Department of Labor Strategic Web Compromise

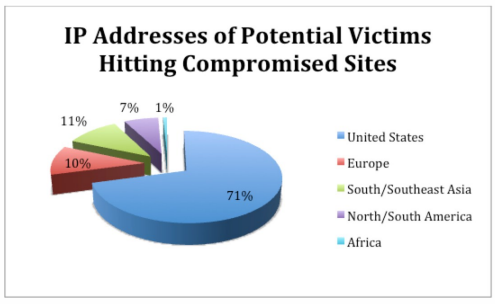
May 3, 2013 Matt Dahl Research & Threat Intel

On April 30, 2013, CrowdStrike was alerted to a strategic web compromise on a US Department of Labor website that was redirecting visitors to an attacker's infrastructure. Eight other compromised sites were also reported to be similarly compromised with the data suggesting that this campaign began in mid-March.

The campaign appeared to exploit visitors to these sites via the recent CVE-2012-4792 vulnerability, however CrowdStrike recently learned from other researchers that the exploit leveraged appears to be a zero-day. Successful compromise resulted in infection with Poison Ivy. The sample observed infecting visitors to the Department of Labor website was conime.exe file (MD5: 8f287f2bc83a8df06a39020f25cd91da) with a build timestamp of April 6, 2013 at 17:53:18 UTC. The RAT attempted to connect to a C2 server at microsoftupdate.ns1.name on TCP ports 80, 443, 53, and 8080. This domain has been seen pointing at two IPs: 173.254.229.176 and 13.58.46.78. It uses a password of "japan092wsx$RFV" to authenticate itself at the backend and installs a mutex named "!)xdrA.I4."

Victimology

Analysis of logs from the malicious infrastructure used in this campaign revealed the IP addresses of visitors to the compromised sites which showed hits from 37 different countries. Here is the breakdown of these IP addresses by region:



It is important to note that the data analyzed showed IP addresses before exploit code was run against the visitors' machines. It is possible that exploit code was not successful against all visitors to these sites, therefore all visitors may not have had their machines compromised.

Targeting

The legitimate sites compromised to deliver malicious code in this campaign give an indication into targets of interest. The specific Department of Labor website that was compromised provides information on a compensation program for energy workers who were exposed to uranium. Likely targets of interest for this site include energy-related US government entities, energy companies, and possibly companies in the extractive sector.

Based on the other compromised sites other targeted entities are likely to include those interested in labor, international health and political issues, as well as entities in the defense sector.

DEEP PANDA

CrowdStrike is aware of multiple reports linking this activity to the adversary CrowdStrike refers to as DEEP PANDA. At this time, CrowdStrike cannot verify this connection due to the C2 server being offline. There is a publicly available report on the CrowdStrike website detailing the indicators associated with the DEEP PANDA adversary. We continue to analyze this incident to verify the possible attribution of the DOL Strategic Web Compromise to the DEEP PANDA adversary.

The following Snort signatures will enable you to detect the Poison Ivy RAT used in this attack.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "[CrowdStrike] Poison Ivy Plugin - japan092"; flow: established, from_server; content: "|f2 b0 80 bf de 19 78 54 2b c7 85 86 97 6e 84 db b7 25 65 cc 16 02 d9 0e 9c be 3d 79|"; offset: 4; depth: 32; sid: x; rev: 1; )

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike] Poison Ivy Victim Keep-Alive  - japan092"; flow: established, to_server; dsize: 48; content: "|0f 07 06 1c 02 bc 42 51 ab ce 22 a7 a2 15 15 0c|"; offset: 0; depth: 16; sid: x; rev: 1; )

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "[CrowdStrike] Poison Ivy Controller Keep-Alive - japan092"; flow: established, from_server; dsize: 48; content: "|f2 82 18 f2 08 53 2e 19  24 d5 8b 54 44 73 55 87|"; offset: 0; depth: 16; sid: x; rev: 1; )
```

Be sure to follow @CrowdStrike on Twitter as we continue to provide updates on this topic. If you have any questions about this incident or the tradecraft used by these adversaries, please contact: intelligence@crowdstrike.com to inquire about our intelligence-as-a-service solutions where we provide actionable intelligence feeds and analysis of targeted attackers and their capabilities.

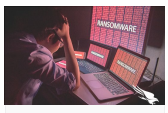
Related Content

Who is REFINED KITTEN?

Common Aliases REFINED KITTEN may also be identified by the following pseudonyms: APT33 Elfin Magnallium Holmium…

WIZARD SPIDER Adds New Features to Ryuk for Targeting Hosts on LAN

CrowdStrike® Intelligence analyzed variants of Ryuk (a ransomware family distributed by WIZARD SPIDER) with new functionality…



Ransomware Increases the Back-to-School Blues

As students all over the United States donned their backpacks and packed their lunches to go…

« Who is Samurai Panda

Rare Glimpse into a Real-Life Command-and-Control Server »