2018 年 12 月 21 日

サービス＆セキュリティ株式会社 e-Gate センター

2018 年の振り返りと長期休暇における情報セキュリティ対策

1. 概要

2018 年も残すところあと僅かとなり、年末年始の長期休暇も目前に迫ってまいりました。
今年も様々なサイバー攻撃が発生し、独立行政法人情報処理推進機構 IPA などの各団体から、脆弱性に関する注意喚起が多くされました。
年末年始など長期休暇の時期は、サイバー攻撃や、クリスマスなどのイベントに乗じたスパムが増加する傾向にあります。
しかしその一方でセキュリティインシデントが発生した際、企業のシステム管理者やセキュリティ担当者などの不在によりその発見が遅れる可能性があり、より一層の注意、対策が肝要となります。
当セキュリティオペレーションセンター（以下、e-Gate センター）からも、今年流行したサイバーセキュリティトレンドを振り返ってご紹介し、長期休暇前後、期間中に実施すべき情報セキュリティ対策について記載致します。

2. 2018 年のサイバーセキュリティの振返り

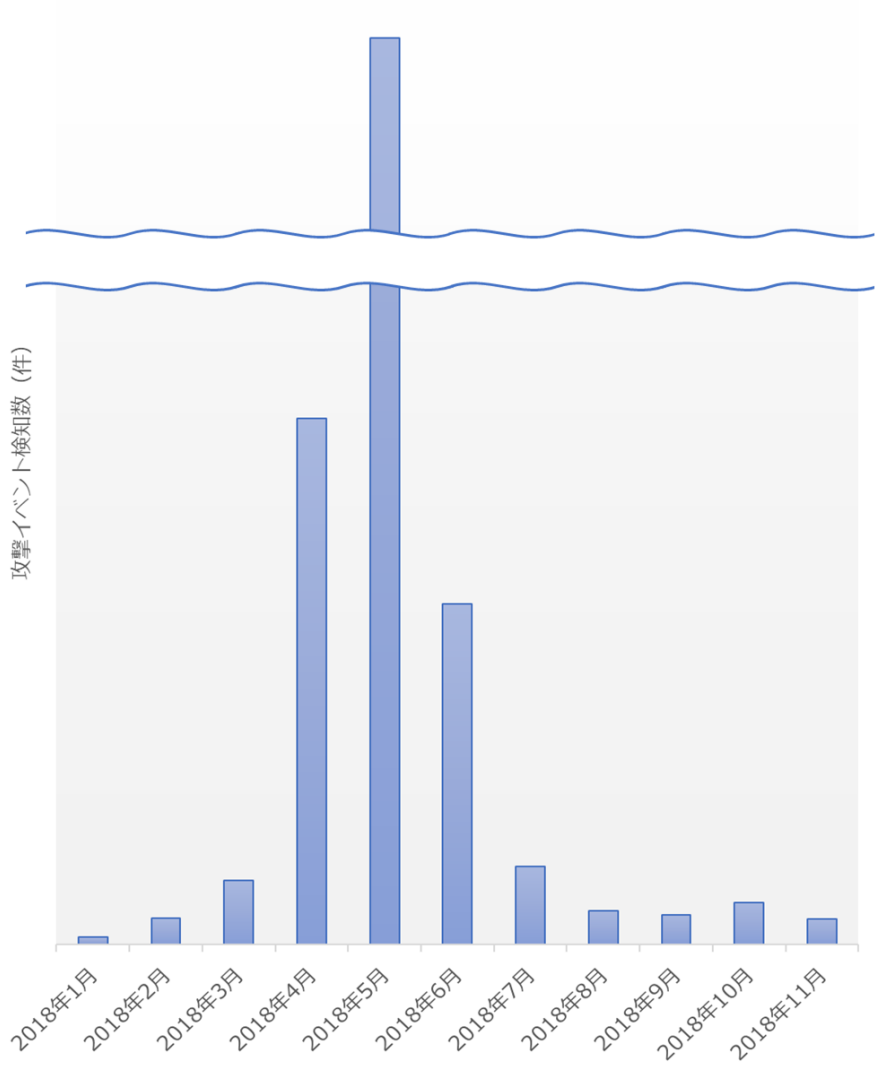
（1） 仮想通貨に関連した脅威について

2018 年は、仮想通貨に関するニュースが多数メディアで取り上げられました。サイバーセキュリティのトレンドとしても、ソフトウェアの脆弱性を悪用し、サーバにマイニングさせて、攻撃者が収益を得ようとする手法が話題となりました。
この様な攻撃の手法やその対策について情報を取りまとめたニュースを、e-Gate センター及びグループ会社セキュアソフトより発行しておりますので、詳しくは下記 URL をご参照下さい。
また、長期休暇中にこれらの被害に遭わぬよう、本章『3.長期休暇時の情報セキュリティ対策について』に記載しております対策を実施してください。

【2018 年に流行した仮想通貨に関連する攻撃や脅威】

- 注意喚起：WebLogic Server の脆弱性を突いた攻撃について
  https://www.ssk-kan.co.jp/topics/?p=9093
- 注意喚起：Drupal の脆弱性を狙った攻撃について
  https://www.ssk-kan.co.jp/topics/?p=9115
- 注意喚起：クリプトジャッキングの脅威について
  https://www.securesoft.co.jp/news_mt/2017/12/2-1/

