15.12. 2015

Schweizer Anti-Malware-App rüstet auf und macht Social Hackern den Garaus

Von LUCY security

Bild Rechte
Oliver Münchow

LUCY 2.6 wird Schweizer Taschenmesser des Cyber-Wars

(Thalwil) DIE Schweizer Malware-Simulations-App LUCY deckt nach ihrem jüngsten Update 2.6 das gesamte Angriffsspektrum des Social Hackings ab. Damit wird LUCY weltweit zur ersten herunterladbaren Applikation, mit der sich neben Phishing und Malware- auch SMiShing-Attacken auf jedem Handy, auf allen Kontinenten, simulieren lassen (s.u. für Begriffserklärungen). Außerdem ist die App nun in der Lage, Simulationen mit “harmlosen” Office Makroviren durchzuführen. Dies ermöglicht es Firmen, in die Schuhe eines Profi-Hackers zu schlüpfen und auf diese Weise sowohl die eigenen Sicherheitsstandards zu überprüfen, als auch ihre Mitarbeiter für bestehende Gefahren zu sensibilisieren. Die App deckt ausschließlich digitale Sicherheitslücken in der eigenen Firma auf. Ein Missbrauch wurde von den

Entwicklern ausgeschlossen.

„Reines Phishing war gestern," sagt LUCYs Gründer und CEO Oliver Münchow. „Auf gefälschte Emails, von denen viele Firmen jahrelang überflutet wurden, fällt heutzutage kaum noch jemand herein. Der moderne Hacker nutzt viel perfidere Methoden. Das Stichwort heißt Social Hacking, bei dem sich die Rolle des Mitarbeiters auf die Übertragung einer Malware beschränkt. Beispiele sind Makro-Attacken, SMiShing und BadUSB (s.u.), doch die Liste von Social-Hack-Variationen ist mittlerweile so lang, dass sie sogar den Kenntnisstand so mancher hauseigenen IT-Sicherheitsabteilung übersteigt. Bei erfolgreicher Datenentwendung die Schuld beim unvorsichtigen Benutzer zu suchen, greift daher viel zu kurz."

LUCY ermöglicht es Firmen, mit oder ohne Einbeziehung der Mitarbeiter, selbst in die Rolle eines Hackers zu schlüpfen und alle möglichen Angriffsmethoden zu simulieren. Die App zeigt gnadenlos sämtliche Schwachstellen im bestehenden Sicherheitssystem auf und demonstriert, welcher Schaden entstanden wäre, wenn es sich um einen echten Angriff gehandelt hätte. Dabei eignet sich die App in ihrer Anwendung sowohl für IT-Laien, als auch für Experten.

„Mit unserem jüngsten Update auf LUCY 2.6 reagieren wir auf aktuelle Entwicklungen und Prognosen in der Welt des Hackings," so Münchow. "Die zu Beginn des Jahres veröffentlichte Warnung von Microsoft1 hinsichtlich von Malware, die mittels Makros installiert wird, hat sich seit dem nur bestätigt und belegt die zunehmende Verbreitung derartiger Attacken. Am beängstigendsten ist dabei die Tatsache, dass diese Attacken sich so einfach realisieren lassen und ganze Weltkonzerne ins Wanken bringen. Man denke an den berüchtigten SONY-Datenklau oder den Milliardendiebstahl durch die Carbanak Gang. Mit LUCY können Firmen nun überprüfen, ob ihnen aktuell etwas Ähnliches widerfahren könnte und ihre Sicherheitsstandards gegebenenfalls rechtzeitig und zielgerichtet verbessern."

In der Basisversion ist die Verwendung von LUCY bei Firmen mit bis zu 100 Mitarbeitern kostenlos. Um die App in größerem Umfang zu nutzen, existieren gestaffelte Preispakete, zugeschnitten auf die individuellen Bedürfnisse verschiedener Zielgruppen (s. phishing-server.com/PS/doc/dokuwiki/doku.php?id=lucy_pricing).

LUCY wurde von Münchow und einem Team aus Schweizer IT-Experten entwickelt und ist seit Januar 2015 online. Bislang ist die App vor allem im US-amerikanischen Raum

bekannt und wurde seit ihrer Veröffentlichung bereits von über 3000 Firmen heruntergeladen. Vor seinem jüngsten Update beschränkte sich das Tool jedoch auf Phishing-Attacken. Aufgerüstet mit modernsten Social-Hacking-Simulationen will Muenchow mit LUCY 2.6 nun auch aktiv in den europäischen Markt einsteigen.

+++

Kurze Begriffserklärungen

Phishing: Das Wort “Phishing” leitet sich vom englischen Wort “fishing” ab und bezeichnet das Angeln nach geheimen Daten oder Passwörtern. Dabei sendet der Hacker zum Beispiel eine E-Mail mit einem Link und der Aufforderung, persönliche Daten zu aktualisieren. Der Link führt zu einer Webseite, die beispielsweise der der eigenen Bank zum Verwechseln ähnlich sieht. Das Opfer füllt seine Daten ein, die so an den Hacker gelangen.

SMiShing: Beim Smishing („Smishing“ steht für SMS Phishing) wird die Täuschung des Absenders perfektioniert: da der Angreifer die Nummer des Absenders frei definieren kann, erscheint eine von ihm gesendete SMS als der vertraute Kontakt, der im Telefon gespeichert ist. Es gibt keine Unterscheidungsmöglichkeit. Wird man vom eigenen Vorgesetzten oder einer befreundeten Person via Kurzmitteilung aufgefordert, sich mal schnell eine Webseite anzusehen, tappt die Falle rasch zu.

Makro-Attacken: Bösartige Emailanhänge, die als gewöhnliche Worddokumente o.ä. getarnt sind und nach dem Öffnen selbstständig und unbemerkt Nutzdaten eines vom Angreifer manipulierten Servers herunterladen. Auf diese Weise kann sich der Hacker auf dem Computer des Angegriffenen einnisten.

BadUSB: Beim BadUSB täuscht der Datenträger dem PC eine nicht vorhandene Hardware vor und führt die Malware beim Einstecken automatisiert, ohne Zutun des Benutzers, aus. Der Angreifer muss somit nur das Opfer verleiten, den USB in den Computer zu stecken. Da reicht es meist aus, irgendwo auf öffentlich zugänglichen Ablageflächen oder sogar auf dem Boden ein paar USB Datenspeicher zu streuen. Die Neugier erledigt dabei den Rest.

1 blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx

Pressekontakt:

CEO: Oliver Münchow
Lucy Phishing GmbH
Seestrasse 13
8800 Thalwil
Switzerland
Webseite (Englisch): http://phishing-server.com/
Email: info@phishing-server.com
Tel: +41 79 6959510

Pressekontakt: Rebecca Jeffreys, Tel. +49 176 72155441, Email: rebecca@lucysecurity.com
LUCY

Kategorie
IT & Software & Neue Medien
