# Hackers Spearphish Professionals on LinkedIn with Fake Job Offers, Infecting them with Malware, Warns eSentire

## Summary

eSentire, a leading cybersecurity solutions provider, is warning enterprises and individuals that a hacking group is spearphishing business professionals on LinkedIn with fake job offers in an effort to infect them with a sophisticated backdoor Trojan. Backdoor trojans give threat actors remote control over the victim's computer, allowing them to send, receive, launch and delete files.

eSentire's research team, the Threat Response Unit (TRU), discovered that hackers are spearphishing victims with a malicious zip file using the job position listed on the target's LinkedIn profile. For example, if the LinkedIn member's job is listed as *Senior Account Executive—International Freight* the malicious zip file would be titled *Senior Account Executive—International Freight position (note the "position" added to the end)*. Upon opening the fake job offer, the victim unwittingly initiates the stealthy installation of the fileless backdoor, more_eggs. Once loaded, the sophisticated backdoor can download additional malicious plugins and provide hands-on access to the victim's computer. The threat group behind more_eggs, Golden Chickens, sell the backdoor under a malware- as- a-service(MaaS) arrangement to other cybercriminals. Once more_eggs is on the victim's computer system, the Golden Eggs seedy customers can go in and infect the system with any type of malware: ransomware, credential stealers, banking malware, or simply use the backdoor as a foothold into the victim's network so as to exfiltrate data.

## What Risk Does More_Eggs Backdoor Pose to Organizations and Business Professionals

"What is particularly worrisome about the more_eggs activity is that it has three elements which make it a formidable threat to businesses and business professionals," said Rob McLeod, Sr. Director of the Threat Response Unit (TRU) for eSentire. They are:

1. It uses normal Windows processes to run so it is not going to typically be picked up by anti-virus and automated security solutions so it is quite stealthy.

2.Including the target's job position from LinkedIn in the weaponized job offer increases the odds that the recipient will detonate the malware.

3.Since the COVID pandemic, unemployment rates have risen dramatically. It is a perfect time to take advantage of job seekers who are desperate to find employment. Thus, a customized job lure is even more enticing during these troubled times.

These three elements make more_eggs, and the cybercriminals which use this backdoor very lethal."

## More_Eggs Attack Steps

In the spearphishing incident, which the TRU team disrupted, the target was a professional working in the healthcare technology industry. Upon downloading and executing the alleged job file, the TRU team saw that the victim unwittingly executed VenomLNK, an initial stage of more_eggs. By abusing Windows Management Instrumentation , VenomLNK enables the malware's plugin loader, TerraLoader, which then hijacks legitimate Windows processes, cmstp and regsvr32. (See Image 1). While TerraLoader is being initiated, a decoy word document is presented to the victim. The document is designed to impersonate a legitimate employment application, (See Image 2) but it serves no functional purpose in the infection. It is merely used to distract the victim from the ongoing background tasks of more_eggs. TerraLoader then installs msxsl in the user's roaming profile and loads the payload, TerraPreter, an ActiveX control (.ocx file) downloaded from Amazon Web Services. At this point, TerraPreter begins beaconing to a Command & Control server (C2) via the rogue copy of msxsl. The beacon signals that the more_eggs backdoor is ready for Golden Chicken's customer to log in and begin carrying out their goal, whether it is to infect the victim with additional malware, such as ransomware, or to get a foothold into the victim's network so as to exfiltrate data. eSentire's security analysts disrupted the operation, and the TRU began investigating.

## What Makes More_Eggs So Stealthy

More_eggs maintains a stealthy profile by abusing legitimate Windows processes and feeds those process instructions via script files. Additionally, campaigns using the MaaS offering appear to be sparse and selective in comparison to typical malspam distribution networks. Because of the stealth and spearphishing capabilities of the more_eggs operation, the Golden Chickens threat group enjoys patronage from notable advanced threat groups, such as FIN6, Cobalt Group and Evilnum.

