16 July 2015

Alert Number

A-000062-PH

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Local Field Offices:
www.fbi.gov/contact-us/field

Spear-phish Campaign Targeting US Government Agencies

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Summary

The FBI is providing the following information with **HIGH confidence**

The FBI has observed malicious actors targeting US Government Agencies with spear phish messages likely for the purpose of obtaining sensitive information. This new, likely ongoing campaign, is similar to another campaign that occurred in June. In the June campaign, private sector and US government agencies were targeted, so it is possible that some private sector organizations may be targeted during this campaign as well.

Technical Details

The FBI is providing the following information with **HIGH confidence**

The FBI has received information regarding a likely ongoing phishing campaign that started 08 July 2015 and was observed targeting US government agencies. This campaign is similar to a June campaign launched by similar malicious actors. In both campaigns, the e-mails contain a link that exploits Adobe Flash vulnerability CVE-2015-5119.

JULY 8TH PHISHING EMAIL

SUBJECT: BBW Analysis report- 2015
FROM: Alan Mertner <allan.mertner@perrydale.com>
Sender IP: 125.227.139.53

Federal Bureau of Investigation, Cyber Division

Flash Notification

SUBJECT: Tomorrow Morning New Starts
FROM: Alan Mertner <allan.mertner@perrydale.com>
Sender IP: 125.227.139.53

SUBJECT: Perrydale Club for Leadership: Financial Literacy 101
FROM: Alan Mertner <allan.mertner@perrydale.com>
Sender IP: 125.227.139.53

SUBJECT: FAS Analysis report-2015
FROM: Alan Mertner <allan.mertner@perrydale.com>
Sender IP: 125.227.139.53

Preliminary analysis on the chain of events for the 08 July 15 infection campaign are as follows:

The e-mails contain a malicious link: hxxp://rpt.perrydale.com/en/rep201507101.pdf

This link loads a page which then loads a javascript file, index.js

This javascript file loads a flash file, show.swf, which pulls down an additional file, b.gif and beacons out to the following C2s:
hxxp://ivc.jiscs.com/logo/logovv.gif
hxxp://psa.perrydale.com/*
hxxp://link.angellroofing.com/*
* indicates the rest of the URL seems to be randomized

MD5s:

File	File Size	MD5
b.gif	184307	a2913de395ffc17195e8ace0cee8c969
Index.js	1170	3c4d7c9c006fe88cadf7a912629727b6
Rep201507101.pdf	318	e131c8e162829571ec54426e373d1d0f
show.swf	15485	e9a57f70f739cb26dc053238b0a97425

In June, similar malicious actors launched another phishing campaign targeting US Government Agencies and private sector companies involved in Information Technology/Telecommunications, Aerospace, Construction, Engineering and Transportation.

JUNE 8TH PHISHING EMAIL
SUBJECT: AEP Energy Program Update: 2015 Program Year Kick Off
FROM: Adam L Hannah <Adam.hannah@cacti.twixel.be>
DATE: June 8th, 2015 10:43PM CT
LINK: http://ml.r-u.org.ua/message/
BODY: In this update: Material and Installation Standards Training, Quality Assurance Quality Control (QA/QC) and Scoring System Training, Kick Off Meeting

Federal Bureau of Investigation, Cyber Division

Flash Notification

No Images? Click here...
IN-HOME ENERGY PROGRAM
CONTRACTOR UPDATE
2015 Program Year Kick Off!

JUNE 9TH PHISHING EMAIL
SUBJECT: Review Link
FROM: Adam L Hannah <Adam.hannah@cacti.twixel.be>
DATE: June 9th, 2015 3:49AM CT
LINK: http://ml.r-u.org.ua/message/
BODY: Here's that link that you can post. This should take anyone to a review form. They don't even need to be a member to leave a review. If non-members leave a review and become a member later, the review will turn into a member review!
Let me know if you have any other questions!
Read More
Thanks,
Adam Hannah
Advertising Account Manager

JUNE 11TH PHISHING EMAIL
SUBJECT: PLS Account A42660861
FROM: Carrie Spencer <Carrie.Spencer@lumbix.com>
DATE: June 11th, 2015 11:34AM CT
LINK: http://ml.r-u.org.ua/message/

Additional indicators recently obtained. Network traffic associated with the following IP addresses/domains should be analyzed for malware activity.

- 107.20.255.57
- dublincore.org
- 125.227.139.53
- bwxt.com