News-Meldung vom 15.01.2010 09:32

Angriffe auf Google und Co. durch bislang unbekannte Lücke im Internet Explorer

Ersten **Analysen[1]** des Antivirenherstellers McAfee zufolge nutzten die vermutlich chinesischen Angreifer bei ihrem Einbruch eine bislang unbekannte Sicherheitslücke im Internet Explorer aus. Die Lücke findet sich in den Versionen 6, 7 und 8 und lässt sich missbrauchen, um über eine manipulierte Webseite Code in einen Windows-Rechner zu schleusen und zu starten. Die Angreifer nutzten dies, um einen Trojaner-Downloader in den angegriffenen Rechner zu schleusen. Der lud wiederum über eine SSL-gesicherte Verbindung weitere Module von einem Server nach, unter anderem eine Backdoor, mit der die Angreifer aus der Ferne Zugriff auf den Rechner hatten. Die Links zu den präparierten Webseiten wurden wohl an ausgesuchte Mitarbeiter in den jeweiligen Firmen per Mail gesendet.

Aufgrund der bei der Analyse der Malware gesammelten Daten glaubt McAfee, dass der konzertierte Angriff gegen Google, Adobe und Dutzende weiteren US-Firmen, darunter wahrscheinlich auch Yahoo, Symantec, Juniper Networks, Northrop Grumman und Dow Chemical, unter dem Codenamen "Aurora" ablief. Zumindest sollen Pfadnamen in den Binaries Rückschlüsse darauf zulassen. Zunächst war spekuliert worden, dass für die gezielten Angriffe präparierte PDF-Dokumente verwendet wurden – in den letzten zwei Jahren ein beliebtes Mittel der Angreifer, deren Spuren regelmäßig nach China führen. Zuletzt wurde ein derart großer Feldzug (Ghostnet) bei Angriffen auf ausländische Regierungen im März 2009 bekannt.

Überraschend kommen die neuen Angriffe nicht, eher überrascht es, wieviele Firmen nun Opfer geworden sind. Immerhin warnte die US-Regierung noch im September 2009, dass China seine Cyber-Spionage stärker ankurbele und dabei immer sorgfältiger und erfolgreicher vorgehe. Die nun bekannt gewordenen Angriffe sollen von Mitte Dezember bis Anfang Januar stattgefunden haben. Möglicherweise spielte den Crackern dabei in die Hände, dass in diesem Zeitraum viele Angestellte Urlaub hatten.

Microsoft hat die IE-Lücke **offiziell bestätigt[2]** und arbeitet bereits an einem Patch, den der Hersteller eventuell auch als "Emergency Patch" außerhalb der Reihe veröffentlicht. Laut Fehlerbericht ist die Lücke zwar in den Versionen 6, 7 und 8 zu finden, die Angriffe zielten aber bislang offenbar nur auf die Version 6 ab – eine interessante Aussage, die die Frage nach dem aktuellen Softwarestand in den betroffenen Unternehmen aufwirft.

Bis zu einem Update empfiehlt Microsoft, die Sicherheitseinstellungen für das Internet und das lokale Intranet auf "hoch" zu setzen. Da der gefundene Exploit JavaScript verwendet, hilft es zunächst auch, JavaScript zu deaktivieren. Zudem empfehlen die Redmonder, die Datenausführungsverhinderung (DEP) zu aktivieren. In den Versionen 7 und 8 ab Vista und später soll sich laut Bericht die Lücke nicht so einfach ausnutzen lassen, da der Internet Explorer dort im geschützten Modus läuft. Alles in allem sind also offenbar XP-Anwender mit Internet Explorer 6 am meisten gefährdet. Derzeit gibt es aber keinen öffentlich verfügbaren Exploit.

Siehe dazu auch:

- **"Rote Hacker": Cyber-Attacken aus China[3]**
- **US-Bericht: China verstärkt Spionageangriffe auf Unternehmen[4]**
- **Chinesische Spionage-Software infiltriert Rechner tibetischer Exil-Regierung[5]**
- **Antivirenhersteller rät vom Einsatz des Adobe Reader ab[6]**

(**dab[7]**)

URL dieses Artikels:
http://www.heise.de/security/meldung/Angriffe-auf-Google-und-Co-durch-bislang-unbekannte-Luecke-im-Internet-Explorer-905183.html

Links in diesem Artikel:
[1] http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/
[2] http://www.microsoft.com/technet/security/advisory/979352.mspx
[3] http://www.heise.de/meldung/Rote-Hacker-Cyber-Attacken-aus-China-904871.html
[4] http://www.heise.de/meldung/US-Bericht-China-verstaerkt-Spionageangriffe-auf-Unternehmen-837365.html
[5] http://www.heise.de/meldung/Chinesische-Spionage-Software-infiltriert-Rechner-tibetischer-Exil-Regierung-Update-210074.html
[6] http://www.heise.de/meldung/Antivirenhersteller-raet-vom-Einsatz-des-Adobe-Reader-ab-214661.html
[7] mailto:dab@ct.de