2019 年 9 月 27 日

サービス＆セキュリティ株式会社 e-Gate センター

標的型攻撃の最近のトレンド

1. 概要

標的型攻撃(Targeted Attack)は特定の組織内の情報を狙って行われるサイバー攻撃の一種で近年、増加傾向となっています。情報処理推進機構(IPA)が選んだ「情報セキュリティ 10 大脅威 2019」でも第一位にランク入りしており、手口も年々、巧妙化されています。

主に攻撃の対象とされる組織・企業には政府／公共サービス機関、製造業が多く、価値の高い知的財産を保有している組織が狙われやすい傾向にあります。しかし近年は、大企業のセキュリティ対策の向上に伴い、単純な標的型攻撃は成功しにくい状況となっています。そのため、従来通り直接、標的の大企業を攻撃するのではなく、セキュリティ対策がまだ十分に実施されていない関連企業を間接的に狙う攻撃(サプライチェーン攻撃)が増えています。

2019 年 8 月 20 日には近畿地方整備局の電気通信施設の保守業務を受注しているインフラ管理会社にて標的型攻撃による情報流出の疑いが発表されています。標的型攻撃メールを開いたために第三者から不正アクセスされ、情報を流出した疑いがあるというものでした。流失した可能性があるファイルには近畿地方整備局の資料が含まれていました。これは近畿地方整備局を間接的に狙ったサプライチェーン攻撃と考えることができます。

セキュリティ事故を引き起こすと会社の信用やイメージの低下は免れることができません。企業として適切なセキュリティ対策を講じることは会社のイメージアップや顧客の満足度にも繋がる重要な要素です。本ニュースでは標的型攻撃の最近の傾向と対策についてご紹介致しますので是非、皆様のセキュリティ対策にご活用ください。

2. 攻撃手法

標的型攻撃手法として下記 5 点が従来から使用されている攻撃手法です。現在も主要な攻撃手法となっています。

（１）標的型攻撃メール

攻撃者が標的型攻撃を開始する際に行われる手法として多いのが、ソーシャルエンジニアリングを悪用して標的の組織の構成員に対してマルウェアなどの不正プログラムを送りつける「標的型メール」という攻撃手法。

（２）ウェブサイト閲覧

メールの Web リンクによる誘導だけではなく、ウェブブラウザやそのプラグインの脆弱性を悪用し、ウェブサイトを閲覧させることによって不正プログラムを送り込む攻撃。

（３）バックドアによる攻撃

組織内部のサーバにアクセスできるようにするため、コンピュータに不正プログラムを感染させることによってバックドアを設置し、遠隔操作する攻撃。

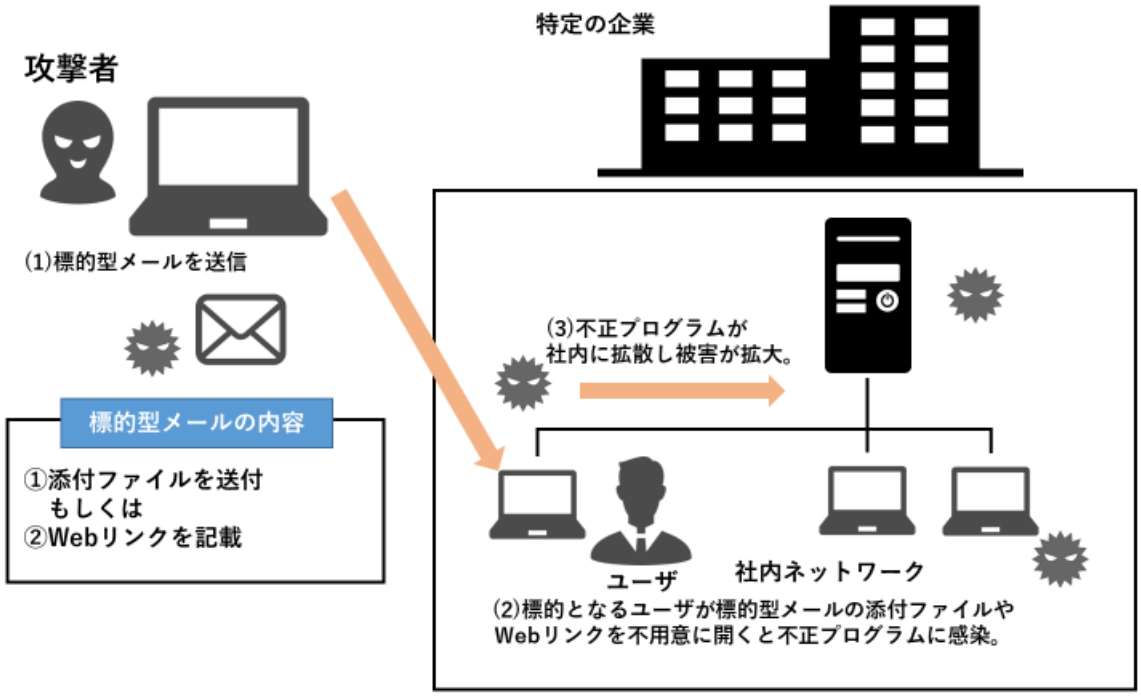
（４）APT 攻撃(Advanced Persistent Threat:持続的標的型攻撃)

