



+ + + Pressemitteilung + + +

Trustwave verrät, wie Hacker mit Zero-Day-Lücken richtig Kasse machen

München, 14. Juni 2016 - Dass Cybercrime ein lohnendes Geschäftsmodell ist, zeigen unter anderem die detaillierten Untersuchungen des [Trustwave Global Security Report 2016](#). Doch wie viel Geld können Hacker eigentlich mit bisher unbekanntem Sicherheitslücken, sogenannten Zero-Day-Lücken, verdienen? Viel! Erst vor kurzem spürten die Experten des Trustwave-Spider-Labs-Teams im Darknet einen Hacker auf, der eine angeblich unbekannte Windows-Schwachstelle für knapp 100.000 US-Dollar anbot.

Ein russischer Hacker hat auf dem Online-Schwarzmarkt eine angebliche Windows-Sicherheitslücke angeboten, die Hunderte Millionen Nutzer betreffen soll. Die Schwachstelle soll in allen Windows-Versionen seit Windows 2000 enthalten sein und Angreifern einen uneingeschränkten Zugriff auf Windows-Rechner erlauben.

Der russische Hacker beschreibt die Sicherheitslücke, die in win32k.sys stecken soll, sehr detailliert und erklärt außerdem, was der Käufer für sein Geld erhält. Eine ins Englische übersetzte Version des Angebots steht im [SpiderLabs-Blog](#) zur Verfügung.

Das Einstiegsangebot des Hackers lag übrigens bei 95.000 US-Dollar, wurde dann aber auf 90.000 US-Dollar gesenkt.

Nach wie vor ist nicht geklärt, ob die vermeintliche Sicherheitslücke tatsächlich existiert. Microsoft ist das Angebot zwar bekannt, es ist aber nicht bekannt, ob Microsoft darauf reagiert hat.

Hacker, die Zero-Day-Lücken aufspüren, können auf jeden Fall eine ganze Menge Geld verdienen. Dafür müssen Sie übrigens nicht den Weg übers Darknet gehen. Firmen wie Microsoft zahlen als Belohnung für eine Zero-Day-Lücke zwischen 50.000 und 100.000 US-Dollar.

Recherchen des Trustwave-SpiderLabs-Blogs zeigen, dass Unternehmen für Zero-Day-Lücken auch deutlich höhere Beträge als Microsoft zahlen. Das auf Zero-Day-Exploits spezialisierte Unternehmen Zerodium bietet zum Beispiel bis zu [500.000 US-Dollar](#) für Zero-Day-Exploits.

Gegen unbekanntem Sicherheitslücken können sich Anwender zwar schwer schützen, grundsätzlich empfehlen die Experten des Trustwave-SpiderLabs-Teams aber folgende drei Punkte zu beherzigen:

- 1) **Software immer aktuell halten**
- 2) **Intelligente Security-Produkte installieren**
- 3) **Den gesunden Menschenverstand nutzen**

Druckfähiges Bildmaterial finden Sie hier:

http://www.laubstein-media.de/News/Trustwave_201606.zip

Pressemitteilung zum Download:

http://www.laubstein-media.de/News/PM_Trustwave_201606.pdf



Über Trustwave

Trustwave hilft Unternehmen die Cyberkriminalität zu bekämpfen, Daten zu schützen und Sicherheitsrisiken zu reduzieren. Mit Cloud- und Managed Security Services, integrierten Technologien und dem Trustwave SpiderLabs, einem Team von Sicherheitsexperten, bestehend aus ethischen Hackern und Forschern, unterstützt Trustwave die Unternehmen bei der Verwaltung und Umsetzung der IT-Sicherheit und den Compliance-Programmen. Mehr als drei Millionen Unternehmen sind auf der Trustwave TrustKeeper® Cloud-Plattform registriert, über die Trustwave ein automatisiertes, effizientes und kosteneffektives Schwachstellen-, Bedrohungs- und Compliance-Management anbietet. Trustwave ist in Chicago ansässig und verfügt über Kunden in 96 Ländern. Für weitere Informationen zu Trustwave, besuchen Sie bitte <https://www.trustwave.com> und <https://www.info-point-security.com/hersteller/ueber-trustwave>.

Pressekontakt:

Laubstein Media
Anja Eichelsdörfer
Untere Parkstr. 42
85540 Haar

Tel.: +49-89-41 85 84 85
Fax: +49-89-41 85 84 86
Mobil: +49-151-41 20 22 32

Mail: presse@laubstein-media.de
Web: <http://www.laubstein-media.de>