## Who is the Cybercriminal Gang Behind the Current LinkedIn Spearphishing Activity?

Thus far, the TRU team has not discovered forensics indicating the identity of the hacking group which is trying to spearphish the LinkedIn members. However, as mentioned, this malware-as a service has been used by three notable threat groups: FIN6, Cobalt Group and Evilnum.

## What are the Hackers After?

Since this spearphishing attack was disrupted, the TRU team cannot know with certainty what the end game is for this incident. What we do know is that this current activity mirrors an eerily similar campaign which was reported in February 2019, where U.S. retail, entertainment and pharmaceutical companies, which offer online shopping, were targeted. The threat actors went after employees of these companies with fake job offers, cleverly using the job title listed on their LinkedIn profiles, in their communications to the employees. Similar to the current incident, they also used malicious email attachments and if the target clicked on the attachment, they got hit by more_eggs.

## Connection Between FIN6, Evilnum, Cobalt Group and More_Eggs

**FIN6-** FIN6 is a financial cybercrime group that primarily steals payment card data and sells it on underground marketplaces. The FIN6 group first gained notoriety in 2014 for their attacks against point- of- sale (POS) machines in retail outlets and hospitality companies. Continuing their quest for credit and debit card data, they later moved on to targeting e-Commerce companies and stole their credit card data via online skimming. The FIN6 threat group has also been known to infect some of their victims with ransomware.

Interestingly, researchers reported in Feb. 2019 that FIN6 was specifically targeting numerous e-Commerce companies and using malicious documents to infect their targets with more_eggs as the initial phase of their attack. This could be the same campaign, which was reported in Feb. 2019 and which we previously mentioned--- in which threat actors were observed attacking retail, entertainment and pharmaceutical companies' online payments systems and using malicious documents, laden with more_eggs, to target the companies' employees. Of course, it could be a separate campaign entirely. However, what we do know is that the targets (eCommerce companies) and tools (more_eggs) were used in both reported attack campaigns.

Later that year, in August 2019, security researchers found that the FIN6 group began another malicious campaign. The researchers believe the FIN6 threat actors were actively going after multinational organizations. Similar to the current incident, FIN6 spearphished specific employees with fake job offers. If the targets fell for the lure, they too were infected with the more_eggs backdoor.

**Evilnum-** The Evilnum cybercrime group is best known for compromising financial technology companies, companies that provide stock trading platforms and tools. Their target is financial information about the targeted FINTECH companies and their customers. They target items such as spreadsheets and documents with customer lists, investments and trading operations and credentials for trading software/platforms and software.

Coincidentally, the Evilnum group is also known to spearphish employees of the companies they are targeting and enclose malicious zip files. If executed, the employees get hit with the more_eggs backdoor, along with other malware.

**Cobalt Group-** The Cobalt Group is also known to go after financial companies, and it has repeatedly used the more_eggs backdoor in their attacks.

## What is the Victim's Industry?

The LinkedIn member is in the healthcare technology sector.

