Ransomware Attack on KADOKAWA an Anomaly?

KADOKAWAを襲ったサイバー攻撃は私たちの多くに大きな衝撃を与えることだったかと思います。ひとつの会社の機能が停止してしまうほどの大きなカをもつランサムウェア攻撃。決して他人事ではないですが、日本の被害は意外にも低いようです。

1. Article

Read the following article aloud.

本ページは出典ニュース記事を要約した英文です。

Ransomware attacks, where critical digital data is held hostage for ransom, have been **impacting** companies globally. A recent attack on the KADOKAWA Group in Japan on June 8 has had significant **repercussions**, **suspending** many operations and leaving the company estimating a recovery time of over a month. However, research indicates a significant decrease in ransomware infection rates in Japan, remarkably low compared to 15 other major countries. This decline is attributed to the low rate of ransom payments in Japan, leading cybercriminals to perceive that targeting Japanese companies is not profitable.

Ransomware can spread through networks, causing widespread damage. Even with precautions at a company's headquarters, an infection at a group company or within the supply chain can **impact** the entire organization. In 2022, an infection at a key supplier led Toyota Motors to **shut down** all its domestic factories for a day, taking about a month to restore the system. Due to the severity of these attacks, ransomware was ranked as the top threat to organizations in 2023 by the Information-Technology Promotion Agency of Japan.

Japanese companies have been consistently refusing to pay ransoms, leading to a sharp decline in the country's ransomware infection rate. In 2023, Japan's ransom payment rate was the third lowest at 32%, compared to an average of 54%. This refusal to fund criminal organizations, along with widespread data backup practices and exclusion of ransom payments from cyberattack insurance policies, has discouraged attackers from targeting Japan. The focus on security is shifting from preventing **intrusion** to swiftly detecting it once it happens, with companies deploying sensors to detect suspicious virus activity within their networks.

Source：Ransomware Attack on KADOKAWA an Anomaly?
JAPAN Forward

2. Key phrases and vocabulary

First repeat after your tutor and then read aloud by yourself.

1. impact 影響を与える

The new government policy will **impact** the lives of many people.

2. suspend 一時停止する

The construction work was **suspended** due to safety concerns.

3. shut down 閉鎖する

The restaurant had to **shut down** due to health code violations.

4. repercussions 影響、結果

The environmental **repercussions** of the oil spill are still unknown.

5. intrusion 侵入

The company is investing in advanced technology to prevent any **intrusion**.

3. Questions

Read the questions aloud and answer them.

1. **What is a ransomware attack and how has it been affecting companies globally?**
2. **How did the ransomware attack affect the KADOKAWA Group in Japan?**
3. **What is the trend of ransomware infection rates in Japan compared to 15 other major countries?**
4. **What are your thoughts on the strategy of companies refusing to pay ransoms? Do you think it's effective?**
5. **In your opinion, what other measures can be taken to further decrease the rate of ransomware infections?**

4. 日本語関連記事：ＫＡＤＯＫＡＷＡ襲った身代金要求ウイルス、日本企業の感染被害率は突出して低く

本ページは出典記事原文の日本語訳です。本教材の要約英文の日本語訳ではありません。

パソコン内のデータを開けなくしたり、盗んだりして、復元や暴露回避のための金銭を要求する「ランサムウェア（身代金要求型ウイルス）」の被害企業が後を絶たず、６月８日のＫＡＤＯＫＡＷＡグループへのサイバー攻撃では今も大きな影響が出ている。一方、民間調査で日本は同ウイルスの感染率が急減しており、主要１５カ国の中で突出して低いことが判明。理由に身代金を支払う割合が低いことが挙げられ、「日本を狙っても割に合わない」との評価が広がり、攻撃回数自体が減った可能性もある。

「ただ今、システム障害のため、お問い合わせをお受けすることができません」

ＫＡＤＯＫＡＷＡ本社に電話をすると、１９日時点で自動音声が流れる。

８日に同社グループ内のサーバーがランサムウェアを含む大規模なサイバー攻撃を受け、グループの広範な事業が停止に追い込まれた。同社は完全復旧まで１カ月以上かかると見通す。

ランサムウェアはネットワークを通じて被害が広がる。本社などが対策をとっていても、グループ会社やサプライチェーン（供給網）のどこかで感染すれば全体に影響が及ぶ恐れがある。

令和４年にトヨタ自動車の主要取引先である部品メーカーのシステムが感染した際は、トヨタも国内の工場が全て１日停止に追い込まれ、システムの復旧には約１カ月を要した。

悪質性の高さから、情報処理推進機構（東京）が公表した昨年１年間の情報セキュリティーにおける組織向けの１０大脅威で、ランサムウェアは１位になった。

対策面では改善も見られる。情報セキュリティー会社の日本プルーフポイントは、主要１５カ国のセキュリティー担当者らを対象に調査を実施。昨年にランサムウェアに感染したことがある組織の割合は、１５カ国平均が前年比５ポイント増の６９％に対し、日本は同３０ポイント減の３８％と突出して低かった。

急減の理由は何か。同社の増田幸美チーフエバンジェリストは「日本の企業が継続して身代金を支払わないようにしてきたことが功を奏した」と推測。令和２～４年の調査は３年連続で日本は被害企業の身代金支払い率が最も低く、５年は３番目の低さながら平均５４％の中で３２％を維持した。

また、日本企業が身代金を支払わない理由には、①災害が多いためデータのバックアップが普及していて修復が可能②反社会的勢力への利益供与を避ける考えが浸透③サイバー攻撃被害に関する保険の補償範囲に身代金の支払いが含まれていないーことを挙げた。

こうした背景も含め、攻撃者らに金銭目的の攻撃を思いとどまらせる効果があったと分析している。

企業側の防衛意識も高まってきている。情報セキュリティー会社のトレンドマイクロによると、ウイルスの侵入経路は、以前はメール経由が多かった。だが、新型コロナウイルス禍を経てテレワークが増えたことを受け、外部から社内の業務システムに接続する際に使うＶＰＮ（仮想プライベートネットワーク）機器の脆弱性を突いて侵入するパターンが増えた。

対抗して企業側もネットワーク内などにウイルスによる怪しい挙動がないかを察知するセンサーの設置が進んでいる。対策の主流は侵入を防ぐよりも、侵入後いかに早く察知するかに移行しているという。

ただ、相手の要求に応じないことが最大の抑止力になることに変わりはなく、日本プルーフポイントの増田氏は「身代金を払っても攻撃者は盗んだデータを消去してくれない。今後は支払いに応じない国が増えていくだろう」としている。

出典：ＫＡＤＯＫＡＷＡ襲った身代金要求ウイルス、日本企業の感染被害率は突出して低く
JAPAN Forward