

Online-Tool analysiert Dateien bei Malwareverdacht

Wiener Entwicklung wird von internationalen Spezialisten genutzt



Anlässlich einer Veranstaltung des Austrian Security Forums hat gestern, Donnerstag, Markus Klemen, Geschäftsführer bei Secure Business Austria, das Projekt Anubis (ANalyzing Unknown BINarieS) vorgestellt. "Ich würde Anubis eine sichere Quarantänestation zur Beobachtung von Schadenssoftware nennen", beschreibt Klemen gegenüber presstext. Das Werkzeug liefert binnen weniger Minuten Informationen über eine etwaige Bedrohung durch eine ausführbare Datei und wird von Sicherheitsexperten etwa in Computer Emergency Response Teams (CERTs) weltweit als Analysehilfe genutzt.

Analys

"Es braucht ein System, mit dem Binärcode teilautomatisiert analysiert werden kann", erklärt Joe Pichlmayr, Geschäftsführer der am Projekt beteiligten Ikarus Software, die Motivation hinter der Entwicklung. Anubis analysiert ausführbare Dateien in einer Sandbox-Umgebung und liefert einen Report darüber, was beim Ausführen des Codes passiert. Was bei einer manuellen Analyse viele Stunden dauern kann, braucht dabei keine zehn Minuten. Das Ergebnis liefert einen Hinweis darauf, ob die Datei eine Bedrohung darstellt und auch, ob diese bereits bekannt ist. "Anubis ist ein ideales Tool für jeden, der verdächtige Dateien analysieren muss", meint daher Pichlmayr.

Selektion

Ikarus nutzt Anubis speziell zur Vorselektion. Wird etwa bekannte Malware identifiziert, ist dies meist eher statistisch interessant. Legt Anubis hingegen den Verdacht nahe, dass eine Datei eine neuartige Bedrohung ist, wird diese von einem Spezialisten genauer analysiert. Anubis wird längst auch über die Grenzen Österreichs hinaus von Experten genutzt. Pichlmayr nennt etwa das Australian CERT, das Japanese CERT sowie das renommierte SANS Institute als regelmäßige Anwender. Als Hinweis auf die Qualität von Anubis sei auch zu sehen, dass die Malware-Szene sogar spezielle Evasion-Techniken gegen Anubis entwickle, betont wiederum Klemen.

Warnung

Zwar gibt es eine Zusammenfassung der Ergebnisse, in der vor bestimmten Arten von verdächtigem Verhalten gewarnt wird, doch für Durchschnittsanwender ist das Tool nicht wirklich gedacht. Die detaillierten technischen Reports sind eher für IT-Spezialisten konzipiert. Normale User, die auf eine verdächtige Datei stoßen, seien meist besser beraten, diese zur Analyse an einen Antiviren-Hersteller zu senden oder zumindest mit einem Analysedienst wie VirusTotal zu prüfen, heißt es von Ikarus.

Uni

Maßgeblich auch an der weiteren Verbesserung von Anubis beteiligt ist das Secure Systems Lab der Technischen Universität Wien. Bei dem seit März 2007 verfügbaren Online-Service wurden bereits mehr als 400.000 verdächtige Dateien eingereicht. Nicht alle davon konnten auch analysiert werden, für einen noch umfassenderen Einsatz sind zusätzliche Server-Ressourcen nötig. (pte)



08. April 2008, 16:00 Uhr