特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続する攻撃。

（５）サプライチェーン攻撃

製品やサービス提供をするために行われる一連のビジネス活動の流れで、セキュリティ対策を強化している大企業を狙わず、関連の中小企業でセキュリティ対策が手薄な企業を狙い、そこを踏み台にして大企業を攻撃するサイバー攻撃。

以下の図１は標的型攻撃メールによる典型的な例です。



【図１：典型的な標的型攻撃】

3. 最近のトレンド(傾向)

■内部活動後に攻撃展開

統計としても標的型攻撃の法人での被害は増加傾向にあります。トレンドマイクロ社のレポートによると、同社への 2019 年上半期のランサムウェア感染被害の報告件数は 37 件と前期比で約 1.5 に増加しています。インシデント対応についても、ランサムウェア感染を起点とする事例が目立ってきています。トレンドマイクロ社の調査によると、攻撃者はネットワーク内に侵入した後、内部活動を経てシステムにランサムウェアを感染させる攻撃が行われたことが明らかとなっており、今後は「一部への侵入を前提とした対策」が重要となってきています。

■サプライチェーン攻撃

概要でも述べさせて頂きましたが、特に注目が集まっているのが「サプライチェーン攻撃」というサイバー攻撃です。大企業のセキュリティ対策向上により、攻撃者としても標的の大企業に簡単に攻め込めなくなっています。そこで直接、標的の大企業を攻撃するのではなく、関連企業(主に中小企業)を攻撃し、間接的に大企業を攻撃するという傾向が増えてきています。

サプライチェーン攻撃を防ぐためには取引相手の複数の企業に対して基準(ガイドライン)を設けて、セキュリティ対策を講じていく必要があると考えられています。

(「サプライチェーン攻撃については以前、弊社の e-Gate セキュリティニュースで詳細を紹介しております。興味のある方は 2019 年 2 月の e-Gate セキュリティニュースをご参照ください。」)

■米国のガイドライン

米国の取り組みとしては NIST SP800-171 という米国政府機関が定めたセキュリティ基準を示すガイドラインが 2015 年 6 月に発行されました。これは政府機関だけではなく、取引企業からの情報漏えいを防ぐため、業務委託先におけるセキュリティ強化を要求する内容になっています。この基準に満たない複数の企業製品が米国防権限法により、2019 年 8 月に政府調達から閉め出されています。

また、米国防省と取引をしている全世界の企業に対して NIST SP800-171 への準拠が要求されており、米国防省と取引をする企業は NIST SP800-171 への対策は避けられない状況になっています。米国政府だけの取り組みにとどまらず主要国でも米国に追随する動きが始まっており、NIST SP800-171 に準拠しない企業とその製品やサービスは、グローバルサプライチェーンからはじき出されてしまう恐れがあります。

4. 対策

■侵入を前提とした対策 「多層防御」

システム全体で 1 箇所でもセキュリティが甘い箇所があれば攻撃の被害にあってしまうことを防ぐことはできません。年々、巧妙化するサイバー攻撃を防ぐためには、1 箇所でセキュリティを破られても別のやり方で防御して被害拡大を防ぐという「多層防御」が主流の考え方となっています。

