



E-Mails mit erpresserischem Inhalt im Umlauf

Art der Bedrohung

Erpressung mit angeblichen Videoaufnahmen bei sexuellen Selbsthandlungen durch vorgegebene Sicherheitslücke am Computersystem. Zur Untermauerung des Vorhaltes werden tatsächlich existente Passwörter zu den E-Mail-Konten angeführt.

Modus Operandi

In einer früheren Erscheinungsform wurden diese „Erpresser E-Mails“ wahllos an zahlreiche E-Mail Empfänger/innen versendet, wobei „auf gut Glück“ versucht wurde, eine Antwort und/oder eine Bezahlung von den vermeintlich „erwischten“ Opfern erpressen zu können.

Das angebliche Videomaterial gibt es in den seltensten Fällen, jedoch sollte man nicht außer Acht lassen, dass durch verschiedene Sicherheitslücken (sog. Exploits) in Einzelfällen auch ein widerrechtlicher Zugriff auf den Computer oder die Kamera „von außen“ möglich wäre.

Regelmäßige Updates von Hardware und Software sind daher besonders wichtig!

Aufgrund zahlreicher aktueller Anlassfälle konnte beobachtet werden, dass in den nunmehrigen Erpresser-E-Mails auch ein Passwort zum jeweiligen Mail-Account angeführt ist. Dadurch soll bei dem/der Mailempfänger/in der Glauben erweckt werden, dass das Passwort durch den Absender ausgespäht worden ist. Nach Auskunft der Opfer handelt es sich dabei durchgängig um ältere oder sehr alte Passwörter, welche aber tatsächlich in Verwendung waren und zum Teil auch noch für andere Zugänge / Dienste im Internet genutzt werden.

Bei den Daten der angeschriebenen und erpressten E-Mail-Empfänger dürfte es sich um Datensätze aus so genannten Daten-Leaks¹ handeln, der genaue Ursprung ist meistens nicht zurück verfolgbar.

In diesem Zusammenhang darf auf die Tragweite bei der Preisgabe von Zugangsdaten hingewiesen werden, dass bei der Anmeldung im Internet äußerste Vorsicht geboten ist, mit welchen Zugangsdaten eine solche Anmeldung durchführt wird und wem man seine Daten anvertraut.

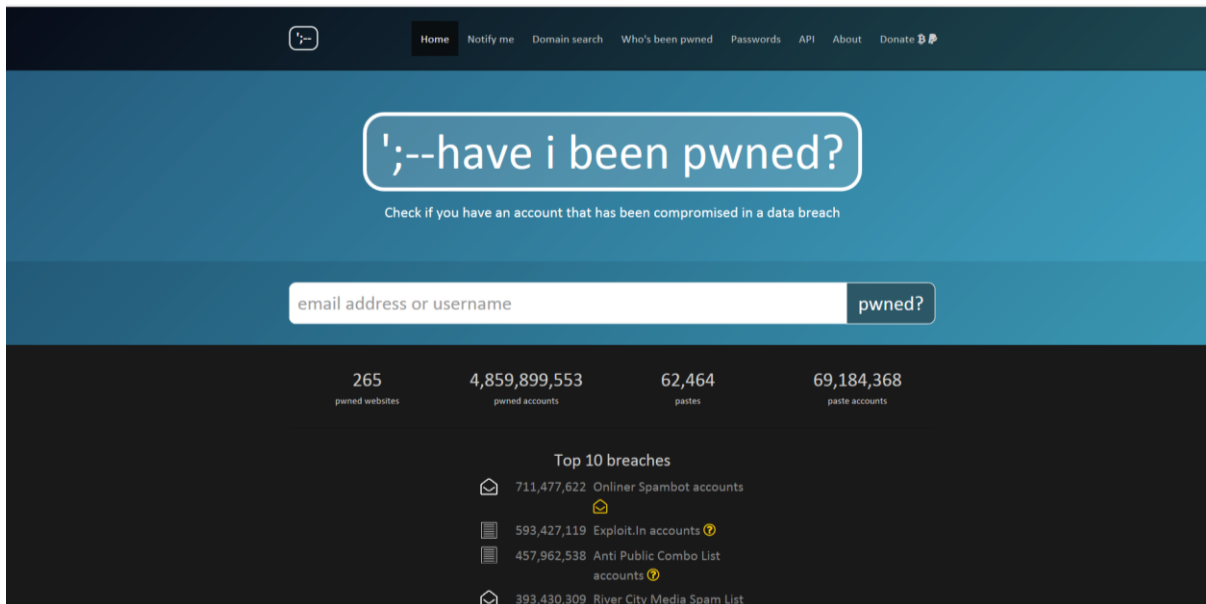
¹ <https://de.wikipedia.org/wiki/Datenpanne>; <https://de.wikipedia.org/wiki/Leak>

Empfohlene Vorgangsweise beim Erhalt einer solchen Erpresser E-Mail:

- Steigen Sie auf Geldforderungen keinesfalls ein und antworten Sie nicht auf die Erpressermail.
- Öffnen sie keine Dateianlagen oder Links bei verdächtigen Emails, weil diese Schadsoftware beinhalten könnten.
- Verschieben Sie verdächtige Emails in den Spam oder Junk-Mail Ordner oder löschen sie diese endgültig mit den Tasten Shift + Entfernen.
- Sollten Sie Webcams und Mikrofone verwenden, so sollten diese und deren Verwendung auch mittels Passwort geschützt sein. Bei (zeitweiser) Nichtverwendung sollten das Mikrofon und Objektiv abgedeckt oder abgeklebt werden, es gibt diesbezüglich wiederverwendbare Lösungen.
- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen.
- Überprüfen Sie in regelmäßigen Abständen, ob Ihre Mail-Adresse(n) und Passwörter unter Umständen kompromittiert sind. Dies können Sie unter anderem auf der Webseite www.botfrei.de, einem kostenlosen Service des eco – Verband der Internetwirtschaft Deutschland, unter der Rubrik Werkzeuge mit den Tools „';--have i been pwned?“ und „HPI Identity Leak Checker“ durchführen.

Möglichkeiten um festzustellen, ob meine E-Mail-Adresse kompromittiert ist:

<https://haveibeenpwned.com/>



The screenshot shows the homepage of the 'Have I Been Pwned' website. The header is dark blue with a navigation menu including 'Home', 'Notify me', 'Domain search', 'Who's been pwned', 'Passwords', 'API', 'About', and 'Donate'. The main content area has a light blue background with a large white rounded rectangle containing the text '';--have i been pwned?'. Below this is a search bar with the placeholder text 'email address or username' and a 'pwned?' button. The footer is dark blue and features four statistics: '265 pwned websites', '4,859,899,553 pwned accounts', '62,464 pastes', and '69,184,368 paste accounts'. Below these is a section titled 'Top 10 breaches' with a list of breaches including '711,477,622 Onliner Spambot accounts', '593,427,119 Exploit.In accounts', '457,962,538 Anti Public Combo List accounts', and '393,430,309 River City Media Spam List'.

<https://sec.hpi.uni-potsdam.de/ilc/search?lang=de/>

HPI Hasso Plattner Institut

Home Statistics FAQ Response E-mails

Is someone spying on you?

Everyday personal data is stolen in criminal cyber attacks. A large part of the stolen information is subsequently made public on Internet databases, where it serves as the starting point for other illegal activities.

With the HPI Identity Leak Checker, it is possible to check whether your e-mail address, along with other personal data (e.g. telephone number, date of birth or address), has been made public on the Internet where it can be misused for malicious purposes.

Please enter your e-mail address here.

The e-mail address you have entered will only be used for searching in our database and, when applicable, to subsequently send an e-mail notification. It will be saved in an obfuscated way to protect you from potential e-mail spam and is never given to a third party.

Check e-mail address!

Our other services and research on IT security

HPI-VDB - Our database for IT attack analysis and self-diagnosis,
tele-TASK - Lectures, not only on IT security,
openHPI - Our interactive online educational program.

... and more about our research in the field of IT security.

Privacy Statement Contact - Disclaimer © Hasso Plattner Institute 2017

Beachten Sie die Sicherheitshinweise und Tipps für einen Sicherem Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: <http://www.bundeskriminalamt.at/praevention>. oder http://www.bundeskriminalamt.at/202/Betrug_verhindern/start.aspx

Weiterführender Link:

Watchlist-Internet: <https://www.watchlist-internet.at/news/erpressung-mit-masturbations-video/>.

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Halaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER
AN-/ABMELDUNG

Hinweis: Die vorliegende Information beruht auf einer Momentaufnahme aus dem Geschehen in der C4-Meldestelle ohne Berücksichtigung allen Falls vorhandener statistischer Daten aus dem Bundesgebiet und dient einem eingeschränkten Empfängerkreis zu Informations- und Präventionszwecken. Der beschriebene Tathergang sowie dazugehörige technische Details wurden im Rahmen der hier vorhandenen Möglichkeiten recherchiert und erheben keinen Anspruch auf Vollständigkeit. Angeführte Web-Links zu weiterführenden Artikeln und Informationen wurden zwar bei der Erstellung des Newsletters auf ihre sachliche und inhaltliche Richtigkeit überprüft, es besteht jedoch keine Haftung für das .BK bei Änderung dieser Inhalte durch Dritte. Medienanfragen sind ausschließlich an die Pressestelle des Bundeskriminalamts zu stellen.