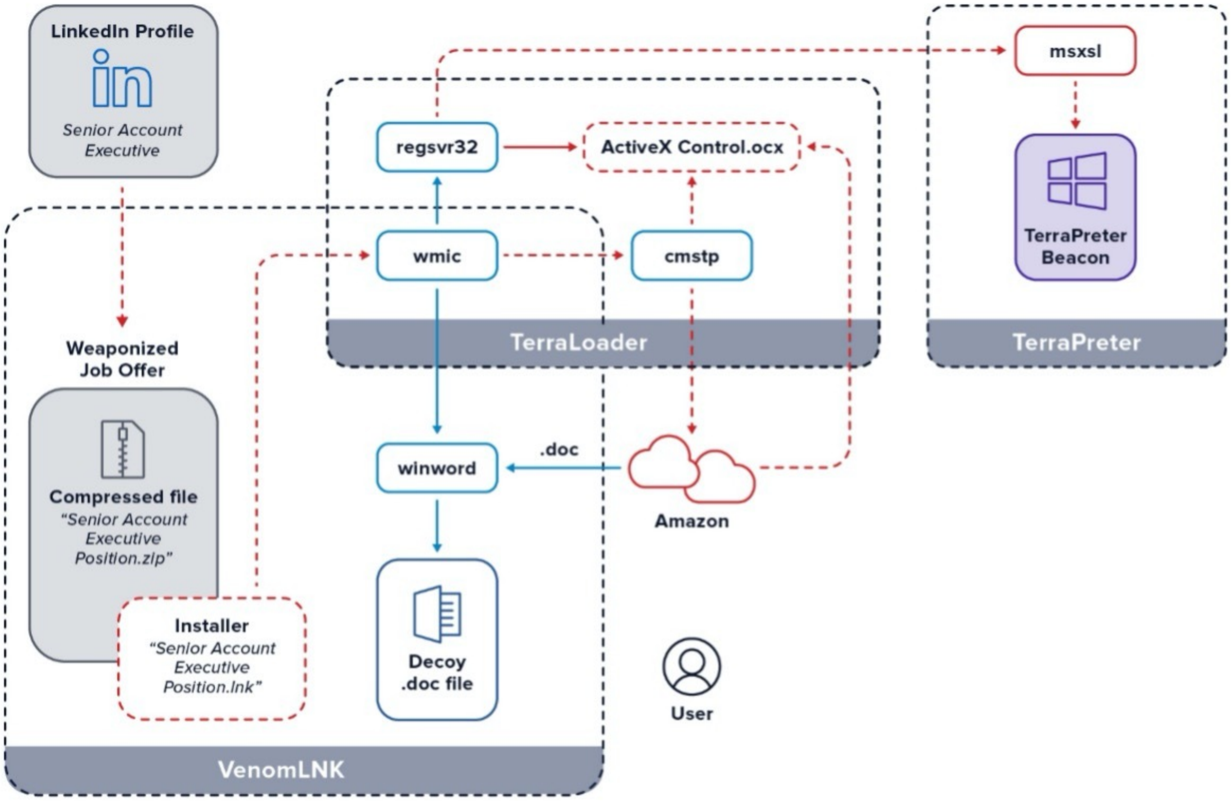
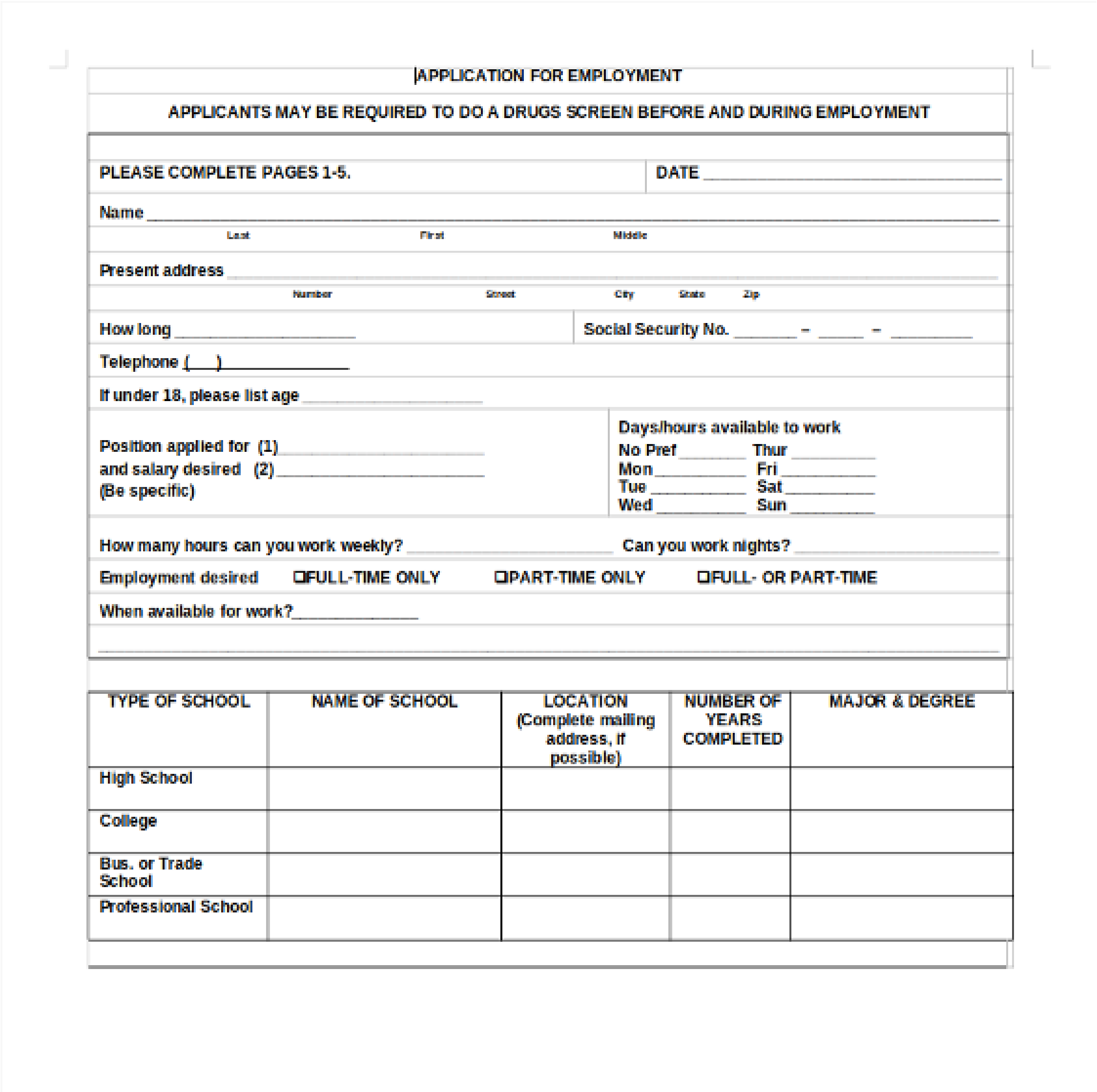


