8つの出来事を予測:

防御不能マルウェアやインフラ標的の同時多発サイバー攻撃――ウォッチガードが2019年のセキュリティ動向を予測

http://www.atmarkit.co.jp/ait/articles/1811/29/news061.html

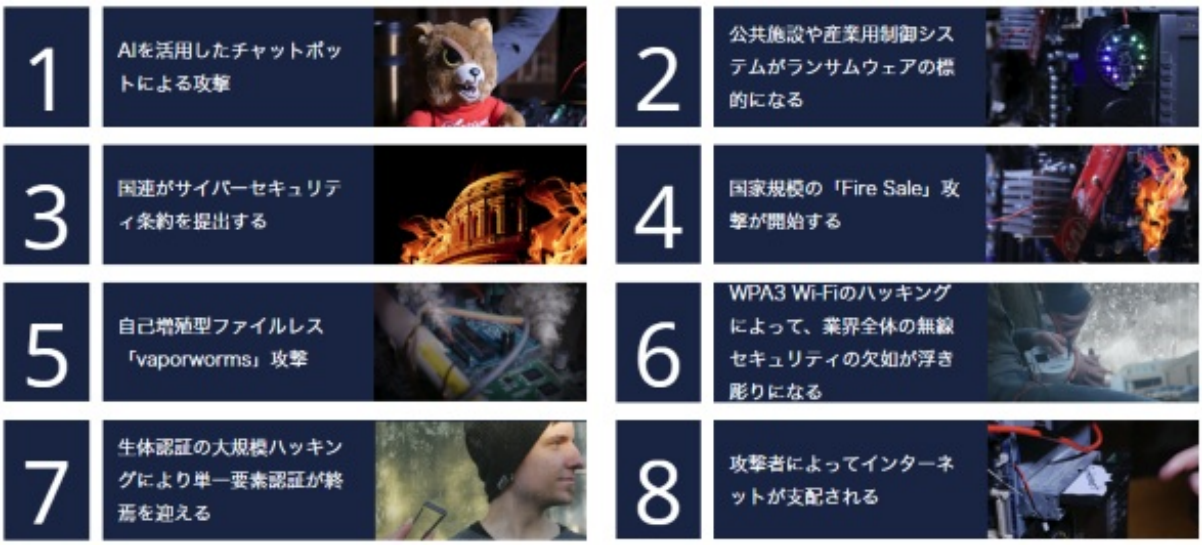
ウォッチガードは、情報セキュリティについての2019年度の動向を予測した。過去の主な脅威に関するトレンドを分析した結果だ。従来の検知機能では防御できないファイルレスマルウェアの拡散や、国家によるサイバー攻撃を背景とした国連でのサイバーセキュリティ条約成立などを挙げた。

2018年11月29日 11時00分 更新

[@IT]

ウォッチガード・テクノロジー・ジャパンは2018年11月27日、情報セキュリティについて2019年度の動向予測を発表した。脆弱(ぜいじゃく)なシステムを介して自己増殖するワームのような性質を持つ新種のファイルレスマルウェア「vaporworms」や、インターネット上のコンテンツを削除する攻撃、公共機関や産業制御システムを標的としたランサムウェアなどが広まると予測した。

今回発表された予測は、ウォッチガードの脅威ラボ調査チームが、過去の主な脅威に関するトレンドを分析して作成した。予測には、次の8項目が挙げられている。



2019年度セキュリティ予測(出典:ウォッチガード・テクノロジー・ジャパン)

まず、ファイルレスマルウェアワーム「vaporworms」が台頭すると予測した。この種のマルウェアは感染システムにファイルを残さず、全てメモリ上で動作する。そのため、従来のエンドポイントの検知機能では特定したり防御したりすることが困難だ。

ウォッチガードによれば、セキュリティパッチを当てていないソフトウェアを稼働させているシステムが多いことを考慮すると、2019年はvaporwormsの拡散が懸念されるという。

2つ目は、攻撃者によるインターネットの支配だ。2019年にはインターネットに対し、ハッカー集団や国家によって組織的な攻撃が仕掛けられる恐れがあるという。インターネットを支える複数のクリティカルポイントや、インターネットを制御するプロトコル（Border Gateway Protocol：BGP）にDDoS攻撃が行われ、インターネットが危険にさらされることが考えられるとしている。

この予測の根拠は、2016年にホスティングプロバイダー「Dyn」に対して発生したDDoS攻撃だ。ホスティングプロバイダーや登録機関への単体攻撃で主要なWebサイトを削除できることが明らかになっている。

3つ目の予測は、国連でサイバーセキュリティ条約が成立すること。これは2つ目の予測と関連したもので、国家が背後で支援するサイバー攻撃の増加を受けた対応だ。国連が、こうした攻撃に対して強い意志を持って取り組むと予測した。

その他、AI（人工知能）を活用したチャットbotによる攻撃、生体認証の大規模ハッキングによる認証の多要素化、映画「ダイハード」シリーズに登場したフィクションの「Fire Sale」攻撃の現実化、公共機関や産業制御システムを標的としたランサムウェアによる都市機能のまひ、WPA3 Wi-Fiネットワークのハッキングを挙げた。

このうちのFire Sale攻撃は、都市や州の交通システムや金融システム、公共機関、通信インフラを標的とした同時多発サイバー攻撃。映画では、この攻撃によって引き起こされた混乱に乗じてテロリストたちが大金を搾取する。

ウォッチガードでは、国家やテロリストはこうした攻撃能力を既に備えていることが、最新のサイバーセキュリティインシデントの分析によって導かれるとしている。

関連記事

特集　セキュリティレポート裏話

2018年も「金銭狙い」で変化続けるフィッシング、最新の手口は
世の中で知られるようになってから10年以上が経つが、いまだに被害が減るどころか、スマートフォンの普及によって新たな手口が登場しているフィッシング。月次・年次で報告をまとめているフィッシング対策協議会に最近の動向と対策を尋ねた。

GDPRや仮想通貨を狙う次世代のサイバー攻撃、NTTデータがレポート公開
NTTデータは、サイバーセキュリティに関する「グローバルセキュリティ動向レポート」を公開した。GDPRや仮想通貨を狙ったサイバー攻撃がエスカレートすることを予測した。既存の攻撃に対してはランサムウェア対策を続けるべきだという。

関連リンク

プレスリリース

2019年セキュリティ予測