Watering Hole Attack Claims US Department of Labor Website

The United States Department of Labor website was hacked in a watering hole attack. The website was redirecting visitors to a malicious site hosting the Poison Ivy remote access Trojan.

The United States Department of Labor website is the latest high-profile government site to fall victim to a watering hole attack. Researchers at a number of security companies reported today that the site was hosting malware and redirecting visitors to a site hosting the Poison Ivy remote access Trojan.

The malware has since been removed and law enforcement is investigating.

The attackers inserted javascript onto the DoL's Site Exposure Matrices (SEM) website that sent visitors to another site hosting an exploit for CVE 2012-4792 targeting Windows XP users running Internet Explorer versions 6-8. The vulnerability, a user-after free memory vulnerability in the browser, enables attackers to remotely run code on a compromised machine. This has been exploited in the wild since December and was patched earlier this year by Microsoft.

"This profile fits the enterprise user machine profile typical of large enterprise and government agencies," said Invincea founder and CEO Anup Ghosh.

The DoL's SEM site is a repository of data on toxic substances present at facilities run by the Department of Energy.

The malware drops an executable called conime[.]exe onto the infected computer and opens remote connections on ports 443 and 53, Invincea said, adding there were two redirects present on the DoL page sending visitors to doll[.]ns01[.]us. Once the user is redirected, a file is executed, ports are opened and registry changes are made to maintain persistence on the machine. Ghosh said that one of the command and control servers had already been blacklisted by Google.

Alien Vault Lab manager Jaime Blasco said the attacker also collects a bit of system information including whether a number of antivirus programs, Flash, Java, and Microsoft Office are running, and sends that data to the remote server. Blasco added that the command and control protocol used in the attack matches that of a Chinese espionage gang known as DeepPanda; other characteristics of this attack match those used against a Thai human rights nongovernment organization website.

Watering hole attacks have been used primarily by state-sponsored attackers to spy on rival governments, dissident citizen groups and manufacturing organizations. Rather than rely on spear phishing, attackers infect websites of common interest to their targets, generally with javascript via an iframe that redirects the victim to a site hosting espionage malware. Some high-profile watering hole attacks have been carried out this year against the Council on Foreign Relations website and a popular iOS mobile developer forum that snared a number of victims at Facebook, Apple and Twitter.

In this case, it's likely the targets were Department of Labor employees and other federal employees tied to the DoL and Department of Energy.

"It is important to note that most websites are vulnerable to exploit. As a result, exploiting legitimate websites have become a common vector for penetrating enterprise networks and individual machines," Ghosh said. "The Department of Labor is no exception."

Share this article:

Malware

SUGGESTED ARTICLES

Spear-Phishing Attack Lures Victims With 'HIV Results'

Attackers are purporting to send victims HIV test results -- but in reality are convincing them to download the Koadic RAT.

March 30, 2020

Double Vision: Stealthy Malware Dropper Delivers Dual RATs

A lengthy, multi-stage infection process leads to a duo of payloads, bent on stealing data.

November 14, 2019

Ex-Twitter Employees Spied on Saudi Dissidents: DoJ

The DoJ charges former Twitter employees for allegedly accessing thousands of accounts on behalf of Saudi Arabia.

November 7, 2019

DISCUSSION

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 22, 2020 2

7 Tips for Maximizing Your SOC
December 31, 2019 5

Mean Time to Hardening: The Next-Gen Security Metric
December 30, 2019 4

Combining AI and Playbooks to Predict Cyberattacks
December 26, 2019 1

The Case for Cyber-Risk Prospectuses
December 24, 2019

Newsletter

Subscribe to *Threatpost Today*

Join thousands of people who receive the latest breaking cybersecurity news every day.

Subscribe now

Twitter

A poll of Threatpost readers shows that #security preparedness is uneven as organizations make an unprecedented tra... https://t.co/HHY7XHNF0W

12 hours ago

Follow @threatpost

Subscribe to our newsletter, *Threatpost Today*. Get the latest breaking news delivered daily to your inbox.

Subscribe now

Copyright © 2020 Threatpost - Privacy Policy - Terms and Conditions - Advertise