

# Weekly Intelligence Summary

Report Date: 09.06.2025

Intelligence Cut-off Date: 06.06.2025

## Weekly Focus: Spear-phishing campaign targets CFOs and financial executives worldwide

**A worldwide, highly targeted spear phishing campaign aimed at CFOs and finance executives has resulted in NetBird, a legitimate remote-access tool, being installed on the devices of its victims.**

NetBird, an open-source peer-to-peer VPN, uses the WireGuard protocol to establish encrypted, direct connections between devices, enabling secure remote networking across home, office, and cloud environments.

The multi-stage operation begins with a phishing email impersonating a Rothschild & Co recruiter, offering a fake 'strategic opportunity' via a link disguised as a company presentation PDF. The link directs the victim to a Firebase-hosted page hidden behind a custom 'math quiz' CAPTCHA.

Upon solving the CAPTCHA, the victim receives a ZIP file containing a VBS script. Running it downloads a second VBS payload that silently installs NetBird and OpenSSH via Microsoft Installer, creates a hidden local administrator account, and enables Remote Desktop Protocol (RDP) for persistent, encrypted remote access. Scheduled tasks are configured to ensure NetBird restarts at boot, while visual indicators such as desktop shortcuts are removed to avoid detection.

The multi-stage campaign reflects a targeted, stealth-oriented approach to establishing long-term network access.

### Why It Matters...

RDP compromise provides direct access to the victim's system, allowing persistent, stealthy control that often evades traditional security defences.

In addition to the highly sensitive information held by executives that may be leveraged for extortion, the compromise of a CFO's device grants threat actors potential access to valuable financial data, including forecasts, budgets, and mergers and acquisitions (M&A) plans. This information could enable unauthorised fund transfers, insider trading, and credential theft, while also serving as a potential backdoor into broader corporate systems. With NetBird's encrypted tunnels, threat actors can maintain persistent, covert access to an organisation. A breach of this nature also poses significant legal, regulatory, and reputational risks.

Furthermore, compromised data could facilitate subsequent phishing and exploitation of the corporate hierarchy to manipulate junior team members into complying with fund transfer requests or otherwise facilitate fraud, as requests can appear to originate from executive team members.

To mitigate the threats posed by this and similar campaigns, any unsolicited 'opportunity' related emails should be treated with suspicion, content or script execution from downloads should be disabled, and current phishing trends should be integrated into regular simulation exercises and employee training programs.

## Intelligence Overview

### Vulnerabilities

Google released an update to address three security vulnerabilities in its Chrome browser, including the actively exploited out-of-bounds read and write issue in Chrome's V8 JavaScript and WebAssembly, tracked as CVE-2025-5419.

Cisco disclosed two critical vulnerabilities: a Cisco IOS XE WLC arbitrary file upload vulnerability tracked as CVE-2025-20188, and a vulnerability in Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI) cloud deployments of Cisco Identity Services Engine (ISE) tracked as CVE-2025-20286.

### Cybercrime

The Android banking Trojan Crocodilus was observed expanding its targeting to Europe and South America as well as increasing sophistication and data exfiltration capabilities using obfuscation methods and masquerading tactics.

The Volkswagen Group was added to Stormous' leak site, claiming to have exfiltrated a range of sensitive data.

### Data Breach

HMRC lost GBP 47 million after a phishing campaign impersonated the HMRC and used compromised accounts to submit fraudulent tax refund claims.

A threat actor re-released data from a 2021 AT&T breach, affecting 70 million customers, adding previously encrypted dates of birth and Social Security Numbers (SSN), now available in plain text.