AlienVault Labs meldet: Gehackte Website des U.S. Department of Labor streut Schadcode

AlienVault Labs meldet: Gehackte Website des U.S. Department of Labor streut Schadcode

Schädling späht Rechner aus und lädt Daten auf verseuchten Server hoch
Wie die Experten der AlienVault Labs herausfanden, wurde die Website des U.S. Department of Labor gehackt. Beim Besuch der Seite führt sich automatisch eine Malware aus, die wichtige Informationen über den Rechner des Users ausspäht und diese an einen verseuchten Server weiterleitet. Zum Beispiel stellt sie die vorhandene Microsoft Office-Lösung sowie die verwendete Java-Version fest. Außerdem ermittelt der Schädling, welche Anti-Viren-Software installiert ist, und versucht diese zu deaktivieren. Anschließend lädt die Malware einen Schadcode auf das System.
Bei der angegriffenen Webseite handelt es sich um die Präsenz des US-amerikanischen "Department of Labor (DOL; Arbeitsministerium) und deren Unterseite "Site Exposure Matrices (SEM)". Dies ist eine Sammlung von verschiedenen Quellen zu toxischen Substanzen, ermittelt durch das Department of Energy (DOE) sowie die "Radiation Exposure Compensation Act (RECA)-Einrichtungen. Wie die Experten der AlienVault Labs ermittelten, reicht der Besuch der Site aus, um den Rechner mit der Malware zu infizieren. Sie spioniert den Rechner aus und analysiert neben Details zum Betriebssystem u.a. die Flash Player-Version sowie Erweiterungen des Browsers Google Chrome, die auf die verwendete Antivirensoftware hinweist. Generell späht der Schädling aus, welche Security Suite auf dem Rechner vorhanden ist, und versucht sie zu deaktivieren, um unerkannt zu bleiben. Sobald der Schädling alle gewünschten Daten gesammelt hat, sendet er diese mittels POST-Request an die URL dol[.]ns01[.]us:8081/web/js[.]php.
Threat kopiert sich selbst
Zum Zeitpunkt der Analyse gingen die AlienVault-Spezialisten davon aus, dass der bösartige Server die Schwachstelle CVE-2012-4792 nutzt. Darüber wird schließlich Schadcode auf das System geladen. Sobald dieser den Rechner infiltriert hat, erstellt die Malware eine Kopie von sich selbst im Ordner "Documents and Settings[CURRENT_USER]Application Dataconime.exe". Zudem legt sie einen Registry-Schlüssel an, der auf conime.exe auf "KEY_USERSSoftwareMicrosoftWindowsCurrentVersionRun conime" hinweist. Nicht zuletzt verbindet sich der Threat mit einem C
 C auf microsoftUpdate.ns1.name, der zum Untersuchungszeitpunkt auf einen Google DNS server 8.8.8.8. hinweist.
Weitere Informationen stehen auf der Seite der AlienVault Labs bereit.
Über AlienVault:
Die Unified Security ManagementTM-Plattform AV-USM von AlienVault ebnet Unternehmen mit eingeschränktem Security-Personal und Budget einen schnellen und kostengünstigen Weg, Anforderungen an Compliance und Threat Management zu erfüllen. Da alle essenziellen Kontrollfunktionen bereits integriert sind, verschafft die AV-USM gerade kleinen Security-Teams eine Enterprise-Class-mäßige Security-Umgebung. AlienVaults Open Threat ExchangeTM, ein System für den Austausch zum Thema Threat Intelligence zwischen OSSIM-Nutzern und AlienVault-Kunden, stellt dabei sicher, dass AV-USM den Bedrohungen stets einen Schritt voraus ist. AlienVault ist ein Privatunternehmen mit Hauptsitz in Silicon Valley (Kalifornien/USA) und wird von Kleiner Perkins Caufield
 Byers, Sigma, Trident Capital und Adara Venture Partners unterstützt. Die Märkte in Deutschland, Österreich und der Schweiz werden von der AlienVault Deutschland GmbH mit Sitz in Ismaning betreut. Für weitere Informationen besuchen Sie www.alienvault.com oder folgen Sie uns auf Twitter.

AlienVault Deutschland GmbH
Gutenbergstraße 6
D-85737 Ismaning
 www.alienvault.com
Oliver Bareiss
Regional Director DACH and Central Europe
Tel.: +49 (0) 89-32 60 70 91
Fax: +49 (0) 89-97 89 93 42
E-Mail: obareiss@alienvault.com
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Fabian Sprengel
Tel.: +49 (0) 26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: alienvault@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=533190" width="1" height="1">

Pressekontakt

AlienVault Deutschland GmbH

85737 Ismaning

obareiss@alienvault.com

Firmenkontakt

AlienVault Deutschland GmbH

85737 Ismaning

obareiss@alienvault.com

Weitere Informationen finden sich auf unserer Homepage