多層防御は主に、「攻撃者にとっての“攻撃コスト”を上げ、攻撃するためのハードルを上げること」と「攻撃が行われた場合の検知力・防止力を向上すること」の 2 点によってセキュリティを向上させる考え方になります。

多層防御の構成要素としては主に下記のような対策があります。

カテゴリー	対策
物理セキュリティ	現場機器のロックダウン
	認証システムの構築
ネットワークアーキテクチャ	DMZ の構築
	仮想 LAN の構築
ネットワーク境界セキュリティ	ファイアウォールの設置
	一方向ゲートウェイの設定
	認証システムの構築(リモートアクセス時)
セキュリティ監視	侵入検知システム（IDS）の導入
	侵入防止システム（IPS）の導入
	セキュリティチームによるログ取得及び監視
エンドポイントセキュリティ	侵害時のアクティビティ調査ツールの導入
	侵害端末の隔離
	NGAV(※1)・EDR(※2)等の侵害検知システムの導入
	定期的にユーザのアクティビティを検査し、リスクアセスメントを実施
人的セキュリティ	サイバー攻撃を受けたと仮定した訓練
	要員のセキュリティ教育

【表 1：多層防御(主な構成要素)】

※1: NGAV(Next Generation Anti-Virus)は従来では検知できないサイバー攻撃に対処するために進化した次世代アンチウイルスプログラムのこと。

※2: EDR(Endpoint Detection and Response)は「エンドポイントの検出およびレスポンス」と訳され、エンドポイントセキュリティのうち、セキュリティの脅威を検知し、対応を支援すること。

インターネットの境界にファイアウォールを構築すれば、攻撃者は内部ネットワークに侵入しづらくなります。IPS などのセキュリティ機器を導入すれば、脆弱性への攻撃を検知・遮断することができ、常時、セキュリティログを監視すれば、インシデントを早期に発見し対応することができます。このように複数のセキュリティ対策を講じることで、総合的にリスクを軽減することができます。

■関係会社も含めたセキュリティ管理

サプライチェーン攻撃の対象となる範囲は広く、一社員から経営者まで含めた組織全体に渡ります。サプライチェーン攻撃を効果的に防ぐためには、ネットワークへの侵入を監視し防御する IPS や、端末の挙動を監視する EDR など導入が必要です。今後としては、一つのセキュリティ担当部署に任せた運用ではなく組織全体が、一団となった取り組み・改善が求められています。

サプライチェーン攻撃を防ぐのには下記 3 点が必要だと考えられています。

・ネットワークへの不正侵入を防ぐ IPS の導入

・EDR 導入による端末の不正な挙動の監視

・取引先や関連会社を含めた啓発とセキュリティ対策の向上

■ガイドラインに適合するセキュリティレベルへの引き上げ

米国のセキュリティ基準のガイドライン(NIST SP800-171)の導入により、日本政府としても日本の防衛産業をハイレベルなセキュリティのモデルとすべく、防衛調達の新基準を NIST SP800-171 と同等にすることを 2018 年 9 月に決定しました。これにより日本の各企業もサプライチェーン攻撃に対する対策を進めなければ、ビジネスに影響が出る可能性が十分に考えられます。

現状、日本企業では NIST の基準に則ったセキュリティ対策を進めている企業はごくわずかであるため、今後の動向として関連企業を含めた組織全体のセキュリティ改革が必要となって来るでしょう。

5. 参考情報

IPA(独立行政法人 情報処理推進機構)

- 情報セキュリティ 10 大脅威 2019
  https://www.ipa.go.jp/security/vuln/10threats2019.html

ScanNetSecurity

- 近畿地方整備局の保守業務事業者へ標的型メール攻撃、設備資料 6 件が流出可能性（国土交通省）
  https://scan.netsecurity.ne.jp/article/2019/08/21/42813.html
- 標的型攻撃手法でのランサムウェア感染被害が法人で増加（トレンドマイクロ）
  https://scan.netsecurity.ne.jp/article/2019/09/06/42894.html

6. e-Gate の監視サービスについて

Firewall や IPS をはじめとするセキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。“e-Gate”の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。“e-Gate”の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター”この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp