- VOL. 94 -

月刊 赤松事務機 通信

2023 7

この7月から 73期 に突入しました！今後とも宜しくお願い致します！！！

IPA『情報セキュリティ10大脅威2023』解説書より

今年1月にIPAが公開した、『情報セキュリティ10大脅威2023』の中から、組織1位の『ランサムウェアによる被害』の解説書をご紹介します。

【1位 ランサムウェアによる被害】～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

ランサムウェアと呼ばれるウイルスにPCやサーバーが感染すると、端末のロックや、データの暗号化が行われ、その復旧と引き換えに金銭を要求される。さらに、暗号化だけではなく、重要な情報を窃取されることもあり、その情報を公開すると脅す。このように複数の脅しを組み合わせる(四重脅迫等)ことで、ランサムウェアに感染した組織が金銭を支払わざるを得ない状況を作り出そうとする。

<攻撃者> ● 組織的犯行グループ ● 犯罪者 **<被害者>** ● 組織 ● 個人
<脅威と影響> PCやサーバーのデータを暗号化し、業務の継続を困難にした上で、データを復旧することと引き換えに、金銭を要求する等の脅迫文を画面に表示するランサムウェアと呼ばれるウイルスの被害が確認されている。暗号化前に重要情報を窃取し、金銭を支払わなければ窃取した情報を公開すると脅迫する「二重脅迫」も確認されている。脅迫に従うことによる金銭的被害に加え、窃取された重要情報(組織の機密情報や個人情報等)の漏えいにより信用の失墜にもつながるおそれがある。また、DDoS攻撃(Distributed Denial of Service Attack：分散型サービス妨害攻撃)を仕掛ける、被害者の利害関係者等へ連絡するといった脅迫を加えた「四重脅迫」も確認されている。なお、金銭を支払ったとしても、データの復旧や漏えいした情報の削除が行われるとは限らない。
<攻撃手口> ◆ **メールから感染させる** メールの添付ファイルやメールの本文中のリンクを開かせることでランサムウェアに感染させる。 ◆ **ウェブサイトから感染させる** ウェブサイトの脆弱性を悪用して、ランサムウェアをダウンロードさせるように改ざんしたウェブサイトや攻撃者が用意したウェブサイトを閲覧させることでランサムウェアに感染させる。 ◆ **脆弱性を悪用しネットワークから感染させる** ソフトウエアやOSの脆弱性対策をしないままインターネットに接続されている機器に対して、その脆弱性を悪用してインターネット経由でランサムウェアに感染させる。 ◆ **公開サーバーに不正アクセスして感染させる** 意図せず外部公開されているリモートデスクトップポートに不正ログインしてランサムウェアに感染させる。
<事例または傾向> ◆ **脆弱性を悪用してランサムウェアを配置** 2022年3月、東京コンピュータサービスは2021年末に発生したランサムウェアの被害の経緯等をまとめた資料を公開した。それによると、攻撃者は、社員向けAD(Active Directory)のパスワードの変更やリセット機能を提供するウェブサービスに、リバースプロキシサーバーを介して接続し、同ウェブサービスの脆弱性を悪用してADサーバーに侵入したという。そして、2021年10月初旬から不正侵入を繰り返し行い、社内管理情報や顧客の情報等を窃取した。その後、同ウェブサービスの脆弱性を悪用して、ランサムウェアを自動的に配布するバッチファイルを配置し、12月31日早朝、組み込まれたバッチファイルが自動実行され、組織内の機器がランサムウェアに感染した。 ◆ **リモートデスクトップ経由によるランサムウェア感染** 2022年6月、ヴィアックスは同社の勤怠管理システムのサーバーがランサムウェアに感染し、従業員1,871人分、退職者2,167人分等の情報が暗号化されたことを公表した。データセンター内のDMZ(DeMilitarized Zone：非武装地帯)上にある勤怠管理システムのウェブサーバーがメンテナンス用に外部からリモートデスクトップ接続が可能となっており、ウェブサーバーへのパスワードの総当たり攻撃により不正侵入されたものとみられる。そして、ウェブサーバー上でランサムウェアを実行され、ウェブサーバーからアクセスできるサーバーのファイルが暗号化された。 ◆ **二重脅迫だけでなく、四重脅迫も横行** 2022年9月、トレンドマイクロは法人組織におけるIT部門の意思決定者を対象に調査した「ランサムウェア攻撃 グローバル実態調査2022年版」を公開した。調査結果では、過去3年間でランサムウェア攻撃の被害を受けたのは日本法人の34.5%に及ぶ。脅迫はデータの暗号化、窃取情報の暴露、DDoS攻撃予告、攻撃を受けていることの暴露といった内容である。これらを組み合わせて最大で四重の脅迫まで確認されている。被害を受けた組織の内、67.1%が2つ目の脅迫である窃取情報の暴露、74.3%が4つ目の脅迫である攻撃を受けている事の暴露に関する脅迫を受けたことが明らかになった。
<対策/対応> **組織(経営者層)** ● 組織としてのランサムウェア対応体制の確立 ・インシデント対応体制を整備し対応する **組織(システム管理者、従業員)** ● 被害の予防 ・ インシデント対応体制を整備し対応する ・ 表1.3「情報セキュリティ対策の基本」を実施 ・ 多要素認証の設定を有効にする ・ メールの添付ファイル開封や、メールやSNSのリンク、URLのクリックを安易にしない ・ 提供元が不明なソフトウエアを実行しない ・ サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う ・ 共有サーバー等へのアクセス権の最小化と管理の強化 ・ 公開サーバーへの不正アクセス対策 ・ 適切なバックアップ運用を行う ● 被害を受けた後の対応 ・ 適切な報告/連絡/相談を行う ・ 適切なバックアップ運用を行う ・ 復号ツールの活用 ・ インシデント対応体制を整備し対応する