**Image1:** An outline of how the more_eggs backdoor behaves once it is initiated by the victim.



APPLICATION FOR EMPLOYMENT

APPLICANTS MAY BE REQUIRED TO DO A DRUGS SCREEN BEFORE AND DURING EMPLOYMENT

PLEASE COMPLETE PAGES 1-5. DATE ____________________

Name ____________________________________________
Last First Middle

Present address ____________________________________________
Number Street City State Zip

How long ____________ Social Security No. ______ - _____ - ________

Telephone (___) ____________

If under 18, please list age ____________

Position applied for (1) ____________
and salary desired (2) ____________
(Be specific)

Days/hours available to work
No Pref ________ Thur ________
Mon ________ Fri ________
Tue ________ Sat ________
Wed ________ Sun ________

How many hours can you work weekly? ____________ Can you work nights? ____________

Employment desired □FULL-TIME ONLY □PART-TIME ONLY □FULL- OR PART-TIME

When available for work?____________

| TYPE OF SCHOOL | NAME OF SCHOOL | LOCATION (Complete mailing address, if possible) | NUMBER OF YEARS COMPLETED | MAJOR & DEGREE |
|---|---|---|---|---|
| High School | | | | |
| College | | | | |
| Bus. or Trade School | | | | |
| Professional School | | | | |

**Image 2:** Word document which poses as an employment application which is served up to the business professional once they download the zip file which alleges to be a job offer.

