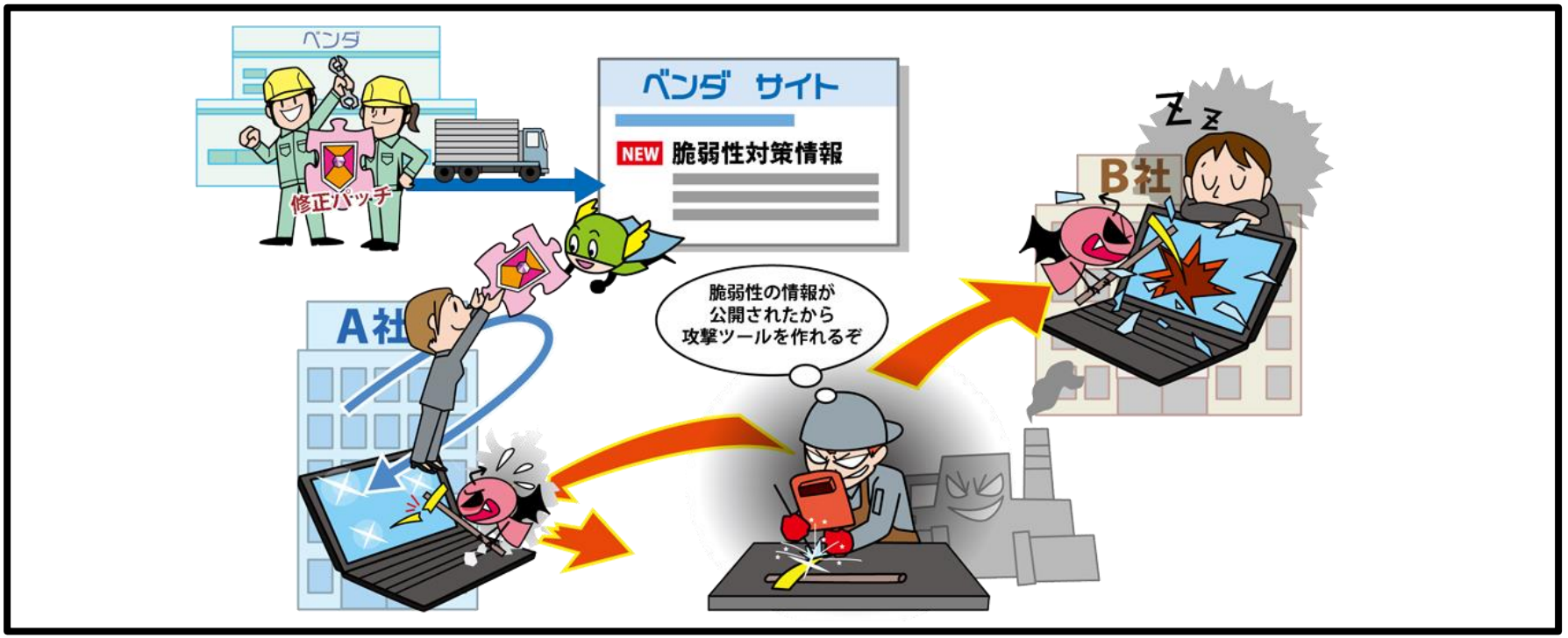
【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～



- 脆弱性対策のために公開された**脆弱性情報を攻撃者が悪用**
- 脆弱性情報の公開後、攻撃コードが流通して**攻撃が本格するまでの時間が近年は短くなっている**傾向
- 広く利用されている製品の脆弱性の場合は被害が大きくなる

Copyright © 2023　独立行政法人情報処理推進機構

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

● 攻撃手口

・公開された脆弱性情報を悪用して攻撃する
・対策が未実施もしくは時間を要している相手を狙う

■ 対策前の脆弱性を悪用

・対策情報が公開されてから**利用者が対策を完了するまでの時間**に存在する脆弱性（Nデイ脆弱性）を悪用

■ 公開されている攻撃ツールを使用

・公開された脆弱性を悪用する攻撃ツールは**短期間で作成されインターネット上（ダークウェブ等）に出回る**

・オープンソースのツールに**脆弱性を利用する機能**が実装される場合があり、それを悪用されることも

Copyright © 2023 独立行政法人情報処理推進機構

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

- 2022年の事例/傾向①
  - 修正未実施の機器を狙った攻撃 (※1,2)
    - 2022年5月4日(米国時間)、F5 Networksが同社のネットワーク製品BIG-IPの**脆弱性を公表**
    - 脆弱性を悪用されると、遠隔の第三者に認証を回避され、任意のコードの実行や不正な操作をされるおそれ
    - 5月9日にセキュリティベンダーからPOC(実証コード)が公開され、その前後から**修正パッチが適用されていない機器を探索する通信や脆弱性を悪用する試みが観測**された

【出典】
※1 K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388(F5, Inc.)
https://support.f5.com/csp/article/K23605346
※2 「BIG-IP」脆弱性に注意 - 実証コード公開済み、探索や悪用も(Security NEXT)
https://www.security-next.com/136392

Copyright © 2023 独立行政法人情報処理推進機構

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

- 2022年の事例/傾向②
  - 「Spring4Shell」を狙った攻撃(※1,2)
    - 2022年3月31日（米国時間）、Vmwareが、JavaのWebアプリ開発を行うためのフレームワークであるSpring Framework における**脆弱性を公表**
    - 脆弱性**公表時点で既にPOC（実証コード）が公開**されていた
    - **公表当日から悪用を試行する通信が観測**され、4日間で最大37,000件にも上り全世界の約16％の組織が影響を受けた

【出典】
※1　深刻な脆弱性「Spring4Shell」（NTT DATA）
https://www.nttdata.com/jp/ja/data-insight/2022/1012/
※2　Spring4Shell（CVE-2022-22965）を悪用したボットネット「Mirai」の攻撃を観測（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/22/d/Mirai-exploits-Spring4Shell.html

Copyright © 2023　独立行政法人情報処理推進機構

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

● 対策

■ 個人、組織（システム管理者/ソフトウェア利用者）

・被害の予防

- 資産の**把握**、体制の**整備**
- 脆弱性関連**情報の収集と対応**
- ネットワークの**監視**および攻撃通信の**遮断**
- セキュリティの**サポートが充実**しているソフトウェアやバージョンを使う
- **一時的なサーバー停止**等

・攻撃の予兆／被害の早期検知

- UTM・IDS/IPS・WAF等の**導入**

・被害を受けた後の対応

- 組織の方針に従い各所へ**報告、相談**する
  上司、CSIRT、関係組織、公的機関等
- 影響調査および原因の追究、対策の強化

Copyright © 2023 独立行政法人情報処理推進機構

【8位】脆弱性対策情報の公開に伴う悪用増加

～「後で対応しよう」、その数日が命取り～

- **対策**
  - **組織（開発ベンダー）**
    - ・製品セキュリティの管理、対応体制の整備
      - –製品に組み込まれているソフトウェアの**把握**、管理の徹底
      - –脆弱性関連**情報の収集**
      - –脆弱性発見時の**対応手順の作成**
      - –情報を迅速に発信できる仕組みの整備

Copyright © 2023 独立行政法人情報処理推進機構