CIRT.GY Guyana National Computer Incident Response Team

AL2025_31 FIN6 Hackers Pose as Job Seekers to Backdoor Recruiters' Devices (June 11, 2025)

Description

The FIN6 threat group, also known as “Skeleton Spider,” has launched a sophisticated social engineering campaign targeting human resource (HR) professionals and recruiters. Unlike typical employment scams, this operation flips the script: instead of luring job seekers, FIN6 impersonates job applicants to deceive recruiters into visiting phishing websites and downloading malware. This latest operation leverages the More_eggs malware-as-a-service backdoor to gain unauthorized access to systems, steal credentials, and deploy additional payloads, including ransomware.

Attack Details

In the newly identified campaign, FIN6 actors use fake job seeker personas to approach recruiters on professional platforms such as LinkedIn and Indeed. Once contact is established, the threat actors follow up via email, sharing a non-clickable URL to a supposed resume or portfolio site. These links are intentionally not hyperlinked, forcing targets to manually enter them into their browsers, an evasion tactic that helps avoid automated security filters.

The phishing domains, registered anonymously through GoDaddy and hosted on Amazon Web Services (AWS), mimic professional portfolio sites. These domains include advanced evasion techniques:

- Environmental fingerprinting to detect the visitor’s OS and network conditions
- Blocking access from VPNs, Linux/macOS, and cloud platforms
- Displaying benign content for unqualified visitors
- A fake CAPTCHA step for qualified victims, adding perceived legitimacy

Once victims pass the CAPTCHA, they are prompted to download a ZIP archive allegedly containing a resume. In reality, it hides a malicious Windows shortcut (LNK) file that triggers a script to download and install More_eggs, a versatile JavaScript backdoor developed by another actor, “Venom Spider.”

More_eggs capabilities include:

- Remote command execution
- Credential harvesting
- PowerShell-based payload delivery
- Deployment of ransomware or other tools

Indicators of Compromise (IOCs)

Domains associated with this campaign:

- bobbyweisman[.]com
- emersonkelly[.]com
- davidlesnick[.]com
- kimberlykamara[.]com
- annalanyi[.]com
- bobbybradley[.]net
- malenebutler[.]com
- lorinash[.]com
- alanpower[.]net
- edwarddhall[.]com

Malware:

- More_eggs JavaScript backdoor

File type used in phishing package:

- .LNK file disguised as a resume within a ZIP archive

Hosting infrastructure:

- Domains hosted on **AWS**, registered via **GoDaddy**

Tactics:

- Non-clickable URLs
- Environment-aware delivery (bypasses security environments)
- Fake CAPTCHA for added legitimacy

Remediation

Organizations, especially HR departments and recruiters, should implement the following security measures:

- **User Awareness and Training**
  - Educate HR and recruitment staff on modern phishing tactics.
  - Warn against manually typing suspicious URLs into browsers.
- **Email Filtering and Security Gateways**
  - Improve detection rules for suspicious resumes or ZIP attachments.
  - Flag emails containing job application links from unverified domains.
- **Endpoint Protection**
  - Deploy EDR (Endpoint Detection and Response) solutions capable of detecting .LNK file misuse and JavaScript-based backdoors.
- **Identity Verification**
  - Independently verify job applicants' details (e.g., through reference checks or LinkedIn cross-verification) before clicking external links.
- **Network Monitoring**
  - Monitor outbound traffic for connections to known malicious domains and AWS-hosted sites not associated with business operations.
- **Incident Response Readiness**
  - Ensure IR teams are prepared to isolate infected machines and trace potential lateral movement if compromise is suspected.
- **Report Abuse**
  - Report suspicious domains and content to **AWS Trust & Safety** using their abuse reporting channels.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (n.d.). FIN6 Uses AWS-Hosted Fake Resumes on LinkedIn to Deliver More_eggs Malware. Retrieved from https://thehackernews.com/2025/06/fin6-uses-aws-hosted-fake-resumes-on.html
- Toulas, B. (2025, June 11). FIN6 hackers pose as job seekers to backdoor recruiters' devices. Retrieved from BleepingComputer.

https://www.bleepingcomputer.com/news/security/fin6-hackers-pose-as-job-seekers-to-backdoor-recruiters-devices/