Aus den SophosLabs: VBAs sind quicklebendig

Die bereits für ausgestorben befundene Malwareform Visual Basic Code (VBA) wird seit einigen Monaten wieder vermehrt gesichtet, wie die SophosLabs bereits im Juli berichteten. Neue Statistiken zeigen nun einen sprunghaften Anstieg.

Karlsruhe, 28. Oktober 2014 – Gabor Szappanos, Forschungsleiter bei SophosLabs beobachtet seit einigen Monaten das jähe Auftauchen der fast schon vergessenen Makrovirenart Visual Basic Code. Neueste Beobachtungen des IT-Sicherheitsspezialisten Sophos zeigen einen Anstieg von Makro-basierter Malware von bescheidenen 6 Prozent aller Dokumentenmalware im Juni auf bemerkenswerte 28 Prozent im Juli. Warum ist das so?

Gegenüber der Nutzung bekannterer Exploits, so erklärt Graham Chantry, Senior Threat Researcher bei SophosLabs UK auf Naked Security, hat VBA einige nennenswerte Vorteile.

VBA vs. Exploits
Nur wenige Nutzer verzichten dieser Tage völlig auf Antiviren-Lösungen, Virenfamilien müssen sich also so häufig wie möglich verändern, um die Aufmerksamkeit des AV-Schutzes zu umgehen. Eine Exploit-Dateistruktur ist in der Regel eher statisch, was eine Bearbeitung schwierig macht.

Visual Basic-Code hingegen ist einfach zu schreiben, flexibel und leicht umzugestalten. Ähnliche Funktionalitäten können auf viele verschiedene Arten dargestellt werden. Malware-Autoren haben so mehr Möglichkeiten, bessere Versionen ihrer Software zu produzieren, als sie es über Exploits könnten. Diese sind zudem an bestimmte Versionen von Microsoft Office, gebunden. Die Malware-Autoren müssen also hoffen, dass die Opfer eine angreifbare Office-Version nutzen und ihr Antivirenschutz veraltet ist. Wird eine dieser Bedingungen nicht erfüllt, scheitert der Angriff.

Nicht so bei VBA. Der große Nachteil bei der Verwendung liegt allerdings in Microsofts Makro Security Level-Funktion. Bei Microsoft Office 2007 und höher sind alle Makros aus nicht vertrauenswürdigen Quellen standardmäßig deaktiviert und ihr Code wird nur ausgeführt, wenn der Benutzer sie explizit aktiviert. Um diese Einschränkung zu umgehen, müssen Autoren von bösartigem Code VBA Social Engineering-Techniken verwenden, um die User zur Ausführung der Makros zu bewegen.

Templates für Dummies
Spezialisten der SophosLabs haben entdeckt, dass es eine Reihe von VBA-Downloader-Vorlagen gibt. Diese enthalten Visual Basic-Code mit hilfreichen Kommentaren, wo die Autoren einen bösartigen Link sowie Informationen über Methoden zur Verschleierung des Codes einfügen sollten.

Der Code hat in der Regel ein einfaches Design. Einige der Templates importieren die Windows API URLDownloadToFile um eine ausführbare Datei in das Temporäre Verzeichnis der User zu

laden. Ist das geschehen, verwendet der Code einen Befehl um die Samples als separaten Prozess auszuführen.

Angehende Malware-Autoren müssen nur noch die Direct-Link-Here-Zeichenfolge mit einer URI zu der bösartigen, ausführbaren Datei übermitteln und der Downloader sollte fast wie von selbst funktionieren.

Diese Codestruktur ist äußerst beliebt. Tatsächlich wiesen zirka 34 Prozent aller Samples von Makro-Downloadern im Juli diese Struktur auf und waren mit Hunderten von verschiedenen URIs übersät, was darauf hindeutet, dass dies eine weit verbreitete und recht beliebte Vorlage ist.

Lügen und Betrügen – aber bitte sorgfältig
SophosLabs stieß vor kurzem auf eine Reihe Samples, die behaupten, mit "SOPHOS-Verschlüsselungs-Software" verschlüsselt worden zu sein. Zwar verfügt auch Sophos über eine Verschlüsselungssoftware – SafeGuard Encryption verschlüsselt Windows und Mac OS Endpoints – aber die Schreibweise war nicht identisch mit dem Original. Der Visual Basic Code in dem gefälschten Sophos Sample war durchaus anspruchsvoll. Abhängig von der Tatsache, ob PowerShell auf dem Computer installiert ist, konnte das Sample zwei unterschiedliche Methoden zur Infektion nutzen.

Ausgestorben ist VBA also ganz sicher nicht.

Mehr zu den technischen Details von VBA finden Sie hier:
http://nakedsecurity.sophos.com/2014/09/17/vba-injectors/

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-40-484434
sophos@tc-communications.de