

ゲームプラットフォームのチャットを用いた フィッシング手法の分析と考察

郷田 大造[†] 島 成佳[†]

長崎県立大学情報システム学部情報セキュリティ学科[†]

1 はじめに

現在インターネット社会におけるコミュニケーションツール(以降, ツールと呼称)には, 主にメールやチャット等のツールが用いられる. これらのツールは個人間の情報交換や共有に有効であり, 特にチャットは近年プライベートだけでなく, ビジネスでも利用が進んでおり, チャットを標的とした攻撃が見られるようになってきている. 本論文では, 筆者らがこのような新しい攻撃の被害に遭ったことから, 被害の内容を分析し考察する.

2 フィッシング被害の状況

フィッシング対策協議会のフィッシングレポート 2022[1]によれば, テイクダウン・検知等のフィッシング対策を行っているにも関わらず国内のフィッシングの報告件数は 2017 年から 2021 年まで増加傾向にあり, フィッシングに用いられるものはメールの他にも SMS やチャットを用いたものなど, 多様化している. 被害報告はメールを用いたものがほとんどであり, チャットを用いたものは見当たらない. このため, 本論文では, 被害に遭った経緯からチャットフィッシングに注目し被害内容に基づく分析結果・考察を述べる.

3 筆者らが遭った被害内容の流れ

筆者らは Steam¹ (Valve 社が提供するゲームプラットフォーム)上のチャットを利用している際に被害に遭った. 以下に, フィッシング被害に至った流れを図 1 に示し説明する.

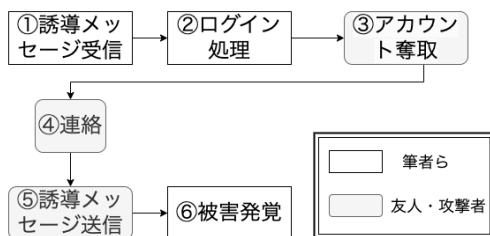


図 1: 被害内容の流れ

・誘導メッセージ受信

筆者らが, Steam 内チャット(以下チャットと呼称)でフィッシングサイト(以下サイトと呼称)に

Analysis and Consideration of Phishing Methods Using Chat of Online Game Platform.

[†] University of Nagasaki.

1

<https://store.steampowered.com/?l=japanese>

誘導するメッセージを受信した.

・ログイン処理

筆者らがサイト上で Steam アカウントのログイン処理を行った.

・アカウント奪取

筆者らがサイト上でログイン処理をしたほぼ同時に, 攻撃者がログイン処理を行っていた.

・連絡, 被害発覚

筆者らは友人からの連絡で被害に遭ったことに気づいた. アカウント奪取から連絡, 被害発覚まで約 3 時間を有した.

・被害発覚後の対応

筆者らは被害発覚後すぐに, Steam アカウントのパスワードを変更した. また, Steam 運営に攻撃者と思われるアカウントの報告を行った.

4 被害内容の分析

これまで筆者らは, メールフィッシングの攻撃に遭ったことはあるが, 被害に至ったことはない.

筆者らは, メールフィッシングの場合は身近な人の被害体験や被害報告, 様々な媒体で図 1①や, ②に該当するようなことに対する注意喚起を見たことがあった. そのため攻撃のプロセス等, メールフィッシングに対する知識を獲得できていた. このことからメールフィッシングに対する意識が自然と形成できていた. しかし, チャットの場合は被害体験や被害報告, 様々な媒体で, 図 1①や②に該当するようなことに対する注意喚起を見たことがなく, 攻撃のプロセス等チャットフィッシングに対する知識を獲得できていなかった. そのため, チャットフィッシングに対する意識が形成できていなかった. このようなメール・チャットの間にある知識獲得・意識形成の差で筆者らは被害に至ったと考える.

