UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00129

LINKEDIN SPEAR PHISHING TARGETS JOB SEEKERS

DATE ISSUED: 6th April 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

A recent surge in fake job offers for job seekers on the popular social networking site LinkedIn in an effort to tempt victims into downloading the more_eggs fileless backdoor perpetuated by the Golden Chickens group.

BREAKDOWN

Using their current job title and appending “position” as the subject line makes this recent phishing campaign seem legitimate to victims, enticing them to download a zip file, which will install a backdoor onto their device. Once infected, the malware is then able to call and install further malware onto the device for a multitude of purposes. It is also known that the group is offering the software in a Malware as a Service (MaaS) capacity to other cyber criminal groups to allow them to gain a hold on their victims as well. With the current state of the world and its unemployment rates, this campaign targets highly vulnerable groups, desperately seeking work as well as those who are potentially seeking to change roles or gain higher experience. To avoid detection, the malware exploits normal Windows processes and evades antivirus protections.

REMEDIATION STEPS

- Use next generation anti-malware endpoint protection, not just anti-virus.
- Never open .ZIP files from unknown sources
- If in doubt, verify by a secondary means, such as a phone call.

REFERENCES & RESOURCES

eSentire	https://www.esentire.com/security-advisories/hackers-spearphish-professionals-on-linkedin-with-fake-job-offers-infecting-them-with-malware-warns-esentire
Threatpost	https://threatpost.com/linkedin-spear-phishing-job-hunters/165240/
Dark Reading	https://www.darkreading.com/threat-intelligence/linkedin-phishing-ramps-up-with-more-targeted-attacks/d/d-id/1340590