Trustwave SpiderLabs warnt vor Phishing-Attacken und neuen Cerber-Ransomware-Varianten

25.04.2017, 10:05 | IT, New Media & Software

Pressemitteilung von: *Trustwave*
Presseagentur: *Laubstein Media*

München, 25. April 2017 - Das Trustwave SpiderLabs, ein Team aus ethischen Hackern und IT-Forensikern, verrät, auf welche Cyber-Gefahren Sicherheitsbeauftragte in Unternehmen im Moment besonders achten müssen. Aktuell sind bei Hackern besonders Phishing-Attacken über die Outlook-Web-App beliebt. Außerdem sind neue Varianten der Ransomware Cerber im Umlauf, die von herkömmlichen Sicherheitslösungen im Regelfall nicht erkannt werden.

Es gibt keine Sicherheitslücke, die von Cyberkriminellen nicht früher oder später entdeckt wird. Woche für Woche untersuchen deshalb die Sicherheitsexperten des Trustwave SpiderLabs aktuelle Sicherheitsbedrohungen und zeigen, von welchen Angriffen aktuell am meisten Schaden droht. Die Untersuchungen werden weltweit durchgeführt.

Phishing-Attacken über die Outlook Web-App

Viele Anwender wissen, dass sie Links in E-Mails von unbekannten Absendern nicht anklicken dürfen. Wenn die E-Mail aber scheinbar von der eigenen IT-Abteilung kommt, denkt natürlich niemand an eine Phishing-Attacke. Und genau das machen sich Hacker gerade zunutze. In scheinbar harmlosen Mails wird zum Beispiel darüber informiert, dass die Obergrenze des Postfachs erreicht wurde oder das Passwort geändert werden muss. In einer zweiten Variante erhalten Nutzer eine E-Mail mit dem Anhang "SUPPORT HELP DESK.pdf".

Sobald der Anwender den enthaltenen Link oder das PDF-Dokument anklickt, wird er auf eine gefälschte Seite weitergeleitet. Auf diese Weise können bösartige Scripte Informationen von Benutzerkonten auslesen und so beliebige Schadcodes ins Unternehmensnetzwerk schmuggeln.

Auch wenn die Phishing-Attacken relativ gut gemacht sind, lassen sich diese trotzdem sehr schnell erkennen. Die Absende-und Empfängeradresse sind identisch, die E-Mail enthält Grammatikfehler und der enthaltene Link führt auf eine unbekannte Domain.

IT-Admins können zwar die entsprechenden IP-Adressen und Domains blockieren, da Phisher aber blitzschnell die Domains und IP-Adressen wechseln, sollten Unternehmen auf regelmäßige Sicherheitsschulungen nicht verzichten. Außerdem empfiehlt Trustwave den Einsatz einer leistungsfähigen E-Mail-Gateway- und Web-Gateway-Lösung.

Neue Varianten der Ransomware Cerber im Umlauf

Haben sich Hacker bei Ransomware-Attacken zunächst primär auf Privatnutzer konzentriert, geraten nun immer mehr Unternehmensnetzwerke ins Visier der Angreifer. Aktuell ist eine neue Variante der Ransomware Cerber im Umlauf. Sobald ein Anwender das entsprechende bösartige Dokument (meist eine Word- oder PDF-Datei) öffnet, wird ein bösartiges Makro ausgeführt, dass große Teile der Festplatte verschlüsselt. Nach der erfolgreichen Verschlüsselung erhält der Nutzer die folgende Meldung: "Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!"

Diese Ransomware-Variante wurde so programmiert, dass sie Statistiken der Infektion an verschiedene hardcodierte öffentliche UP-Subnetze übermittelt. Die Kommunikation findet über einen UDP-Tunnel (Port 6892) statt. Die WHOIS-Informationen führten zu Servern und Webseiten, die in Frankreich, Österreich und Ungarn registriert sind. Weitere Untersuchungen von Trustwave SpiderLabs haben gezeigt, dass Nutzer, die die schädliche Datei angeklickt haben, auf folgende Webseiten geführt wurden: hxxp://86vd5nf67c146v.sortban.loan/1fay69g32cidt und

hxxp://10et8431by7fa743.gunkind.com.

Da die Ransomware eine wirklich ausgereifte Verschlüsselungsmethode verwendet, die Dateien auf dem PC des Betroffenen wurden mit einem RSA asymmetrischen Algorithmus verschlüsselt und ständig angepasst wird, ist es für herkömmliche Sicherheitslösungen schwierig, Cerber-Attacken aufzuspüren. Trustwave empfiehlt, eine leistungsfähige Backup-Lösung zu installieren, mit deren Hilfe die verschlüsselten Daten problemlos wiederhergestellt werden können. Der infizierte Rechner sollte umgehend vom Netz genommen und neu aufgesetzt werden.

Druckfähiges Bildmaterial finden Sie hier:
http://www.laubstein-media.de/News/Trustwave_201704II.zip

Pressemitteilung zum Download:
http://www.laubstein-media.de/News/PM_Trustwave_201704II.pdf

Portrait

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.

News-ID: 948362 • Views: 731 (Stand: 21.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/948362/Trustwave-SpiderLabs-warnt-vor-Phishing-Attacken-und-neuen-Cerber-Ransomware-Varianten.html