資料1

最近のサイバー動向について

2020 年 11 月 26 日

名和 利男

1. 2020 年における象徴的なサイバー攻撃と得られた教訓

1-1. 防衛関連企業へのサイバー攻撃

（発生事象）

- NEC が、2014 年頃に北陸地方の子会社でネットワーク侵害を受けた。
  - 出典：NECにサイバー攻撃　中国系集団関与疑い　海自情報流出か
    https://www.tokyo-np.co.jp/article/1619
- 三菱電機が、2019 年 3 月に中国拠点でネットワーク侵害を受けた。
  - 出典：不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）
    https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf
- NTT コミュニケーションズが、 2020 年 5 月にシンガポール拠点でネットワーク侵害を受けた。
  - 出典：当社への不正アクセスによる情報流出の可能性について（第 2 報）
    https://www.ntt.com/content/dam/nttcom/hq/jp/about-us/press-releases/pdf/2020/0702.pdf

（得るべき教訓）

- 「サイバー脅威主体」は、ターゲットが属する企業グループの中で侵害可能（脆弱）な箇所を特定することが可能な情報を獲得することができる、或いはすでに保有している。（サイバー脅威主体及びその活動について、適宜かつ的確な動向把握を怠っていた。）
- 企業グループ間のネットワークにおいてセキュリティ（異常）検知の機能が組み込まれていない。（グループ全体のセキュリティ司令塔が整備されていない。）
- 防衛事業領域で発生していた同種サイバー事案に関する積極的な情報収集及び分析評価を（組織として）実施していない。（数年前から、防衛事業領域においてセキュリティや更新管理システムの乗っ取り被害が増加傾向にあった。）

1-2. イスラエルとイランの重要施設へのサイバー攻撃

（発生事象）

- 2020 年 5 月 24 日から 25 日にかけて、イスラエル国内の複数の水道局施設においてサイバー攻撃が発生し、水道局の全職員に対して、次の指示が出された。
  - 「水道施設のシステムのパスワードを直ちに変更すること」
  - 「特に運用システムと塩素管理に重点を置くこと」

- 「パスワードを変更できない場合は、システムをインターネットから完全に切断すること」

- この攻撃の挙動と被害は、次のとおり。
  - イランが作成した悪意のあるコードが、米国とヨーロッパのサーバーを経由してルーティングされた上で、ポンプ場の制御システム（水ポンプを遠隔操作する市販のソフトウェアコントローラー）に到達した。
  - この攻撃により、塩素が急増したポンプ場が自動的に安全停止し、数万人の民間人や施設への給水が制限された。

（得るべき教訓）

- 重要システムに組み込まれているソフトウェア（業務運用、保守管理、セキュリティ対策などすべて）の脆弱性管理を徹底しても、コンポーネント（構成要素）レベルまでの管理は不可能である。（ソフトウェア・サプライチェーン管理は莫大な人的リソースとコストがかかる。）
- メーカー、運用・保守委託者、データセンター、セキュリティ会社などの関係会社における侵害防止のためのセキュリティ対策を完全に徹底させることは事実上不可能である。（国家レベルの支援が求められるが、日本は司令塔不在（関係省庁に広く分散）の状況。）
- 複数の「国家の支援を受けている攻撃主体」は、敵対国の重要施設に侵害しようとすることができる能力をすでに保有している。（現時点では、「サイバー犯罪グループ」は、その能力を保持していない。）

1-3. Twitter の重要システム（ユーザー管理システム）へのサイバー攻撃

（発生事象）

- 2020 年 7 月 15 日、Twitter において有名人や大手企業の公式(認証済み)アカウントが一斉に乗っ取られ、同アカウントから暗号通貨詐欺を狙ったツイートが投稿された。
  - 被害を受けたのは、ビル・ゲイツ氏(マイクロソフト創業者)、イーロン・マスク氏(テスラ共同創設者)、ジェフ・ベゾス氏(アマゾン共同創設者)などの企業家、ジョー・バイデン氏(米民主党の大統領候補)、バラク・オバマ氏(前米国大統領)といった政治家、アップルやウーバーといった企業、Bitcoin や Coinbase といった暗号通貨関連の公式(認証済み)アカウントであった。
- 社内のサポートチームのみが利用できるツールを使って 130 のアカウントが攻撃を受けた。当初、送金先が同一であることから単独犯による犯行とみられた。
- 判明した攻撃プロセスは、次のとおりである。
  ① 2020 年 7 月 15 日、攻撃者は「数名の従業員」に電話スピアフィッシング攻撃を成功させ、社内システム(Slack)のアカウントを、複数の手段(アカウントに紐づけられているメールアドレスの変更等の 2 段階認証回避)で不正アクセス(乗っ取り)した。
  ② 最初に標的にされた「数名の従業員」は、重要システムである「アカウントサポート・ツール」の使用許可を持っていなかったが、攻撃者は彼らの Slack アカウントを使用して、何らかの方法(非公開)で、社内プロセスに関する情報を入手した。

