# James Bond lässt grüßen

## Verschlüsselungstrojaner Goldeneye greift gezielt deutsche Personalabteilungen an

**Eine besonders perfide Erpressermasche hat viele Firmen kalt erwischt. Der Trojaner wurde in Phishing-Mails verteilt, die wie plausible Bewerbungen auf tatsächlich offene Stellen aussahen. Die Täter scheinen James-Bond-Fans zu sein.**

**Von Fabian A. Scherschel**

Am 6. Dezember trat ein neuer Verschlüsselungstrojaner auf den Plan, der sich innerhalb von Stunden rasant in Deutschland verbreitete. In den frühen Morgenstunden registrierten Sicherheitsexperten und Admins zum ersten Mal infizierte Excel-Dateien, die per E-Mail in ihren Netzen aufschlugen. Wurden diese geöffnet, begegnete dem potenziellen Opfer ein einigermaßen offiziell aussehendes Dokument mit der Bitte, die Makro-Funktionen des Tabellenkalkulationsprogramms zu aktivieren. Kam der Nutzer der Bitte nach, baute das infizierte Dokument mit Hilfe von VBScript zwei EXE-Dateien mit Schadcode zusammen und führte sie aus. Dann wurden Dateien verschlüsselt und die Originale gelöscht sowie die System-Partition so manipuliert, dass nicht mehr gebootet werden konnte.

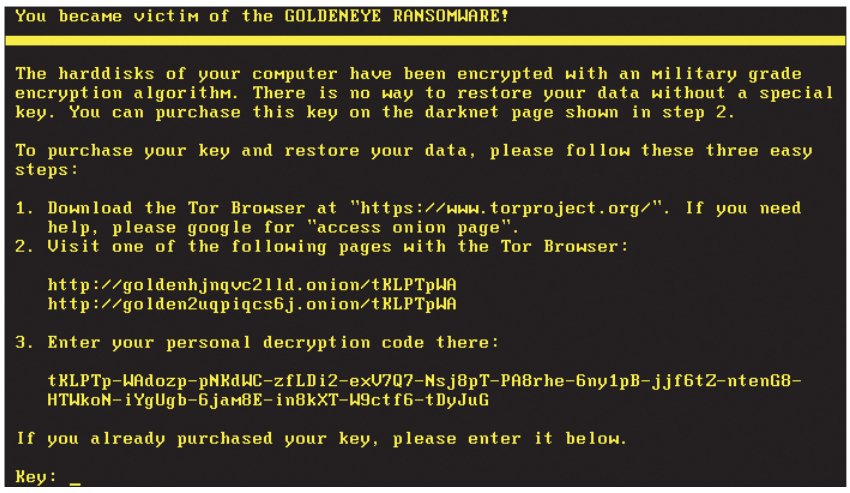
Nach der ersten Warnung vor der neuartigen Ransomware namens Goldeneye auf heise Security erreichten uns hunderte E-Mails von Betroffenen. Viele große Firmen und Institutionen blockierten als Reaktion auf die Bedrohung noch am selben Tag Mail-Anhänge mit Excel-Dokumenten oder gar alle Anhänge. Später zeigte sich, dass die Angriffe fast ausschließlich gegen deutsche Opfer gerichtet waren. Was war passiert?

### Ungewöhnlich perfide

Die Angreifer haben offensichtlich massenweise Mails an personalverantwortliche Mitarbeiter in deutschen Unternehmen und Organisationen verschickt. Dabei handelte es sich um Anschreiben in fehlerfreiem Deutsch, oft mit einer angehängten Bewerbung im PDF-Format und der verseuchten Excel-Datei. Anschreiben und Bewerbung waren fast immer korrekt adressiert und nahmen auf eine tatsächliche Stellenausschreibung des Unternehmens Bezug. Die Schadcode-behaftete Excel-Datei war mit einem Logo der Bundesagentur für Arbeit versehen und gab vor, aktivierte Makros zu benötigen, um Daten über den Bewerber von Servern der Agentur herunterladen zu können.

Vielen Empfängern schienen diese Mails durchaus plausibel, daher verwundert es wohl auch nicht, dass eine beträchtliche Anzahl von Adressaten die Makros in der Excel-Datei aktivierten und so die Goldeneye-Infektion ihren Lauf nahm. Sogar der Absender der Trojaner-Mail war eine real existierende Person; zum Teil wurde sogar deren Adresse und Telefonnummer angegeben. Die Angreifer vermieden mit diesen Tricks viele der Faktoren, über die man normalerweise Phishing-Mails identifizieren kann. Allein bei der Bitte, Makros zu aktivieren, und beim Design des angeblichen Arbeitsamt-Formulars hätte man stutzig werden können.

