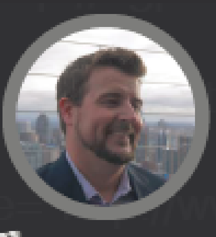
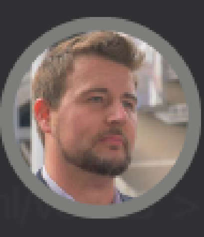
2017 SECURITY PREDICTIONS

身近に迫るセキュリティの脅威

2016年は、IoTボットネット、CaaS (Crimeware as a service)、Cryptランサムウェアなど、サイバー攻撃が急増した年となりました。2017年には、いったいどのようなセキュリティ事件が世界中のニュースで取り上げられるのでしょうか？ランサムワームからサイバー戦争による民間人犠牲者まで、WatchGuard Technologies CTO、Corey Nachreiner による2017年のセキュリティ予測をご紹介します。


OVERVIEW


TOP SECURITY TRENDS


SUMMARY OF PREDICTIONS

1 2017年にランサムウェア ワームが登場し、ランサムウェアの拡散が加速する。

CodeRedやConfickerなどのネットワークワームに見られる自動増殖の特性をサイバー犯罪者が使うようになることで、2017年は、ランサムウェアが新たなレベルへと進化するでしょう。ランサムウェアが自己複製を無限に繰り返してネットワーク全体に感染が拡散するような状況は想像したくありませんが、自己増殖型ランサムウェア、すなわち、ランサムワームが登場して大混乱するのは時間の問題です。

2 攻撃対象プラットフォームと攻撃方法の両面で、それぞれに特化した IaaS (Infrastracture-as-a-Service)が使われるようになる。

クラウドの採用は、企業や組織の規模にかかわらず、驚異的な割合で増加しています。クラウドプラットフォームが企業の業務運営に深く関わるようになればなるほど、サイバー攻撃の格好の標的になるでしょう。攻撃手段と攻撃対象プラットフォームの両面で、それぞれに特化した公開済のIaaS(Infrastructure-as-a-Service)が使われるようになるはずです。2017年には、公開されているIaaSが標的になったり、利用されたりする、サイバー攻撃のニュースが、報告されると予想されます。

3 IoTデバイスがボットネットゾンビの最大の標的となる。

2016年にIoTボットネットであるMiraiのソースコードが流出し、犯罪者が大規模ボットネットを構築して、過去最大のトラフィック量によるDDoS 攻撃による事件が発生しました。 攻撃者がこの方法でのIoTデバイスの武器化を着々と進めていることから、2017年には、DDoS攻撃がさらに深刻化すると予想されます。脆弱性が解決されずに製造されたデバイスがインターネット接続されれば、そのような脆弱性を悪用した新たなタイプの攻撃が大量に発生する可能性が高まります。
犯罪者がIoTに特化した大規模ボットネットによるクリックジャッキング攻撃やスパム攻撃を開始し、従来のコンピューターボットネットと同じ方法を新たな攻撃に取り入れて、金銭を要求するようになるでしょう。

4 国家間のサイバー戦争で民間人の「犠牲者」が出る。

国家間のサイバー戦争がすでに始まっていることから、2017年には、少なくとも1人以上の「民間人」の犠牲者が何らかの被害を受けると予想されます。数年前から、マルウェアを使って他国の核遠心分離機を攻撃したり、民間企業から知的財産を盗み出したり、政府の機密情報システムに侵入したりする国家間のサイバー攻撃が既に発生しています。
現段階で、米国、ロシア、イスラエル、および中国が戦略的サイバーセキュリティ作戦を進めており、ゼロデイ脆弱性が狙われています。政府自らがこのように脆弱性を狙った攻撃を繰り広げていることから、間違いなく、民間企業や個人が未公開のゼロデイ脆弱性を悪用した攻撃の犠牲になるでしょう。

5 サイバー犯罪の増加に伴い、中小企業がMSSPを自社のサイバーセキュリティに活用するようになる。

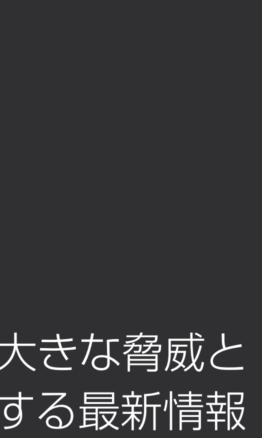
サイバー犯罪者が常に攻撃対象を拡大していることから、中小企業は引き続き、ネットワークセキュリティに優先して取り組まなければならないでしょう。IT部門が少なく、専任のセキュリティ専門家が不在であり、自社のセキュリティ対策を構成、監視、調整するリソースがない中小企業は、身近な管理サービスプロバイダ(MSP)を活用してこの問題を解決しようと考えるでしょう。そのため、MSP側でも、自らの基本ITサービスにセキュリティサービスを追加しようとするはずです。2017年には、小規模企業の4分の1以上が、専門のMSSP(マネージドセキュリティサービスプロバイダ)を利用して、自社のセキュリティニーズを解決するようになり、この割合は年を追うごとに増加するでしょう。

6 生体認証の普及で、認証情報に対する懸念が表面的には沈静化するが、パスワードはなくならない。

認証情報の漏えいが数年にわたり、立て続けに発生したことで、指紋認証などの生体認証技術がパスワードの代替手段として広く採用されるようになるでしょう。また、漏えいのニュースが次々と報道されたことで、認証方法としてのパスワードの有効性が疑問視されるようにもなりました。
生体認証がパスワードに代わる便利な認証方法として広く採用されるようになり、最も一般的な認証方法になる可能性がありますが、オペレーティングシステムの中核には弱いパスワードの問題が引き続き存在し、脆弱性が解消されるわけではありません。

7 マルウェアや攻撃に機械学習やAIが活用されるようになる。

サイバーセキュリティ関連企業は、2017年に、機械学習の恩恵を受けるのが自分たちだけではないことに気付き、慌てることになるでしょう。セキュリティ業界は既に、マルウェア対策に機械学習を活用することで、人間だけでは予測できない多くの脅威を事前に予測し、対応型から予測型への移行を推進してきました。機械学習を活用したシステムは、膨大なデータと大量の正規ファイルおよび不正ファイルを分析して分類することで、情報セキュリティの専門家が未発見の脅威を根絶するのに役立つパターンを認識します。ところが、サイバー犯罪者側もこのような技術を取り入れるようになり、機械学習を活用して高度化された新たなマルウェアが登場して、機械学習によるマルウェア対策に戦いを挑むようになるでしょう。



サイバー攻撃は、2017年以降も引き続き企業にとって大きな脅威となります。情報セキュリティに関する脅威と解決策に関する最新情報を日頃から収集しておく事が、防御を向上させる最善の方法です。

詳しくはウォッチガード・テクノロジー・ジャパンまでお問合せ下さい。

WatchGuard

ウォッチガード・テクノロジー・ジャパン株式会社
東京都港区麻布台1-11-9　CR神谷町ビル5階
TEL: 03-5797-7205　mail: jpnsales@watchguard.com