③ 攻撃者は、この社内プロセスに関する情報を利用して、「アカウントサポート・ツール」を操作するアクセス権を持つ従業員を標的にした攻撃（ソーシャルエンジニアリング等）を仕掛けて、「アカウントサポート・ツール」の資格情報（ログイン情報）の窃取に成功した。

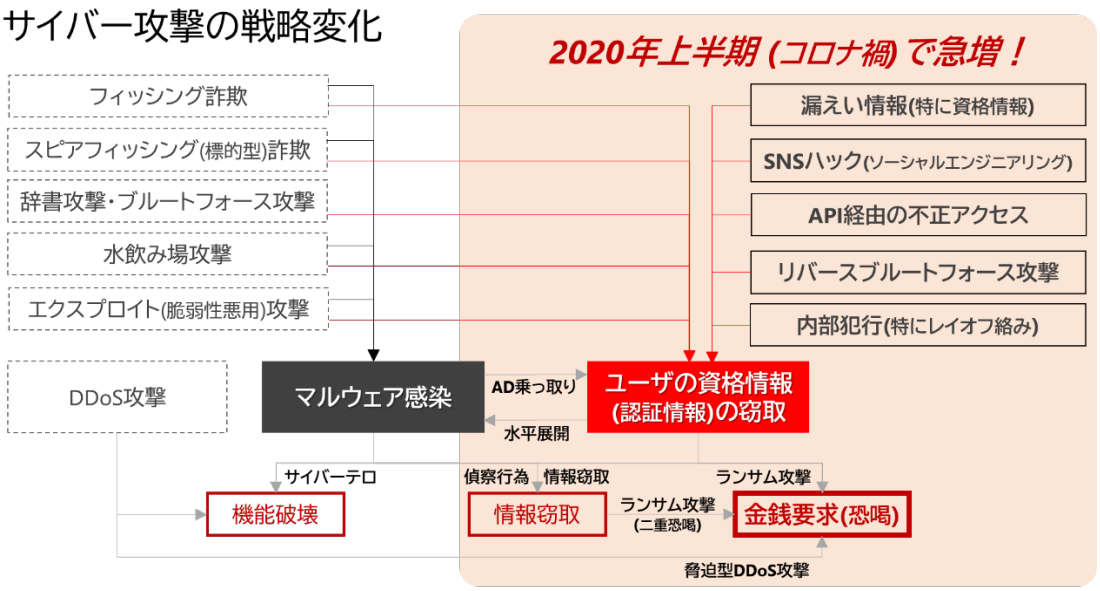
④ 攻撃者は、「アカウントサポート・ツール」に不正ログインして、130 アカウントの乗っ取り、45 アカウントによる偽ツイート、36 アカウントの DM（ダイレクトメッセージ）トレイへの不正アクセス、7 アカウントのユーザ詳細データのダウンロードを行った。

（得るべき教訓）

- 「個人のサイバー攻撃者」は、重要システム周辺の従業員及び彼らの電話番号を入手し、電話スピアフィッシング攻撃(phone spear phishing attack)を仕掛けることができる。（サイバー攻撃の動向把握を怠っていた。）
- 社内ネットワーク（システム）を通じて、重要システムへのアクセスを可能にする「社内(業務)プロセス」情報が、一般従業員のアカウントでも入手可能な状況となっていた。（ネットワーク境界防衛の概念に依存しすぎていた可能性がある。）
- 重要システムに、単純な資格情報だけでアクセス（操作）可能な状況となっていた。（物理デバイスを伴う多要素認証を利用していなかった。）

2. 2020 年におけるサイバー脅威の戦略変化

従来の「マルウェア感染」に加えて、「ユーザの資格情報の窃取」が急増した。



（了）