Kaspersky Security Bulletin 2014:

2015年サイバー犯罪の予測

KASPERSKY lab · GREAT

サイバー犯罪とAPTの融合

2015年はサイバー犯罪活動が新たな進化を遂げ、金銭の搾取を目的とするオンライン犯罪活動に、APTの戦術と技法が用いられることが予測されます。

最近の調査で確認された攻撃では、ある銀行の経理担当者のコンピューターがマルウェアに感染し、多額の送金手続きに悪用されていました。これは、銀行に対する直接的な標的型攻撃が行われた注目すべき傾向といえます。

APTの戦術をそのまま用い、銀行に侵入するマルウェアの事例は急激に増加しています。銀行のネットワークに侵入できれば、攻撃者は必要な情報を収集し、次のような方法で銀行から直接金銭を搾取することが可能になります。

— 遠隔操作でATMにコマンドを送り、現金を引き出す

— 銀行の顧客の口座からSWIFT送金を実行する

— オンラインバンキングシステムを操作して、密かに送金を実行する

こうした攻撃は、サイバー犯罪の世界でAPT型の攻撃が用いられつつあるという、新しい傾向を示しています。

APTグループの分裂と攻撃の多様化

2014年、複数のAPTグループによるサイバー犯罪が公表されたことがきっかけで、あるハッカーグループが米国企業に対するスパイ活動の容疑で起訴されました。

Kaspersky Labのグローバル調査分析チーム（Global Research and Analysis Team: GReAT）は、国家主導のAPTグループの摘発を続けていますが、2015年には大規模なAPTグループが小規模な単位に分裂し、個々に独立して活動すると予測しています。この変化によって攻撃拠点が拡大し、グループの小規模化に伴って攻撃も多様

化するため、攻撃を受ける企業の数が増えることになります。同時に、これまでは2、3の大規模なAPTグループ（Comment CrewやWebkyなど）に攻撃されていた大企業も、より多くの攻撃者からさまざまな攻撃を受けることになるでしょう。

古いコードに起因する新たな脆弱性

最近では、暗号化の実装に意図的な改変や意図しない不備が見つかったり（「goto fail」問題）、必須のソフトウェアに致命的な脆弱性が見つかる（Shellshockや、OpenSSLにおけるHeartbleedなど）という報告が相次いだことから、未監査のソフトウェアはいまも警戒の対象となっています。これまでの対策は、主要なソフトウェアを個別に監査するか、セキュリティリサーチャーが確認しながら致命的な脆弱性を見つける（非公式な監査に等しい）というものでした。引き続き、2015年も古いコードから危険な脆弱性が新たに見つかり、インターネットインフラストラクチャが危険な攻撃にさらされると考えられます。

ATMに対する攻撃の増加

現金自動預け払い機（ATM）に対する攻撃は今年になって爆発的に増えています。いくつもの事件が公表され、世界各国の捜査当局がこの危機への対応を急いでいます。こうした事例が広まることで、ATMは格好の標的であることが知れわたり、サイバー犯罪者にも察知されることは明白です。大半のATMはWindows XPで稼働しており、また、物理的にもセキュリティが不十分なケースが多く、金融機関の現金を無人で守る機械としてはかなり脆弱と言えます。サイバー犯罪者が真っ先にATMを狙ってくることは確実でしょう。

2015年には、APTの手法を用いてATMの「中枢部」に侵入することで、ATMへの攻撃はさらに進化するものと予測されます。次の段階として、攻撃者は銀行のネットワークに侵入し、攻撃に必要なアクセスレベルを使用してリアルタイムでATMを操作すると考えられます。