<身代金の支払いと復旧業者の選定について>
要求された身代金を支払ってもデータの復旧や情報の流出を防げるとは限りません。また、対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧し、最終的に自組織が身代金を支払ったとみなされるおそれもあります。対応を依頼する業者の選定にも注意が必要です。

出典：IPA(情報処理推進機構)「情報セキュリティ10大脅威2023」解説書より
https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

赤松事務機株式会社
香川県高松市塩上町1丁目7番13号 TEL：087-833-3434 FAX：087-835-2485
URL：https://www.akamatsu-jimuki.co.jp

赤松事務機株式会社
代表取締役　片松　保佳

『社長のつぶやき VOL.68』

7月になりました。ここ数日、暑い日々が続いております。夏が本格的にやってきたな～と感じます。屋外で仕事をされている皆様も多いと思いますが、水分・塩分補給・十分な休憩などご自身を守る行動を心よりお願いいたします。

さて、冒頭にも記載がございますが弊社は7月から第73期に入りました。毎年期初に感じることは「今まで社業を継続してこれたことに対する感謝」です。それもひとえに本通信をご愛読いただいております皆様のおかげございます。この場をお借りして心より感謝申し上げます。6月30日の期末と7月1日の期初は特別な感情が湧いてきます。本当に有り難く・感謝の気持ちで一杯になり、少し感傷に浸ってしまいます。とはいえ、また新しい期がスタートしておりますのでスタッフ一同気を引き締めて今期もお客様のお役に立てるように精進して参ります。

今月号では恒例(？)となっております出張報告をさせていただきます。

- 6月6日　関西コニカミノルタbizhub会総会　@神戸
- 6月22日　WithSecure主席研究員　ミッコ・ヒッポネン氏講演会　@東京
  お取引先でもあり情報セキュリティの世界的権威でもあるミッコ・ヒッポネン氏の講演会でした。
  日本語訳にされた著書：「インターネットの敵」とは誰か？　～サイバー犯罪の40年史と倫理なきウェブの未来～をサイン入りでいただきました。30年以上にわたりF-secure（現WithSecure）で経験されたサイバー世界のお話はとても衝撃的でした。著書の冒頭に"「スマートならば脆弱である」－ヒッポネンの法則"と1ページに1行だけで記されていたのが印象的でした。
- 7月13日　ChekPoint　Spark Summit参加　@東京
  こちらもお取引先であるCheckPointの最新ソリューション・導入事例・他社製品比較等の実演を交えたプログラムがございました。他社比較では製品カタログでは記載されていない項目についての比較や実際にランサムウェア・バックドアなどのマルウェアを装置に通した際の検知率・各メーカの明るみになっている脆弱性の数の比較などをスライドで説明していただきました。

WithSecureはフィンランド、CheckPointはイスラエルの会社です。両社とも業界以外の方にはそれほど認知されていませんが、情報セキュリティ業界ではとても名の知られている会社です。また、世界的に見てもフィンランドとイスラエルはサイバー先進国でもあり政治的にも日本と友好関係がありますので安心感があります（日本政府はイスラエルとサイバーセキュリティ分野で協力関係にあります。）。両社とも皆様に自信を持ってご案内できるメーカーさんです。

表面に引き続き、サイバーセキュリティ関係の話が多くなってしまいましたが、何か起こってから弊社にご相談いただくことがほとんどです。できるだけセキュリティリスクを下げる対策を日頃からしておきたいものです。

IT用語

■ センドバック保守 ■

『センドバック保守』とは、メーカー直送修理サービスのことです。

故障や不具合が発生した製品をメーカーや販売店へ送ると、修理や代替品との交換を受けられます。
保証期間内は無償、以降は有償の場合が一般的です。

[先出しセンドバック]　メーカーや販売店側が代替品を発送し、利用者が代替品と入れ替わりに故障品をメーカー側に送り返す方式

[後出しセンドバック]　利用者が故障品をメーカーや販売店に発送、あるいはメーカーの手配した運送業者に引き取ってもらい、メーカー側がこれを修理・交換して送り返す方式。この場合、修理・配送期間中はその製品を使用出来ません。

弊社では、情報セキュリティ対策商品、UTM(統合脅威管理)等の取扱いをしております！
HPでも紹介しておりますのでぜひご覧頂ければと思います!!!
対策は早目にしましょう！