Cyber Threat Intelligence Report

CTI Report Analysis: Suspected APT29 Phishing Campaign

ATT&CK Tactics:

* **Initial Access:** Phishing (Spearphishing Attachment)
* **Execution:** Command and Scripting Interpreter (PowerShell)
* **Persistence:** Registry Run Keys / Startup Folder, Scheduled Task/Job
* **Command and Control:** Application Layer Protocol (HTTPS), DNS Tunneling
* **Exfiltration:** DNS Tunneling
* **Defense Evasion:** Obfuscated Files or Information (Macro-enabled Documents)

ATT&CK Techniques:

* T1566: Phishing
* T1566.001: Spearphishing Attachment
* T1059: Command and Scripting Interpreter
* T1059.001: PowerShell
* T1547: Boot or Logon Autostart Execution
* T1547.001: Registry Run Keys / Startup Folder
* T1053: Scheduled Task/Job
* T1071: Application Layer Protocol
* T1071.001: Web Protocols
* T1573: DNS Tunneling
* T1027: Obfuscated Files or Information
* T1027.006: Deobfuscate/Decode Files or Information

Indicators of Compromise (IOCs):

* **Email Subjects:** "Urgent Account Verification Required", "Payroll Update March 2025"
* **Attachments:** Invoice_March2025.pdf.exe, payment_receipt_2025.docm
* **PowerShell Script:** update.ps1
* **Payload URL:** hxxpc2server.xyz/secondstage.bin
* **C2 IP:** 185.220.101.3 (HTTPS)
* **Domains:** secureloginbanking.com, clientupdate.xyz, govdocumentsauth.com

Other Relevant Details:

* **Targeting:** Financial organizations and government agencies in APAC. Potentially targeting
* **Start Date:** Early March
* **Suspected Threat Actor:** APT29 (Cozy Bear) – Needs further confirmation
* **Malware:** RAT (Remote Access Trojan)
* **Persistence Mechanism:** Registry keys and scheduled tasks (re-execution every 6 hours)
* **Exfiltration Method:** DNS Tunneling via clientupdate.xyz
* **Similar Previous Campaigns:** Resembles past APT29 operations

Severity Score: High

Attack Description Summary:

The attack begins with a spearphishing campaign targeting financial and government entities in th