

vor einem Jahr

in IT/Hightech und Digital World

Weitere Malware nutzt Microsofts LNK-Sicherheitslücke aus

ESET warnt vor Win32/TrojanDownloader.Chymine.A und Win32/Autorun.VB.RP

(ddp direct) Der Antivirenhersteller ESET hat zwei neue Schädlinge in freier Wildbahn entdeckt, welche die Microsoft LNK-Sicherheitslücke (CVE-2010-2568) ausnutzen. Win32/TrojanDownloader.Chymine.A und Win32/Autorun.VB.RP beabsichtigen – im Gegensatz zu Win32/Stuxnet – eine möglichst große Verbreitung.

Hat Win32/TrojanDownloader.Chymine.A einen Rechner infiziert, lädt der Schädling den Keylogger Win32/Spy.Agent.NSO trojan aus dem Internet herunter und installiert ihn. Dieser zeichnet alle Tastatureingaben auf und leitet sie an die Malwareautoren weiter. Der Server, der diese verseuchten Dateien bereitstellt, befindet sich derzeit in den USA. Dessen IP-Adresse ist jedoch auf einen Kunden in China registriert.

Auch Win32/Autorun.VB.RP nutzt die CVE-2010-2568 Lücke als zusätzlichen Verbreitungsweg. Die Malware lädt ebenfalls weitere Komponenten herunter und installiert sie auf dem befallenen PC.

Die neuen Schädlinge beabsichtigen eine möglichst starke Verbreitung und sind somit auch für den Endanwender eine ernste Bedrohung. Sie unterscheiden sich somit von Win32/Stuxnet, das „nur“ einzelne Ziele attackierte.

In einem Punkt unterscheiden sich Win32/TrojanDownloader.Chymine.A und Win32/Autorun.VB.RP deutlich: Letzterer ist in der Lage, neue LNK-Dateien zu erzeugen und sich so fortzupflanzen. Win32/TrojanDownloader.Chymine.A ist hingegen auf „Hilfe“ angewiesen, um sich weiter zu verbreiten.

Abgesehen vom Ausnutzen einer zero-day-Sicherheitslücke zeigt Win32/Stuxnet weitere interessante Eigenschaften, wie z.B. die gezielte Attacke auf das SCADA-System von Siemens und den Einsatz von gestohlenen Software-Zertifikaten. Die neu entdeckten Schädlinge sind jedoch keine extrem ausgefeilte Neuentwicklung. Sie setzen lediglich auf bekannte Schädlinge auf bzw. auf deren Technologien, die von anderen entwickelt wurden.

Diese Entwicklung zeigt erneut den mittlerweile typischen Weg in der "Malware-Evolution". Die Abstände zwischen dem Bekanntwerden einer neuen kritischen Sicherheitslücke und der Anpassung von Malware, die genau diese ausnutzt, werden immer kürzer. Es ist ziemlich sicher, dass Malware-Autoren diese Lücken verstärkt nutzen werden, um ihren Schadcode zu verbreiten und somit ihre Gewinne zu maximieren.

Weitere Informationen erhalten Sie unter <http://blog.eset.com/> oder <http://www.eset.de>.

ESET - we protect your digital worlds

Seit 1992 schützt ESET mit modernsten Antimalwarelösungen Unternehmen und Privatanwender vor PC-Schädlingen aller Art. Der slowakische Sicherheitsspezialist gilt - dank der vielfach ausgezeichneten ThreatSense-Engine - als Vorreiter bei der proaktiven Bekämpfung selbst unbekannter Viren, Trojaner und anderer Bedrohungen. Die hohe Malwareerkennung und Geschwindigkeit sowie eine minimale Systembelastung zeichnen die Top-Produkte ESET NOD32 Antivirus und ESET Smart Security aus.



ESET hat seine Zentrale in Bratislava (Slowakei) und besitzt eigene Niederlassungen in Prag (Tschechische Republik), San Diego (USA), Bristol (UK) und Buenos Aires (Argentinien). ESET-Lösungen sind über ein Netz exklusiver Distributoren, wie bspw. DATSEC in Deutschland, in mehr als 180 Ländern weltweit erhältlich.

DATSEC Data Security e.K.
Talstraße 84
07743 Jena
Deutschland

E-Mail: [Kontakt aufnehmen](#)

Pressekontakt

Herr Michael Klatte

DATSEC Data Security
Talstraße 84
07743 Jena

Email: [Kontakt aufnehmen](#)
Website: <http://www.eset.de>
Telefon: +49 3641 3114 257
Fax: +49 3641 3114 299

Schlagworte

ESET Win32/Stuxnet LNK
Sicherheitslücke Microsoft

Permanenterlink

<http://www.themenportal.de/it-hightech/weitere-malware-nutzt-microsofts-lnk-sicherheitsluecke-aus-59699>

Website: www.eset.de
Telefon: +49 3641 3114 250
Fax: +49 3641 3114 299

© 2010 ddp direct GmbH | Impressum | AGB

ddp || direct
mehr Medien

 themen || portal