Was Goldeneye im Weiteren besonders gefährlich machte, waren die äußerst niedrigen Erkennungsraten der gängigen Virenscanner innerhalb des ersten Tages der Angriffe. Zwar wurden die Signaturen der EXE-Dateien relativ schnell an viele Scanner verteilt, die XLS-Datei in den Mail-Anhängen schlüpften dagegen auch Tage später noch durch Signatur-basierte Scans. Das lag daran, dass die Angreifer diese Dateien im Stundentakt veränderten, um ihre Mails weiterhin durch die Mail-Scanner zu den Opfern zu schleusen.




Der Erpressungsbildschirm von Goldeneye. An diesem Punkt ist die Systemplatte bereits nicht mehr bootfähig.

### Boris' Rache

Auffällig an den Infektions-Mails war der Absender: Unsere Recherche ergab schnell, dass es sich um eine real existierende Person handelte, die eine Unternehmensberatungsfirma in der Nähe von Ansbach betreibt. Diese hatte eine Entschlüsselungshilfe für den Erpressungstrojaner Petya und seinen Nachfolger Mischa

angeboten. Bei Petya und Mischa wurde angenommen, dass sie vom selben Autor stammen, und auch Goldeneye wies Ähnlichkeit zu den beiden Trojanern auf.

Der Name ist ganz offensichtlich eine Anspielung auf den James-Bond-Film „GoldenEye“ aus dem Jahr 1995. In diesem Film muss James Bond abtrünnige russische Militärs und ein Verbrechersyndikat stoppen, die den Schlüssel (das sogenannte GoldenEye) zu einer orbitalen EMP-Waffe des russischen Militärs geklaut haben und durch dessen Einsatz reich werden wollen. Diese Waffe besteht aus mit Atomsprengköpfen bestückten Satelliten, die im Orbit gezündet werden und so mittels EMP elektronische Geräte unbrauchbar machen. Die beiden Satelliten im Film heißen Petya und Mischa, und sie werden von einem russischen Hacker-Genie namens Boris kontrolliert. Es deutet also alles drauf hin, dass die drei Trojaner-Varianten von denselben Drahtziehern stammen. Vielleicht sitzen diese in Russland, vielleicht mögen sie aber auch einfach nur Pierce Brosnans Debüt in der Rolle des James Bond.

Ziemlich sicher scheint zu sein, dass die Kriminellen sich am Betreiber der Entschlüsselungsseite rächen wollten. Immerhin hatte dieser versucht, ihnen das Geschäft mit Petya und Mischa zu verderben. Im Gespräch mit c’t erklärte eine Vertreterin der Unternehmensberatungsfirma, am ersten Tag der Infektionen über 500 Anrufe und unzählige Mails bekommen zu haben. Die Firma sei komplett lahmgelegt worden, und man habe Strafanzeige gegen die Drahtzieher hinter der Goldeneye-Kampagne gestellt.

## Daten für die Angriffe stammen von der Arbeitsagentur

Die Daten über die Ansprechpartner bei Firmen und deren offenen Stellen, welche die Angreifer für ihre Phishing-Kampagne verwendet haben, scheinen von der Bundesagentur für Arbeit zu stammen. Zum Teil handelt es sich um E-Mail-Adressen, welche die Firmen ausschließlich zur Kommunikation mit der Bundesagentur verwendet haben. Auch wurde uns von mehreren Stellen versichert, dass in den Mails zum Teil Jobs referenziert wurden, die ausschließlich beim Arbeitsamt ausgeschrieben waren.

Ob tatsächlich ein Datenleck bei der Bundesagentur für Arbeit vorliegt, wissen wir nicht. Auf unsere Anfrage reagierte die Arbeitsagentur lange gar nicht, dann teilte man uns mit, es sei nicht bekannt, dass ein Einbruch in die eigenen Server vorliege. Zu einem etwaigen Datenleck bei einer Drittfirma oder einem externen Dienstleister der Agentur äußerte man sich nicht.

Es ist denkbar, dass die Angreifer aus öffentlich verfügbaren Informationen der Bundesagentur für Arbeit geschöpft haben. In der Vergangenheit wurde dies schon bei anderen Trojaner-Wellen beobachtet. Viele Opfer, die sich mit uns in Verbindung gesetzt haben, vermuten auf Grund von Indizien zwar, dass ein Hack bei der Arbeitsagentur vorliegt, wir haben aber letztlich keine stichfesten Hinweise auf ein Datenleck finden können.

## Was tun, wenn ich infiziert bin?

Wird der Trojaner auf einem System aktiviert, kombiniert er die negativen Eigenschaften der Vorgänger Petya und Mischa. Er verschlüsselt zunächst Daten in den persönlichen Windows-Ordnern des Benutzers. Dann manipuliert er den Bootloader und führt einen Bluescreen herbei, der den Rechner in der Regel zum Neustart zwingt. Dabei bootet dann nicht mehr Windows, sondern ein eigener Kernel der Ransomware, der einen Chkdsk-Bildschirm vortäuscht. Im Hintergrund zerstört der Schadcode den Bootsektor und weitere wichtige Teile der Systemplatte, sodass ein Zugriff auf deren Partitionen nicht mehr möglich ist.

Unseren Tests nach zu urteilen wird die Platte dabei nicht vollständig verschlüsselt. Die Windows-Installation und Daten, die der Trojaner im ersten Schritt nicht verschlüsselt hat, lassen sich also eventuell mit Forensik- und Systemrettungs-Tools wiederherstellen. Die Systempartition ist aus einem gebooteten Rescue-System zwar immer noch sichtbar, sie lässt sich aber nicht ohne weiteres reparieren. Auf Blockebene konnten wir allerdings nach wie vor Daten auslesen.

Hat es das Opfer geschafft, nach der Aktivierung des Trojaners das System auszuschalten, bevor Goldeneye im zweiten Schritt der Infektion den Bootloader und den Bootsektor der Platte beeinträchtigt, lässt sich die Festplatte ohne Probleme in ein anderes System umbauen und dort als Datenplatte ansprechen. So können unverschlüsselte Daten gerettet werden. Für die im ersten Schritt verschlüsselten Dateien war bis Redaktionsschluss allerdings noch keine Rettung bekannt. Da hilft es nur, die Platte beiseite zu legen und darauf zu hoffen, dass die Goldeneye-Verschlüsselung in Zukunft geknackt wird.

### Verschlüsselungstrojaner?

Seit Anfang des Jahres boomen Verschlüsselungstrojaner geradezu. Eine Welle nach der anderen bricht per Phishing-Mail oder Drive-By-Infektion über Windows-Anwender herein. Das liegt vor allem am finanziellen Erfolg der Kriminellen: Ransomware ist längst ein Millionengeschäft.

Im Vergleich zum Betrug mit Banking-Trojanern und dem Handel mit abgephischten persönlichen Daten brauchen die Erpresser viel weniger Infrastruktur. Haben sie ihr Opfer einmal infiziert, läuft alles automatisch ab. Das Opfer bezahlt und bekommt, im besten Fall, seinen Entschlüsselungscode. Die Kriminellen brauchen also nur den Schadcode und einen verdeckten Server, um die Bezahlung entgegenzunehmen. Es gibt keine Mittelsmänner. Die Kryptowährung Bitcoin und Hidden Services im Anonymisierungsnetz Tor sorgen dafür, dass die Täter nur schwer enttarnt werden können.

Anfänglich begingen die Kriminellen immer wieder Fehler bei der Implementation ihrer Verschlüsselungssysteme, aber auch solche Lichtblicke werden immer seltener. In Zeiten, wo die Trojaner oft einfach die Krypto-Infrastruktur von Windows nutzen oder sich quelloffene Bibliotheken zu eigen machen, ist ihrer Verschlüsselung immer seltener etwas anzuhaben.

Grundsätzlich hilft gegen Verschlüsselungstrojaner nur eins verlässlich: Regelmäßige Backups! Zusätzlich sollte man einen Virenwächter laufen haben, der ordnungsgemäß mit Updates versorgt wird. Aber wie der Fall Goldeneye deutlich zeigt, nützt das manchmal einfach nichts.

Wer darüber nachdenkt, auf die Forderungen der Erpresser einzugehen, muss sich darüber im Klaren sein, dass er mit seiner Zahlung das Geschäftsmodell der Virenschreiber unterstützt. Je mehr Opfer zahlen, desto mehr Verschlüsselungstrojaner wird es in Zukunft geben. Außerdem zeigen die Erfahrungsberichte von Opfern, die bereit waren zu zahlen, dass ihre Daten mit dem Entschlüsselungscode von den Erpressern nicht immer korrekt entschlüsselt werden. In manchen Fällen scheint der Entschlüsselungsalgorithmus der Malware gar nicht zu funktionieren. *(fab@ct.de)* c't