**Incident Name:**

**Unauthorized Phishing Attack Leading to C2 and Persistence on Windows 10**

V

Investigation Date: 2/23/2025

Escalation Date: 2/20/2025

MTTR: 15 Hrs

**Contents**

Incident Handling Workflow

**Alert Summary:**

At [Time, Date], an alert was generated after a phishing email was delivered to the target email address (sprintspro123@outlook.com). The email, sent from no-reply noreplyspri@gmail.com with the subject “Your February Payslip is Now Available,” contained a link to download a file. The link directed the user to download a file that appeared to be a legitimate PDF, but was actually a malicious executable. Upon execution, this file established a Meterpreter reverse shell on the Windows 10 workstation. Subsequently, a persistent backdoor was installed using Metasploit’s windows/local/persistence module.

Alert Information

**1. Alert Information**

**Summary:**  
At 19:03:39 20:02:25 we received an alert from **Gophish** stating that a phishing email was delivered to **[User: sprintspro123@outlook.com]**. The email sender was **no-reply noreplyspri@gmail.com**, and the subject

was:  
**"Your February Payslip is Now Available."**

The email contained a **malicious link** directing the user to download a disguised executable file from the following

URL:  
🔹 [**http://100.123.236.70:8080/Payslip.exe**](http://100.123.236.70:8080/Payslip.exe)

Upon further analysis, we determined that the link contained a Windows executable embedded with a **reverse shell payload**, granting the attacker remote access upon execution.