MACに対する攻撃:OS Xのボットネット

AppleはMac OSの保護に取り組んでいますが、torrentや海賊版ソフトウェアパッケージを通じて拡散する悪質ソフトウェアは後を絶ちません。Mac OS Xデバイスの人気の高まりに伴い、サイバー犯罪の世界でも注目が集まるようになり、犯罪者にとってOS Xプラットフォーム向けのマルウェアを開発することがますます魅力的になっています。OS Xは本来クローズドエコシステムであることから、マルウェアに完全に乗っ取られることは困難です。しかし、OS Xのセキュリティ対策が機能しないユーザーが一部に存在し、その多くは、海賊版ソフトウェアを使用するユーザーです。つまり、さまざまな理由からOS Xシステムを乗っ取ろうとする攻撃者は、必要なソフトウェアにマルウェアを忍ばせる(おそらくキージェネレータの形で)だけで、攻撃の成功率を簡単に上げられるということをわかっています。OS Xプラットフォームは安全という定説が広まっているため、感染を防御するマルウェア対策製品がインストールされていないことも多く、一旦マルウェアに感染すると、長期間にわたって気づかないことも考えられます。

券売機に対する攻撃

チリの公共交通機関に対するNFCハッキングなどの事例から、交通機関のような公的リソースの悪用が注目を集めていることは明らかです。一方で、攻撃で利益を上げることには興味がなく、ほかのハッカーと攻撃手法を共有し、ある種の「ただ乗り」や「権力に対する反抗」だけで満足するハッカーもいます。しかし、発券システムの脆弱性が明らかになりつつあり(多くの券売機でWindows XPが稼働)、このシステムでクレジットカードの取引データを直接処理している都市も少なくありません。発券システムに対する攻撃は、愉快犯的な攻撃や、クレジットカードデータを盗み出す目的など、さらに大胆になっていくものと予測されます。

仮想決済システムに対する攻撃

サイバー犯罪者は可能な限りシンプルかつ効率的に、大胆なエクスプロイトを仕掛けて利益をあげようとします。サイバー犯罪者にとっては、初期段階にある仮想決済システムは大変魅力的な標的です。エクアドルなど一部の国は仮想決済システムの導入を急いでおり、サイバー犯罪者はこのシステムを悪用できる機会があれば必ず狙ってくるでしょう。ユーザーに対するソーシャルエンジニアリング、携帯電話に代表されるエンドポイントへの攻撃、銀行への直接的なハッキングなど、どのような手口を使うにせよ、サイバー犯罪者は直接の利益につながるあらゆる攻撃を仕掛けてきます。仮想決済システムがその矢面に立つことは間違いないでしょう。

こうした懸念は、NFC（近距離無線通信）を利用して無線で取引を処理するApple Payにも波及する可能性があります。Apple Pay、バーチャルウォレット、その他の仮想決済システムにおける脆弱性が、今後も頻繁に見つかると予測しています。

APPLE PAY

これまでの主な攻撃対象はNFC（近距離無線通信）決済システムでしたが、NFCの普及が限定的だったため、攻撃によって得られる利益も限られていましたが、この状況はApple Payによって変わるでしょう。Apple Payは非常に大きな関心を集めているため、一気に普及する可能性があります。その結果、必然的に多くのサイバー犯罪者がApple Payの決済から利益を得ようと考えるでしょう。Appleの設計は、決済データの仮想化など以前よりセキュリティが重視されていますが、ハッカーがこの機能をどのような形で悪用するのか、大いに懸念されます。

「モノのインターネット」に対する攻撃

「モノのインターネット」（IoT）に対する攻撃は、概念実証型に限られており、スマートテレビや冷蔵庫がハッカーに狙われてボットネット化したり、悪質な攻撃に利用されたりする可能性が過剰気味に警告されています。

ネットワークに接続するデバイスが増えるにつれて、セキュリティとプライバシーに関する議論が同企業の間で盛んになると予測されます。2015年には、ネットワークプリンターなど、ネットワークに接続したデバイスに対する攻撃が実際に行われ、高度な技術を持つ攻撃者は企業ネットワーク内に潜伏して、ラテラルムーブメントを継続することが可能になるでしょう。特に、製造プロセスや工業プロセスにインターネット接続が導入されており、攻撃に値すると考えられる標的では、IoTデバイスがAPTグループが利用する兵器の一つになると見られます。

コンシューマー側では、IoTに対する攻撃はプロトコル実装における脆弱性か、スマートテレビにアドウェアやスパイウェアが組み込まれるといった程度にとどまるでしょう。