前述の攻撃の中から、e-Gate センターで検知した攻撃を代表して「WebLogic Server の脆弱性（CVE-2017-10271）を悪用した攻撃」について、検知の状況を以下に記載します。
下記のグラフは、2018 年 11 月時点の e-Gate センターの監視システムにおいて、当脆弱性を狙った攻撃イベント検知数の推移を示しています。
攻撃検知数のピークは過ぎておりますが、現在も継続的に検知されており、年末年始にかけて増加する可能性も考えられますので、依然として注意が必要となります。



【図 1　WebLogic Server の脆弱性（CVE-2017-10271）を狙った攻撃イベント数の推移】

（2） 電子メールを介した脅威について

IPA が発表している「情報セキュリティ 10 大脅威」の組織編において、2018 年を含めここ数年の脅威第 1 位は、「標的型攻撃」関連であり、その主な攻撃のきっかけはメールだと言われています。
標的型攻撃はそのほとんどの場合、企業や民間団体や官公庁など、特定の組織を狙って攻撃が行われ、メールの添付ファイルを開かせたり、悪意あるウェブサイトにアクセスさせたりしてウイルスに感染させ、組織内の PC やサーバに感染を拡大させます。最終的に業務上の重要情報や個人情報が窃取され、大きな損失が出てしまう可能性が高く、注意が必要です。
また第 3 位には、昨年まで 10 大脅威に入っていなかった「ビジネスメール詐欺による被害」がランクインしています。ビジネスメール詐欺では、関係者になりすましてメールをやりとりすることにより、企業の担当者を騙し、攻撃者の用意した口座へと送金させます。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもあります。
長期休暇明けには、多数のメールが溜まっていることが想定されますので、誤って不審なメールの添付ファイルを開いたり、本文中の URL にアクセスしたりしないよう、十分注意をしてください。

今年は、マクロ実行の許可を必要とせずにメールを通じてマルウェアに感染させる「マクロレスファイル攻撃」や、金融情報の窃取を目的としたマルウェア「バンキングトロージャン」に感染させる、添付ファイル付きのメールによる攻撃が流行しました。
攻撃手法やその対策など詳細につきましては、e-Gate センター及びグループ会社セキュアソフトより発行しております過去のニュース（下記 URL）をご参照ください。

【2018 年に流行したメールを介してマルウェアに感染させる攻撃の手法や対策】

- マクロレスファイルを用いた最新の攻撃手法
  https://www.ssk-kan.co.jp/topics/?p=9355
- 注意喚起：バンキングトロージャンに感染させる拡張子"iqy"添付ファイル付きメールの国内大量拡散について
  https://www.securesoft.co.jp/news_mt/2018/08/iqy-1/

◆ 参考情報

- 独立行政法人情報処理推進機構（IPA）
  情報セキュリティ 10 大脅威 2018
  https://www.ipa.go.jp/security/vuln/10threats2018.html

3. 長期休暇時の情報セキュリティ対策について

一般的な対策は、「長期休暇前」、「長期休暇中」、「長期休暇明け」の三段階に分類され、システム管理者だけでなく、一般社員、職員など利用者全員が、情報セキュリティ対策を適切に行うことが大切です。
IPA 及び JPCERT/CC より、長期休暇に備えた情報セキュリティ対策について紹介がされております。対策のポイントを下記にまとめておりますので、身の回りのセキュリティ対策が適切になされているか、今一度見直してみてください。

[長期休暇前]

1. 最新の修正プログラムが適用されているかを確認する
2. 休暇中に使用しないサーバ等の機器は電源を OFF にする
3. インシデント発生時の対応方法・手順、連絡体制を明確にしておく
4. 重要データのバックアップを取得する

[長期休暇中]

1. 持ち出し機器やデータの管理を厳重にする
2. SNS に不要な情報を公開しない様、投稿内容や投稿範囲に注意する
   （SNS への投稿により長期休暇中である事が知られてしまう可能性もある）
3. 必要のない PC 等は電源を切っておき、施錠可能な場所へ保管しておく

[長期休暇明け]

1. 休暇中に修正プログラムが公開されている場合があるので必ず確認し、修正プログラムを適用する
2. 休暇中に不審なアクセスなどが発生していないか、サーバ等のログを確認する
3. 休暇中に持ち出した PC については、社内 NW へ接続する前にウィルススキャンを実施する
4. Web サーバで公開しているコンテンツが改ざんされていないかを確認する
5. 新年のごあいさつメールなどが偽装されている場合があるのでリンク等に注意する

◆ 参考情報

- 独立行政法人情報処理推進機構（IPA）
  長期休暇における情報セキュリティ対策
  https://www.ipa.go.jp/security/measures/vacation.html#section2

- JPCERT/CC
  長期休暇に備えて
  https://www.jpcert.or.jp/pr/2018/pr180002.html

4. “e-Gate” の活用について

前述の年末年始の長期休暇における対策を行った上で、よりセキュリティ対策を強固にするために、“e-Gate”の MSS の導入をぜひご検討ください。e-Gate サービスでは年末年始などの長期休暇においても、24 時間 365 日で監視をしております。
サイバー攻撃への対策として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い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。
“e-Gate” のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

■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、全方位でのセキュリティサービスを展開しております。

【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標、または商標です。

«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