

A cunning predator: How Silver Fox preys on Japanese firms this tax season



welivesecurity.com/en/business-security/cunning-predator-how-silver-fox-preys-japanese-firms-tax-season



【従業員持株会規約の...
3 MB

【従業員持株会規約の一部改正について】

各位様

平素より当社の業務運営にご尽力いただき、誠にありがとうございます。

従業員の長期的な資産形成を支援し、持株会の運営をより充実させるため、当社において従業員持株会規約の一部を改正することを正式に決定いたしました。

今回の改正に関する詳細な内容は、別添ファイルにてご確認ください。

(※スマートフォンでの表示が不安定な場合がございますので、パソコンにての閲覧をお願いいたします)

【改定の主な内容】

- ・加入資格の拡大：入社後 3 年以上勤務者 → 入社後 1 年以上勤務者
- ・月額拠出金の上限増額：5,000 円 → 10,000 円に引き上げ
- ・配当金再投資制度の新設：配当金を自動的に株式購入に充てるオプションを追加

【改正規約の施行日】

令和 8 年 4 月 1 日

【改正内容説明会の開催について】

日時：令和 8 年 3 月 20 日（木）15:00～16:00

場所：本社 会議室

※参加を希望される方は、令和 8 年 3 月 15 日必着にて人事部宛にメールにて申し込みをお願いいたします。

【お問い合わせ】

メール：hr_system@company.co.jp

敬具

令和 8 年3 月11日

Japan has entered its annual tax filing and organizational change season, a period when companies generate a high volume of legitimate financial and HR-related communications. A threat actor known as Silver Fox is actively exploiting this busy period by conducting a targeted spearphishing campaign against Japanese manufacturers and other businesses.

The ongoing campaign uses convincing phishing lures related to tax compliance violations, salary adjustments, job position changes, and employee stock ownership plans. All emails share the same goal – trick the recipients into opening malicious links or attachments. As employees actually expect to receive emails about these subjects this time of year, they're more likely to trust and act on such messages without a second thought. Needless to say, this significantly increases the risk of compromise.

The operation is also a reminder for organizations to increase vigilance, reinforce awareness around phishing attempts, and ensure that employees verify the authenticity of tax- and HR-themed requests – including those that look routine. Immediate reporting of suspicious emails to security teams is essential to reduce exposure and prevent successful compromise.

What is the threat?

[Active since at least 2023](#), Silver Fox initially focused on [Chinese-speaking targets](#) before expanding into Southeast Asia, [Japan](#), and potentially [North America](#), running each campaign in a local language. This broadened scope shows in the range of verticals the group has hit over the years – [finance](#), [healthcare](#), [education](#), [gaming](#), [government](#) and even [cybersecurity](#). The group also primarily operates in Southeast Asia and has a [well-documented history](#) of [finance-themed](#) spearphishing campaigns during seasonal business cycles.

In the ongoing campaign, the group is taking advantage of Japan's annual cycle of tax filing, financial reporting, salary adjustments, and personnel changes. This pattern isn't new – similar activity was observed during the same period last year, indicating that Silver Fox deliberately aligns its operations with this season. The volume and urgency of legitimate internal communication around these topics is high this time of year, which is exactly what Silver Fox is counting on and what makes its campaigns effective.

In this operation, Silver Fox sends tailored spearphishing emails crafted to look like legitimate HR or tax-related messages. To make the emails appear authentic, the attackers often include the name of the targeted company directly in the subject line. Examples of subjects observed in this campaign include:

- 「会社名」【従業員持株会規約改正に関するお知らせ】
(Translation: <Company Name> Notice of amendments to the ESOP terms and conditions)
- 「会社名」【従業員持株会規約の一部改正について】
(Translation: <Company Name> [Revisions to the ESOP Terms and Conditions])
- 「会社名」【人事異動・給与改定について】
(Translation: <Company Name> [Personnel Changes and Salary Adjustments])
- 税務コンプライアンスおよび罰金通知
(Translation: Tax Compliance and Penalty Notice)

The sender fields impersonate real employees and even CEOs at the targeted companies. Silver Fox is clearly doing some reconnaissance on each target before sending what aren't generic blasts. The attackers are picking names that the targets are likely to recognize and trust, which makes it more difficult for the recipients to distinguish the malicious messages from real internal notifications.

The emails typically contain either a malicious attachment or a link leading to a malicious file. The files are named to resemble common HR, financial, or tax-related documents, such as:

- 【給与調整のお知らせ】
(Translation: Salary Adjustment Notice)
- 人事異動・給与改定について
(Translation: Personnel Changes and Salary Adjustments)

- 人事異動及び給与改定に関するお知らせ
(Translation: Notice regarding personnel changes and salary adjustments)
- 【従業員持株会規約の一部改正について】
(Translation: [Partial amendment to the Employee Stock Ownership Plan terms and conditions])

The following are examples of observed emails and lures:

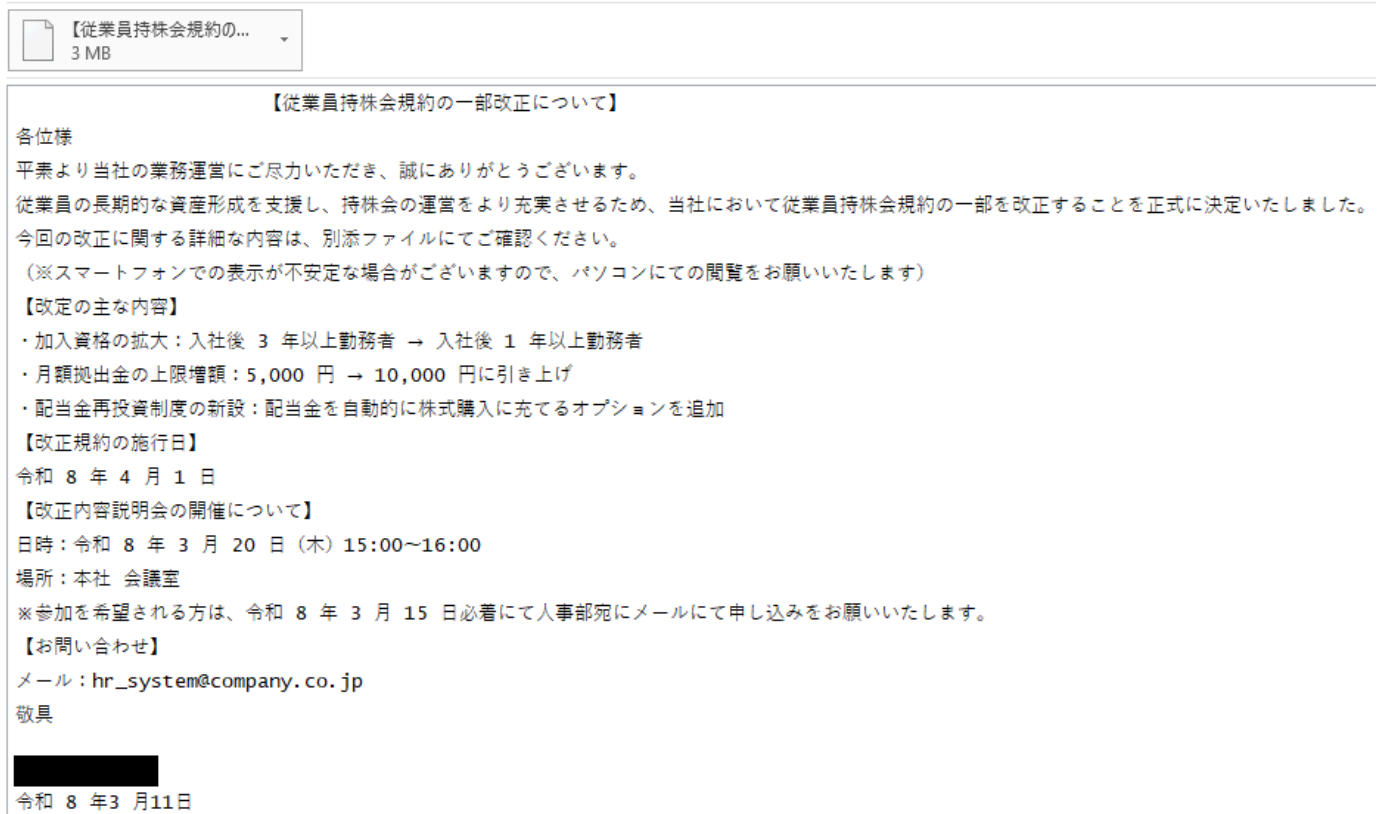


Figure 1. Spearphishing email distributed on 2026-03-11



cftbbi <Marmara2004Norma8489@hotmail.com>

株式会社【人事異動・給与改定について】

【給与調整のお知らせ】

平素より貴重なご貢献とご努力を賜り、誠に感謝いたします。

当社人事部における総合的な評価及び経営陣の協議を経て、氏のこれまでの優れた業務実績と組織への貢献を肯定するため、給与を調整することを決定いたしました。

本次の給与調整に関する核心的な情報は、別添ファイルに詳細を記載しております。

敬請ファイルを確認の上、ご理解を賜りますようお願い申し上げます。

ただいま、人事異動と給与改定のお知らせをメールでお送りしました。

【給与調整の主要ポイント】

調整適用開始日：2026 年 3 月分給与より

詳しい内容：<https://gofile.io/d/ezKv7D>

(パソコンでのご確認をお願いいたします)

今後も氏の一層の活躍を期待しております。

これからも当社の発展に引き続きご協力を賜りますよう、どうぞよろしくお願い申し上げます。

敬具

株式会社

令和 8 年 3 月 12 日

Figure 2. Spearphishing email distributed on 2026-03-12

国税庁 (NATIONAL TAX AGENCY)

調査取締部

令和8年1月15日 (2026年1月15日)

税務コンプライアンス違反及び罰金に関する通知

件名: 税務申告不適合及び罰則に関する通知

- 本通知は、財務省所管の機関である国税庁 (National Tax Agency, NTA) 調査取締部より正式に発行された公的文書であり、「租税特別措置法」及び「国税通則法」の関連規定に基づき制定され、完全な法的効力を有します。
- 御社に対する税務調査が完了いたしました。調査結果により、御社が「法人税法」第11条第1項の規定に違反する申告不適合があることが確認されました。本結論は国税庁の標準的なコンプライアンス調査プロトコルに基づき検証済みです。

税務コンプライアンス不適合の常見事例

- 所得の少申告又は誤分類: 課税所得を全て申告していない (例: サービス料、手数料収入、海外源泉所得の漏れ)
- 費用の不正控除: 控除不能な費用 (例: 株主の個人費用、罰金、不正支出) を控除申告する
- 消費税コンプライアンス違反: 規定の期限内に消費税申告書を提出していない又は消費税を納付していない
- 帳簿書類の保存不備: 正確かつ完全な会計帳簿を少なくとも7年間保存していない
- 源泉徴収税コンプライアンス違反: 従業員の給与から所得税を源泉徴収していない
- 移転価格違反: 関連企業との取引において独立企業間価格ではない価格を使用

提出必要文書一覧

本通知を受信した日から72時間 (3営業日) 以内に提出してください

1. 御社の直近の納税年度における完全な財務諸表
2. 調査対象となる取引に係る原本証明書類、契約書及び保存している領収書の写し
3. 税務申告に関する補足説明文書（御社の公印を押印）

 公式ウェブサイトで手続き

照会番号: NTA/COMP/PEN/2025-078

3. 御社が規定の期限内に完全、正確かつ要求に合致した文書を提出しない場合、国税庁は「法人税法」第150条及び「国税通則法」第65条に基づき正式な法的手続きを発動します。

小松 一郎
国税庁 長官
(こまつ いちろう)

国税庁 (National Tax Agency)

本庁:

〒100-8978 東京都千代田区霞が関3-1-1

電話: 03-3581-4161

公式ウェブサイト: <https://www.nta.go.jp>

無料サービスホットライン:

0120-210-364 (平日 9:00-17:00)

問い合わせ: </about/organization/access/index.htm>

同報: 国税庁 情報システム部長; 国税庁 監査管理部

© 2025 国税庁 (National Tax Agency). All rights reserved.

Figure 3. Tax-related lure webpage instructing the target to download a malicious file

Opening the malicious files drops ValleyRAT, a remote access trojan that Silver Fox has used across multiple campaigns. ESET products detect this malware as Win64/Valley. Once deployed, ValleyRAT enables the actor to take remote control of the compromised machine, harvest

sensitive information, monitor user activity, and maintain persistence in the targeted environment. This can allow the attacker to burrow deeper into the network, steal confidential data, or prepare additional stages of an attack.

How to recognize the threat and protect yourself

While Silver Fox's emails may appear credible at the first glance, especially during Japan's busy tax and organizational change season, a closer look reveals hints rendering the emails suspicious. The following signs are the key to recognizing and stopping the attack:

- If you receive an email about salary changes, tax penalties, or personnel updates, verify it through a separate channel (Teams, phone, or direct email lookup) before acting on it. This applies even if the message looks routine.
- Even if the sender's name belongs (or seems to belong) to a colleague, make sure that the email address and the name match. If they don't or the address looks unfamiliar, treat the email as suspicious.
- Ask yourself whether this communication follows your company's usual HR or Finance process.
- Be cautious if the language feels overly formal, stiff, or mismatched with typical internal communications. Since the threat actor is not a native Japanese speaker, the emails may contain awkward phrasing and subtle giveaways.
- Documents are unlikely to be shared through a publicly available file hosting services such as gofile[.]io or WeTransfer.
- Pay attention to the attachment type. If it's an archive such as RAR or ZIP, look at what's actually inside before opening the files.
- Install software updates when prompted.
- Ensure your security software is running and up-to-date.
- If something feels off about an email, forward it as an attachment to your IT or security team. Reporting is never a mistake – even if the email turns out to be legitimate.