## Indicators

**C2 beacon: d27qdop2sa027t.cloudfront[.]net**

**Download Server: ec2-13-58-146-177.us-east-2.compute.amazonaws[.]com**

**.zip hash: 776c355a89d32157857113a49e516e74**

**Ipconfig: cmd /v /c ipconfig /all > "C:\Users\<REDACTED>\AppData\Local\Temp\64813.txt" 2>&1**

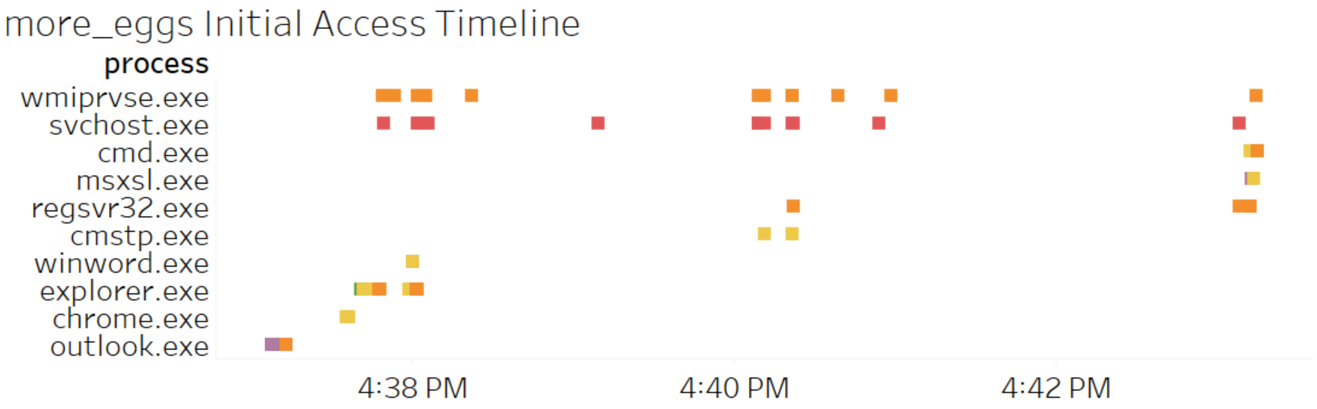
**regsvr32 /s /u "C:\Users\<REDACTED>\AppData\Roaming\Microsoft\<REDACTED>.ocx"**

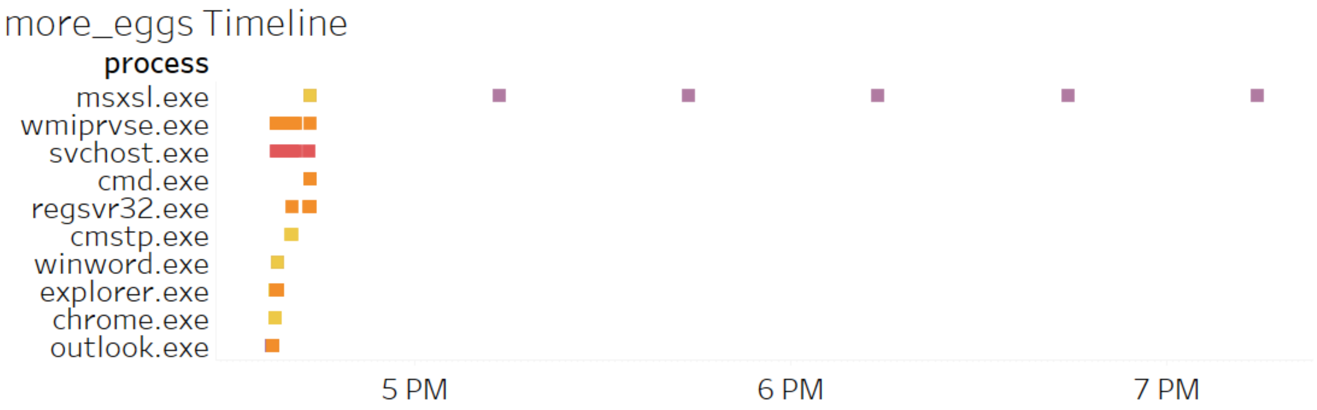
**sh = new ActiveXObject("Shell.Application")**

```
sh.ShellExecute("msxsl.exe", "<REDACTED>.txt <REDACTED>.txt", "C:\Users\<REDACTED>\AppData\Roaming\Microsoft\", "", 0)
```

```
evlinum js: C:\Users\<REDACTED>\AppData\Roaming\Microsoft\57930.ocx
```

## Timelines





[1] https://quointelligence.eu/2020/01/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors/

[2] https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers