

Gekaperte Dateien entschlüsseln



Das Tool gibt verschlüsselte Dateien wieder frei.

Von Petya, Mischa oder Goldeneye verschlüsselte Daten können mit einem kostenlosen Werkzeug von Malwarebytes wieder entschlüsselt werden. Nachdem die Entwickler der Trojaner vor einigen Wochen die Master-Schlüssel für die Trojaner veröffentlichten, war das fertige Entschlüsselungstool nur noch eine Frage der Zeit.

Betroffene anderer Verschlüsselungstrojaner sollten Festplatten in der Hoffnung auf vergleichbare Tools ausbauen und aufbewahren. Immer wieder finden Sicherheitsforscher Fehler in der Umsetzung von Trojanern, die eine Entschlüsselung ermöglichen. *(jam@ct.de)*

Mischa Decrypter: ct.de/yhun

Schlampige Cloud-Migration

Der schwedischen Regierung drohen ernste Probleme wegen Nachlässigkeiten beim Übertragen von Daten in die Cloud. Die schwedische Verkehrsbehörde und das Militär hatten bereits 2015 damit begonnen, ihre Datenbanken in eine von IBM betreute Cloud auszulagern. Die Rechenzentren befinden sich dabei ausschließlich in Schweden – aus Sicherheits- und Datenschutzgründen. Es wurde allerdings versäumt, die Mitarbeiter von IBM und Subunternehmern aus Tschechien und Rumänien einer Sicherheitsüberprüfung zu unterziehen – aus Zeitgründen. Bereits 2016 wurde der Fall bekannt; die Leiterin der Verkehrsbehörde musste ihren Posten räumen. Ministerpräsident Stefan Löfven sprach von einem „unglaublich ernststen Vorfall“. Jetzt hat der Fall auch politische Bedeutung: Nachdem der Inlands-Nachrichtendienst „Säkerhetspolisen“ den Fall als „größte Gefahr“ für das Königreich bezeichnete, drohen jetzt die Oppositionsparteien mit einem Misstrauensantrag. *(jam@ct.de)*

Hacker-Auftrag für die Hochzeitskasse

Über eine Million Router der Telekom waren außer Gefecht, Internet und EntertainTV damit nicht erreichbar, es entstand ein Schaden von über zwei Millionen Euro. Jetzt stand der Verantwortliche in Köln vor Gericht. Der Brite gab zu, einen Auftrag für einen weltweiten Angriff auf Router über die Fernwartungsprotokolle TR-069 und TR-064 angenommen zu haben. 10.000 US-Dollar seien ihm dafür von einer liberischen Telekommunikationsfirma geboten worden – das Geld habe er für seine Hochzeitskasse verplant. Das Urteil blieb unter den Anträgen der Staatsanwaltschaft und der Verteidigung: Ein Jahr und sechs Monate wurden zur Bewährung ausgesetzt. Großbritannien hat allerdings bereits einen Auslieferungsantrag gestellt. Dort droht dem 27-Jährigen ein weiteres Verfahren.

Ziel war es, die Geräte zu übernehmen, um sie später als Botnetzwerk einzusetzen. Der Angriffsvorversuch wurde für Telekom-Router allerdings zur Denial-of-Service-Attacke, weil die Geräte gegen den geplanten Angriff gar nicht angreifbar waren. Die wiederholten Angriffe führten zu kontinuierlichen Abstürzen der Router. Der Angeklagte bezeichnet sich selbst als Laie, er habe sich das Wissen selbst angeeignet.

(jam@ct.de)

Sicherheitsnotizen

Der Kopf hinter dem Untergrund-Marktplatz **AlphaBay** wurde offenbar wegen seines leichtsinnigen Umgangs mit seiner privaten Hotmail-Adresse vom FBI gefasst. Die Adresse hatte er immer wieder hinterlassen – sie enthielt seinen Vornamen und sein Geburtsjahr.

Betreiber von **Joomla** sollten dringend nach Updates suchen. Version 3.7.4 behebt Sicherheitslücken in der Installationsroutine.

Kaspersky will seinen Gratis-Virenwächter **Kaspersky Free** künftig weltweit anbieten – ab Oktober auch hierzulande. Im Vergleich zum kostenpflichtigen Kaspersky Anti-Virus beschränkt sich die Gratis-Variante auf das Wesentliche – den Schutz vor Schadsoftware.

Wer **Outlook** 2007, 2010, 2013 oder 2016 unter Windows nutzt, sollte sicherstellen, dass die aktuellen als wichtig eingestuft Sicherheitspatches via Windows Update eingespielt sind. In den E-Mail-Komponenten der Outlook-Versionen klaffen drei Sicherheitslücken.

Microsoft erweitert sein Bug-Bounty-Programm um die Insider Preview von **Windows 10** aus dem sogenannten Slow Ring. Das Entdecken einer Sicherheitslücke kann bis zu 15.000 US-Dollar einbringen.