5 考察

5.1 現状に基づく被害原因の考察

前節で述べた知識獲得に関しては, 身近な人の被害体験や報告の他に公的機関等からの注意喚起文書の有無が知識獲得の差に影響している. メールフィッシングの場合には, 公的機関等からの注意喚起文書が存在している. また被害報告も集

計的にまとめられ公開されており情報が得やすい。一方チャットフィッシングの場合、メールと異なりチャット運営からの文書すら存在していないこともある。また被害報告も集計的にまとめられているものも見当たらず、個々の運営での被害報告に留まっている。このため、メールとチャットを比較すると知識獲得、意識形成の有無が異なっている。これを表1で整理した。表1の表頭はメール、チャットとし、表則は知識獲得、意識形成とした。知識獲得、意識形成がなされているものに「有」なされていないものに「無」を設定した。

表1：知識獲得、意識形成の比較表

	メール	チャット
知識獲得	有	無
意識形成	有	無

一般にメールは運営元が異なっても、メールを一意に存在するアドレス宛てに送信する所は同じである。運営元が違えどメールは同じシステムを採用していると言える。このことから注意喚起がしやすいと考える。対してチャットの場合アドレスが存在しておらず、チャットごとに送信形式が異なっておりシステムが同一ではない。そのためチャットごとのバラバラな注意喚起に留まり、公的機関等からの注意喚起文書、集計的な被害報告がないと考える。このことよりメールと比べチャットの知識獲得が難しく意識形成も困難になっている。このことがメールと比べフィッシング被害を受けやすい原因の一つであると考えられる。

5.2 友人からの連絡がなかった場合の被害

図1④で友人からの連絡に気づけなかった場合、Steamアカウントを完全に奪取されていた可能性がある。Steamにはアカウントが奪取されログインできなくなった場合運営に連絡し本人確認を行うことでアカウントを取り返せる可能性がある。しかしアカウント盗難に関するサポートページが存在しているのみであり、このことはあまり知られていない。クレジットカードの場合フィッシング被害報告の数も多い。そのためクレジットカード情報詐取に遭った後の連絡窓口に関する情報周知や、ガイドラインの文書も多数存在していることから被害後の対応が明らかである。

Steamの場合被害に遭った後の連絡窓口に関する情報周知やガイドラインの文書¹が不十分であるのに加え、明らかになっておらず被害発覚の遅れや被害拡大を助長する可能性がある。

1

<https://help.steampowered.com/ja/wizard/HelpWithAccountStolen>

5.3 Steamでのマネタイズについて

フィッシングの目的は金銭であり、奪取することで直接金銭に結びつきやすいクレジットカード情報が攻撃の主要な対象である[1]。しかし、フィッシングは直接・間接的に金銭に結びつけば媒体を問わず行われている。Steamでのチャットフィッシングは直接的に金銭に結びつきにくいと思われるアカウントを狙ったもの、アイテムを狙ったものである。これはSteamが展開しているサービスを利用することでアカウント、アイテムを金銭に変えられる環境があることが影響している。Steamには一定の条件を達成することで、得られるSteam内アイテムを金銭で売買できる仕組みがある。これを利用する前提で、アカウントを奪取し、奪取したアカウントでアイテムを売買することで間接的に金銭が得られる。また、Steamではゲーム等のソフトを購入でき、多数のソフトを保有しているアカウントは資産価値が高くなる。このようなアカウントもまた売買できる。さらに保有しているソフトに加えSteam内アイテムが加わるとより高額で乗っ取ったアカウントが売れる。ただしSteamではアカウントの売買は認められていないが、実際にインターネット上で確認してみたところSteamアカウントを売買するサイトを確認できた。今回筆者らが被害に遭ったのも、マネタイズ²ができる環境が整っていることが背景にある。そのためその他のチャットサービスにおいてもマネタイズができる環境さえ整えば、新たな攻撃の対象となりうると考えられる。

6 おわりに

チャットが知識の獲得、意識の形成に失敗しているのはメールと比べ、獲得・形成の際に必要な注意喚起等の情報の量で見劣りしてしまうからである。これはチャットが抱える問題であり、被害拡大の原因であり続ける可能性がある。またチャットに紐付いているサービスによっては、攻撃によって金銭に結びつく可能性がある。現在のそのようなチャット運営ごとの情報発信だけでなく、ゲーム、金融等異なる業界ごとで垣根を越えた、情報発信が早急に必要であると考えられる。

7 参考文献

[1]フィッシング対策協議会, フィッシングレポート2022, 入手先<https://www.antiphishing.jp/report/phishing_report_2022.pdf>(参照2023-1-6).

2

<https://dictionary.goo.ne.jp/word/%E3%83%9E%E3%83%8D%E3%82%BF%E3%82%A4%E3%82%BA/>