



## CYBERSPACE THREAT ADVISORY



Defensive Cyberspace Operations Division (DCO-D)  
US Army Regional Cyber Center - CONUS

ID: 005  
20161110

### **SUBJECT: Locky Targets OPM Breach Victims**

#### **Bottom Line Up Front (BLUF)**

It is expected that the distribution base of this notification has an increased likely hood of being impacted by this phishing campaign than others due to the subject matter. There is an ongoing phishing email campaign currently which is delivering Locky ransomware posing as a warning letter from the US Office of Personnel Management (OPM) regarding fraudulent bank account activity for the victim. Be aware that you should not open attachments unless you can verify the authenticity and identity of the sender in question.

#### **Details**

The perpetrators of this phishing campaign are impersonating OPM officials in the email communications they are sending out. It is worth noting that the US Office of Personnel Management (OPM) is not monitoring your bank activity. If you were previously notified of the breach of your personal information OPM provided you with an opportunity to sign up for credit/identity monitoring. This service is not being provided by OPM this monitoring service was generally offered up by a third part monitoring provider such as CSID or ID Experts<sup>1</sup>.

Here is one example of the email. As noted by the phishme.com website there is strange wording within this email that should raise suspicions such as "suspicious movements" and "out account".

Dear [REDACTED] Carole from the bank notified us about the suspicious movements on out account. Examine the attached scanned record. If you need more information, feel free to contact me.

---  
King regards,  
Eli Lucas  
Account Manager  
Tel.: 202-767-1800  
U.S. Office of Personnel Management  
1668 E Street, NW  
Washington, DC 20415-1000

Screenshot of phishing message impersonating OPM

<sup>1</sup> <https://krebsonsecurity.com/2015/09/opm-missspends-133m-on-credit-monitoring/>



The Locky ransomware is delivered in multiple fashions the largest distribution of this campaign appears to be .zip files which contains a .js file. Understand that there are a number of measures in place to detect and prevent this type of activity within Army networks. It is unclear if the campaign actors have access to the OPM breached data or if they are just blindly targeting individuals. It is worth noting that while individuals may have entered their Department of Defense email address within their OPM documentation it is more likely that a personal account was used while applying for their security clearance.

## RECOMMENDATIONS

- If there is any doubt about the authenticity of an email urging you to open an attachment do not open it, it's better to be safe than sorry.
- Understand that the perpetrators of this campaign are attempting to use fear to trick individuals into executing this payload.
- If you had previously agreed to identity monitoring as provided by OPM check your records to determine which company is providing this service to you and contact them directly regarding their monitoring activities.

Sources:

<https://threatpost.com/locky-targets-opm-breach-victims/121879/>

<http://phishme.com/unscrupulous-locky-threat-actors-impersonate-us-office-personnel-management-deliver-ransomware>

For questions or comments regarding the content within this report, please contact the DCO-D at [usarmy.huachuca.2rcc-wh.mbx.dco-d@mail.mil](mailto:usarmy.huachuca.2rcc-wh.mbx.dco-d@mail.mil) (NIPR) or [usarmy.huachuca.2rcc-wh.mbx.dco-d@mail.smil.mil](mailto:usarmy.huachuca.2rcc-wh.mbx.dco-d@mail.smil.mil) (SIPR)

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**