Clipping Scripted Sparrow's wings: Tracking a global phishing ring - Help Net Security

By Help Net Security

Published: 2025-12-18 · Archived: 2026-04-05 15:14:42 UTC

Between June 2024 and December 2025, Fortra analysts tracked a persistent business email compromise (BEC) operation that we have now classified as Scripted Sparrow. The group carries out well-crafted highly targeted phishing campaigns that masquerade as professional services firms to mislead finance teams into transferring money to fraudsters' accounts.

However, unlike conventional BEC actors, Scripted Sparrow uses a structured, consistent, and disciplined approach. Each campaign shows how they have conducted research, used consistent language with a familiar tone, and chosen payment amounts that hover just below approval limits.

This article outlines the tactics, infrastructure, and behavioral markers associated with this group.

Campaign overview

Scripted Sparrow first appeared on the radar in June 2024. A smattering of fake invoices appeared in the inboxes of companies across North America and Europe, with recipients reporting that the messages looked convincingly real, complete with fabricated executive approvals for overdue consulting or coaching fees.

To add to its credibility, the actors included a chain of prior correspondence, a forged email trail to make it appear that a company executive had authorized the payment and had instructed the collections agent at the coaching company to contact a specific accounts payable staff member at the victim company.

By early 2025, our telemetry confirmed repeat sightings across a range of industries. We have since catalogued 512 unique variants.

Scripted Sparrow's campaigns typically involve relatively modest volumes. We estimate that the group sends between 10,000 and 50,000 emails a day, distributed in small, targeted batches. While this volume may seem small compared to commodity email threats, it's actually massive when compared to other targeted attacks.

Operational Playbook

Rather than a group of opportunists, Scripted Sparrow works as a structured organization, with defined roles across research, domain creation, email development, and financial coordination.

Each campaign follows a recognizable workflow:

Reconnaissance and domain setup: The group registers lookalike domains resembling known firms (such as teneo-strategyy.com, vistageglobal.co). These domains are usually registered in clusters within a 24-hour window

and use privacy-protected WHOIS data.

Email crafting: The group's messages reference fictitious companies (such as Catalyst Executive Circle or Vistage Global Consulting) and mimic internal approvals between executives. The forged email threads show consistent sentence patterns and polite, non-urgent phrasing to maintain plausibility.

Delivery and payment request: The attached invoice PDF or W-9 form lists totals just under standard manual approval limits (under USD $50,000). The recipients are instructed to wire funds to an account controlled by the criminals.

Cash-out: The group utilizes a large collection of US-based mule accounts for the initial transfer. As of this writing, We have identified 249 unique bank accounts used by Scripted Sparrow. While the group seems to prefer a handful of banks, we've seen them use accounts at 42 different financial institutions.

Although the group's technical sophistication is low, its campaigns exhibit internal consistency in formatting, file structure, and language.

Infrastructure and geographic indicators

Our analysis points to a group that's spread across regions. Many of their emails seem to come from U.S. IP addresses, but this is a red herring.

To get closer to their true locations, we engaged with the bad actors. When they requested confirmation of payment, they were directed to controlled file-sharing services that captured browser fingerprints and asked for location permissions. This data, combined with timezone settings and connection patterns, helped our analysts identify likely operators in Nigeria, South Africa, Iran, and Turkey. Our team believes the group has members located in the US, UK, and Canada as well, though with lower confidence due to the various countermeasures the group uses to hide their tracks.

Domain clusters often share hosting providers and registration timelines, pointing to coordinated infrastructure management. Also, banking activity overlaps across campaigns, indicating a common laundering network.

Even so, attribution remains tentative. IP addresses and financial trails can be easily masked, so these findings suggest probable regions rather than definitive actor origins.

Behavioral characteristics

Scripted Sparrow has mastered how companies communicate. Their emails mimic internal tone, formatting, and rhythm. Messages from "executives" have a formal yet conversational feel, with an urgency subtle enough to not raise suspicion.

Certain linguistic quirks appear again and again: polite sign-offs like "Thank you for your quick attention," consistent U.S.-style date formatting even in emails aimed at European firms, and tidy HTML layouts, all crafted without obfuscation or tracking pixels, making the messages feel genuine.

The evolution of activity

Since early 2024, Scripted Sparrow has shown small but noticeable changes in how it operates:

- **Invoice design updates:** Fonts, logos, and branding are tweaked to resemble legitimate firms more closely.
- **Identity reuse:** Fake personas and company names reappear throughout campaigns, hinting at shared templates or internal style guides.
- **Infrastructure recycling:** Domains often resurface months later with minor variations, reflecting a deliberate rotation instead of random reuse.

Importantly, the group rarely attempts privilege escalation or data theft. Their focus remains clear and consistent: use social engineering to push targets into making real financial transfers.

Detection and attribution

From a defense point of view, this campaign's subtlety muddies detection. There is no malware payload, link shortener, or credential-harvesting form, only a PDF attachment and a convincing story.

Our detection systems flagged anomalies in:

- Header routing paths that are inconsistent with declared sender domains.
- Domain registration timestamps that indicate rapid, clustered creation.
- Templates repeated across messages are seen in different industries.

By clustering these signals, Fortra analysts attribute activity to the same operational entity despite the superficial variety of company names.

Observed TTPs

Our findings show a group that relies on psychology, using familiar communication patterns, minimal infrastructure, and consistent routines to stay hidden.

Spearphishing via attachments: Emails arrive with polished PDF invoices that look authentic and contain no malicious code. The goal isn't infection, but to convince finance teams to approve payments.

Reconnaissance: Before each campaign, the group studies its targets, collecting public details about company staff and approval processes to make messages sound authentic.

Masquerading and impersonation: The group mimics executives, consultants, or vendors by using lookalike domains that differ by a single letter or by a different top-level domain.

Template reuse and consistency: Their templates rarely change. The same phrasing and invoice formats reappear across campaigns, offering a reliable pattern for identification.

Domain and account rotation: Each wave of emails uses new domains and bank accounts. When one is detected, it's quickly replaced, keeping activity a step ahead of blocklists.

Payment manipulation: Amounts hover just below review thresholds to slip past internal checks and speed up processing.

These consistent TTPs reinforce the assessment of a cohesive actor group maintaining an ongoing, profitable scheme.

Mitigation and response recommendations

While Scripted Sparrow's methods are simple, their success comes from consistency and timing.

Understanding their playbook is only half the battle, the next step is knowing how to break the pattern. We advise companies to:

- **Implement verification protocols:** Require secondary confirmation for new vendor payments or invoices exceeding a set threshold. Never rely on an email reply chain as evidence of expense approval, as this can be easily spoofed.
- **Monitor domain and header anomalies:** Automated tools should flag mismatched domains, unusual reply-to headers, or recent domain registrations.
- **Educate finance teams:** Awareness training remains effective. Emphasize linguistic red flags and request validation.
- **Leverage behavioral analytics:** Track deviations in communication frequency, time zones, and sender-recipient patterns.

These controls can interrupt the group's primary success condition: unverified trust. The campaign's consistency suggests a central management structure coordinating multiple operators rather than loose affiliates.
