More_eggs Malware Targets Recruiters in Phishing Attack

Date: 10th June 2024 | Severity: High

Summary

- Cybersecurity researchers have spotted a phishing attack distributing the More_eggs malware by masquerading it as a resume, a technique originally detected more than two years ago.
- The attack, which was unsuccessful, targeted an unnamed company in the industrial services industry in May 2024, Canadian cybersecurity firm eSentire disclosed last week.

Attack Vectors

- “The targeted individual was a recruiter that was deceived by the threat actor into thinking they were a job applicant and lured them to their website to download the loader,” it said.
- More_eggs, believed to be the work of a threat actor known as the Golden Chickens (aka Venom Spider), is a modular backdoor that’s capable of harvesting sensitive information. It’s offered to other criminal actors under a Malware-as-a-Service (MaaS) model.
- The latest attack chain entails the malicious actors responding to LinkedIn job postings with a link to a fake resume download site that results in the download of a malicious Windows Shortcut file (LNK).
- More_eggs activity has targeted professionals on LinkedIn with weaponized job offers to trick them into downloading the malware.
- “Navigating to the same URL days later results in the individual’s resume in plain HTML, with no indication of a redirect or download,” eSentire noted.
- Microsoft program called ie4uinit.exe, after which the library is executed using regsvr32.exe to establish persistence, gather data about the infected host, and drop additional payloads, including the JavaScript-based More_eggs backdoor.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 37831e465728a913acab317b65c4474b8e6a4570e78c39c8b8c9b956e5d6db25 • 78a87d540c1758c6b4dcabb7b825ea3a186ef61e7439045ece3ce3205c7e85a2
Domain	• api[.]cloudservers[.]kz • mail[.]rediffmail[.]kz • secure[.]cloudserv[.]ink • metric[.]onlinefonts[.]kz • news[.]bradpitt[.]kz • jobhyper[.]com
IP	• 185[.]243[.]115[.]50 • 192[.]99[.]20[.]90 • 192[.]187[.]103[.]42 • 37[.]1[.]221[.]212

Recommendation

- Security Awareness Training: Mandate training for all employees to raise awareness about phishing tactics. Ensure employees recognize suspicious emails and avoid clicking on malicious links.
- Beyond Antivirus: Antivirus alone is insufficient. More_eggs can bypass binary detection approaches. Consider additional security layers, such as endpoint detection and response (EDR) solutions.
- Monitor Threat Landscape: Stay informed with relevant threat intelligence. Act promptly on threat information to prevent attacks.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//thehackernews.com/2024/06/moreeggs-malware-disguised-as-resumes.html
- https[:]//github.com/esThreatIntelligence/iocs/blob/main/more_eggs/more_eggs_iocs_5-29-2024.txt