、ますます攻撃者の特定や対応は困難になる見通しだ。サイバー攻撃の範囲を最小化するためには、やはりセキュリティパッチに対する使用者の認識向上が求められる。従業員のセキュリティパッチ適用を強制し、効率的に管理するための対策やソリューション投資を検討することが望ましい。

結論:
すべては「人」の成せる技

最近世界で発生しているインシデントのほとんどは、特定の組職に属する者やグループを標的にして実行されたケースが多い。攻撃技法もピンポイントで特定の人やグループ宛てメールを送信し、添付ファイルを展開するように誘導する「Spear　Phishing」や、特定の人が利用するWebサイトをハッキングしてマルウェアを配布する「Watering Hole」手法などがある。
一連のケースで注目すべきは標的型攻撃もまたマルウェアの流入から始まり、管理外のPCやサーバーが橋渡しをしている点だ。インシデントを事前に遮断するために多様なソリューションを構築して専門サービスを利用することも大事だが 、さらに重要なのはこれらをどう活用するかである。セキュリティ管理者レベルでソリューション導入で十分だと性急に判断したり、ユーザーの安易なセキュリティ認識によって、インシデント発生の可能性は高まってくる。

すべての最初と最後には「人」がいる。
2017年は各ソリューションとサービスを効果的に運用するための努力に加えて、常にネックとなるセキュリティホール「人」への教育と管理が両立されるべきだ。内部の一般ユーザーからセキュリティ管理者、企業責任者に至るまで、人から発せられるセキュリティ問題を最小化するための努力が継続して行われるべきだ。

AhnLab

2017年
5大脅威予測

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。

発行所　株式会社アンラボ
発行者　AhnLab Security Emergency Response Center
編集　アンラボ・コンテンツ企画チーム

〒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）
© 2017 AhnLab, Inc. All rights reserved.

著作権者の許可なくこのコンテンツの内容の全て又は一部をいかなる手段においても複製・転載・流用・転売・複写等することを固く禁じます。

AhnLab.com

AhnLab

2017年
5大脅威予測

AhnLab