VARINDIA

Fake Bonus Emails, Real Espionage: Seqrite Identifies Operation DupeHike Attack Chain

Seqrite, the enterprise security arm of Quick Heal Technologies Limited, a global provider of cybersecurity solutions, has recently uncovered a sophisticated cyber-espionage campaign. Dubbed Operation DupeHike, the campaign targets Russian corporate entities, specifically HR, payroll, and internal administrative departments. Criminals behind this attack, tracked as the UNG0902 group, send zip files named "Bonus 2025" with a shortcut that looks like a normal PDF about yearly bonuses, but clicking it quietly pulls in harmful software to spy on and control victims' machines.

The scam starts with what seems like a regular company email about bonuses, set at 15% of salary based on performance and rules, making it easy to fool office staff who get these updates often. When opened, the shortcut uses a hidden Windows tool called PowerShell to grab the first piece of malware from a bad server. This sneaky program then brings in a second tool that fakes being a font file, checks running apps like Notepad or Edge to hide inside them, and finally sets up AdaptixC2 (a remote-control gadget that lets attackers steal files) to watch activity and run commands from afar.

The APT research team at Seqrite Labs, India’s largest malware analysis facility, detected the campaign on 21 November 2025. The team also found the bad servers linked to Russian hosting firms. The attackers first used open web ports but switched to secure ones to stay hidden, showing they're quick to change tactics as they're being watched. This multi-step trick - fake file, hidden download, code injection, and remote spying - relies on trusted HR lures to slip past basic defences. These attacks hit hard because they prey on everyday work emails, especially in HR and payroll, where money and personal info reside. Researchers at Seqrite Labs warn that no company is safe, calling for simple steps like teaching staff to double-check surprise attachments, use two-factor logins, and limit what regular users can access, turning potential weak spots into strong defences. Deploying tools that flag odd PowerShell activity or unsigned code is also recommended.

In response to this campaign, Seqrite has already deployed complete protection across its products. All components of this threat are now actively blocked, ensuring customers remain secure. Enterprises are urged to instruct their employees to never open unexpected files, even from "HR", and confirm them by phone or official channels first. Seqrite continues to track Operation DupeHike and will disseminate updated indicators of compromise to enterprise customers and law enforcement partners to disrupt attacker infrastructure and strengthen corporate networks.