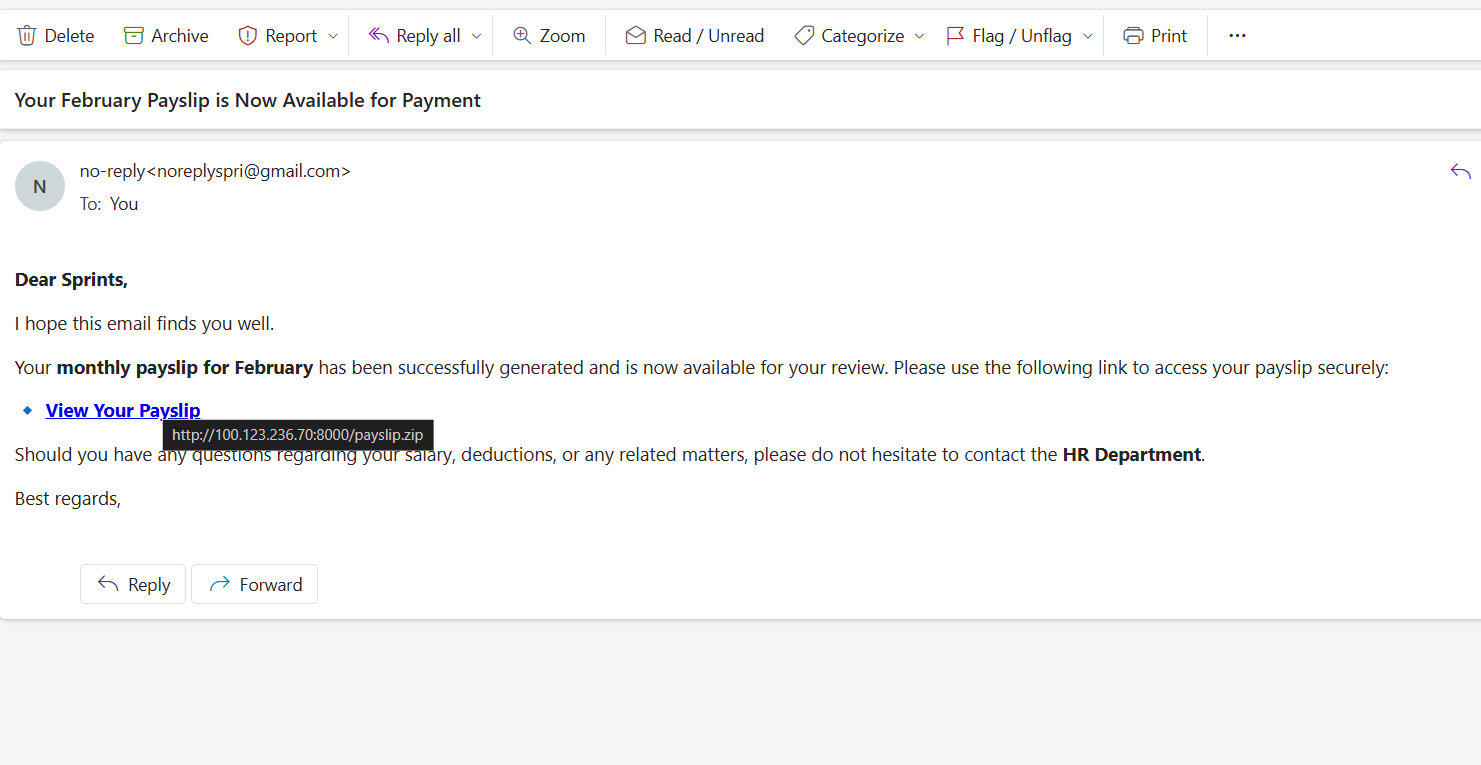
|  |  |  |  |
| --- | --- | --- | --- |
| Alert Summary L1 | | | |
| First Handler | Asma | | |
| Alert Type | New | | |
| Alert Name | Phishing Attack: Reverse Shell and Persistence Detected | | |
| Time Generated | 19:03:39 20:02:25 | | |
| Alert Severity | Critical | | |
| Product | Gophish Phishing Campaign (Email) | | |
| Compromised Entity Type | Windows 10 Workstation | **Entity** | Desktop-sprint 100.113.47.90 |
| Detection Time | 19:03:39 20:02:25 | **Investigation Time** | 07:03:39 21:02:25 |
| Follow up Time | 11:14:22 22:02:25 | **Response Time** | 11:14:22 22:02:25 |
| Analysis:  Dear Team,  At 19:03:39 20:02:25, Splunk detected unusual network activity from [Victim IP], suggesting a possible reverse shell. Upon investigation, we confirmed that a phishing email was delivered to sprintspro123@outlook.com and bypassed email security.   1. Email & Sender Analysis  * The sender’s domain, flagged by MXToolbox, showed a history of malicious activity. * The phishing link was blacklisted on VirusTotal, Cisco Talos, and other OSINT sources. * Threat intelligence databases linked the sender’s email to prior phishing campaigns.  1. URL & Payload Analysis    1. The phishing link led to a disguised .exe file, analyzed in Anyrun, confirming malware behavior.    2. The payload established a reverse Meterpreter session to 100.123.236.70:9001, allowing remote control.    3. The malware set up a C2 connection for persistent access. 2. Network & System Activity  * The infected Windows 10 machine made repeated outbound connections to 100.123.236.70. * A Metasploit persistence module (windows/local/persistence) was deployed, ensuring access after reboot. * Registry modifications allowed automatic execution of the payload on startup. | | | |
| Remediation Steps:   1. Immediate Actions:    1. Isolated the infected machine to prevent further C2 communication.    2. Removed the malware and disabled persistence mechanisms.    3. Blocked 100.123.236.70 and the phishing URL at the firewall and email gateway.    4. Updated security policies to prevent unauthorized .exe execution. 2. Short-Term Fixes: 3. Conducted full forensic analysis on the compromised system. 4. Quarantined affected email accounts and reset credentials. 5. Strengthened email security policies (DMARC, DKIM, SPF). 6. Long-Term Preventive Measures:    1. Security awareness training to help users spot phishing attempts.    2. Strict application whitelisting (e.g., AppLocker) to block unauthorized executables.    3. Enhanced IDS/IPS detection rules to flag unusual outbound connections. | | | |

**Indicators of Compromise (IoCs):**

|  |  |  |
| --- | --- | --- |
| **IoC Type** | **Value** | **Description** |
| **Sender Email** | no-replyspri@gmail.com | Malicious phishing sender |
| **Malicious URL** | http://100.123.236.70:8080/Payslip.exe | Hosted malware payload |
| **Attacker IP** | 100.123.236.70 | Reverse shell C2 server |
| **Victim Machine** | 100.113.47.90 | Infected Windows 10 workstation |

Evidence

Evidence 1: Email



Evidence 2: Splunk