The following are illustrative examples of what to watch out for:

Suspicious sender's name

Suspicious sender's address



ctfbbi <Marmara2004Norma8489@hotmail.com>

株式会社【人事異動・給与改定について】

【給与調整のお知らせ】

平素より貴重なご貢献とご努力を賜り、誠に感謝いたします。

当社人事部における総合的な評価及び経営陣の協議を経て、氏のこれまでの優れた業務実績と組織への貢献を肯定するため、給与を調整することを決定いたしました。

本次の給与調整に関する核心的な情報は、別添ファイルに詳細を記載しております。

敬請ファイルを確認の上、ご理解を賜りますようお願い申し上げます。

ただいま、人事異動と給与改定のお知らせをメールでお送りしました。

【給与調整の主要ポイント】

調整適用開始日：2026 年 3 月分給与より

詳しい内容：<https://gofile.io/d/ezKv7D>

(パソコンでのご確認をお願いいたします)

Link to a publicly available
file hosting service

今後も氏の一層の活躍を期待しております。

これからも当社の発展に引き続きご協力を賜りますよう、どうぞよろしくお願い申し上げます。

敬具

株式会社

令和 8 年 3 月 12 日

Figure 4. Signs revealing that the email is not legitimate



【従業員持株会規約の...
3 MB

Suspicious RAR archive

【従業員持株会規約の一部改正について】

各位様

平素より当社の業務運営にご尽力いただき、誠にありがとうございます。

従業員の長期的な資産形成を支援し、持株会の運営をより充実させるため、当社において従業員持株会規約の一部を改正することを正式に決定いたしました。

今回の改正に関する詳細な内容は、別添ファイルにてご確認ください。

(※スマートフォンでの表示が不安定な場合がございますので、パソコンにての閲覧をお願いいたします)

【改定の主な内容】

- ・加入資格の拡大：入社後 3 年以上勤務者 → 入社後 1 年以上勤務者
- ・月額拠出金の上限増額：5,000 円 → 10,000 円に引き上げ
- ・配当金再投資制度の新設：配当金を自動的に株式購入に充てるオプションを追加

【改正規約の施行日】

令和 8 年 4 月 1 日

【改正内容説明会の開催について】

日時：令和 8 年 3 月 20 日 (木) ~~15:00 - 16:00~~ Mistake, should be 金 as it's Friday

場所：本社 会議室

※参加を希望される方は、令和 8 年 3 月 15 日必着にて人事部宛にメールにて申し込みをお願いいたします。

【お問い合わせ】

メール：hr_system@company.co.jp

Likely mistake, should be targeted
company's email address

敬具

令和 8 年 3 月 11 日

Figure 5. Signs revealing that this email is not legitimate, either

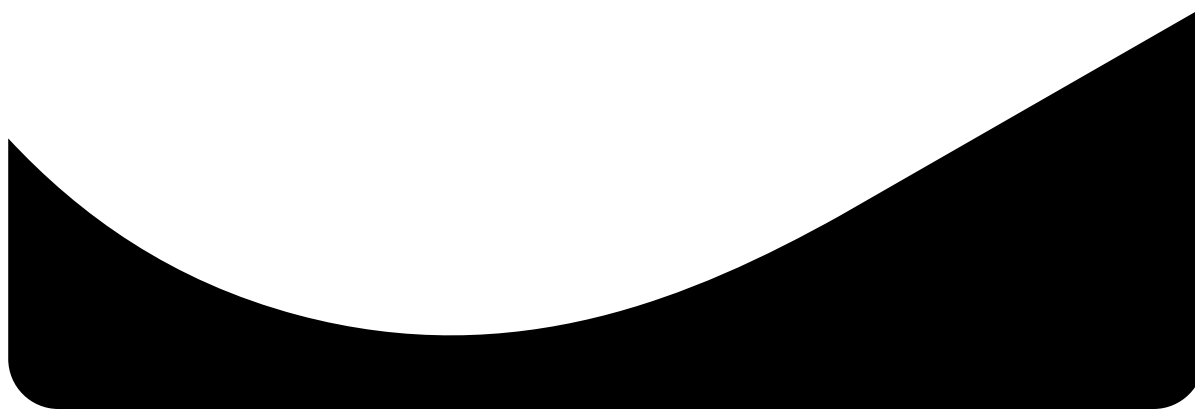
IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in [our GitHub repository](#).

Let us keep you up to date

Sign up for our newsletters

Ukraine Crisis newsletter Regular weekly newsletter



Related Articles

[Business Security](#)

[Virtual machines, virtually everywhere – and with real security gaps](#)

[Business Security](#)

[Cloud workload security: Mind the gaps](#)

[Business Security](#)

[Cyber fallout from the Iran war: What to have on your radar](#)