RANSOMWARE TROJANER VIRUS – WAS STECKT HINTER LOCKY, WANNACRY & CO.

Veröffentlicht am 6. Juni 2017 von Judith

Immer wieder kommt es zu Schlagzeilen über die neueste Version eines Verschlüsselungstrojaners, der sich im Internet ausbreitet. WannaCry, Locky oder der GVU-Trojaner sind die bekanntesten Beispiele. Was genau Ransomware auf Eurem Computer ausrichtet, wie die Erpresser vorgehen und wie ihr Euch schützen könnt, erfahrt ihr im folgenden Blogbeitrag.

WAS IST RANSOMWARE? – KURZ & KNAPP FÜR EILIGE

Ransomware ist eine spezielle Form von Computer Virus. Diese Malware, auch Verschlüsselungstrojaner, Lösegeld Trojaner oder Krypto Trojaner, verschlüsselt die Dateien & Daten auf dem infizierten Computer und fordert ein Lösegeld für die Freigabe und Entschlüsselung.

HILFE – ICH WERDE ERPRESST!

Während dieses Szenario für die meisten von uns zum Glück eher Bestandteil des abendlichen Krimiprogramms ist, steht man in der virtuellen Welt immer häufiger vor genau diesem Problem. Sogenannte Ransomware, auch Verschlüsselungstrojaner genannt, schaffen es mit Hilfe von schädlichen Links, E-Mail Anhängen, oder Exploit Kits, den Computer zu infizieren und alle vorhandenen Daten zu verschlüsseln.

Wenn der PC einmal mit **Ransomware** infiziert ist, kann die Malware Dateien, Ordner oder im schlimmsten Fall, die ganze Festplatte sperren, sodass der Zugriff auf alle Bilder, Videos und Nachrichten verhindert wird. Die Ransomware ist eine bestimmte Form der Malware, zu Deutsch **Schadprogramm**, die Daten erst wieder freigibt, wenn die Geschädigten bereit sind, einen gewissen

Lösegeld-Betrag (vom engl. ransom für Lösegeld) zu bezahlen. Die beliebteste Zahlungsmethode der Erpresser heißt Bitcoins, da diese Art der Zahlungsmethode kaum zurück zu verfolgen ist.

WIE FUNKTIONIEREN BITCOINS?

Unter **Bitcoins** versteht man ein **dezentrales Zahlungssystem,** welches mit Hilfe von kryptographischen Techniken sicherstellt, dass Transaktionen nur vom Kontoinhaber selbst durchgeführt werden können. Überweisungen werden beispielsweise über einen Zusammenschluss von Rechnern über das Internet abgewickelt. So wird verhindert, dass virtuelles Geld mehrfach ausgegeben wird. Auch erschwert die Benutzung von Bitcoins die Verfolgung von getätigten Geldtransaktionen, da die Nutzung von Bitcoins den Usern völlige **Anonymität** zugesteht. Bitcoins sind demnach die perfekte Lösung, um ein Lösegeld für Ransomware einzufordern.

WIE WIRD MAN ZUM OPFER VON RANSOMWARE?

Leider haben es die Täter recht einfach, sich Zugriff zu einem Rechner zu verschaffen. Durch sogenannte **„Drive-by-Infektionen“** gelingt es den Erpressern, Ransomware auf den Computer zu spielen. Wenn der Rechner keinen **Antivirenschutz** installiert hat und demnach nicht ausreichend geschützt ist, können sich PCs durch das alleinige Aufrufen einer **manipulierten Website** mit Ransomware infizieren.

Ein weiterer Risikofaktor sind **Exploit Kits**. Mit Exploit Kits könnt ihr beispielsweise dann in Berührung kommen, wenn ihr eine **infizierte Website** aufruft, eine infizierte Werbeanzeige auf einer ansonsten virenfreien Website anklickt oder ihr zu einer schädlichen Website weitergeleitet werdet. Das große Gefahrenpotenzial der Exploit Kits liegt darin, dass sie gezielt die **Schwachstellen** des Computers angreifen. Sobald das Exploit Kit einen Angriffspunkt findet, lädt es die Ransomware herunter und installiert sie auf dem Computer. Exploit Kits stellen sich als besonders gefährlich heraus, da die Nutzer des Computers die Installierung der Ransomware erst bemerken, wenn es bereits zu spät ist und der PC infiziert wurde.

Opfer von Ransomware kann auch jeder werden, der unbekannte E-Mail Anhänge öffnet, Filesharing von Dateien betreibt oder präparierte Facebook-Links anklickt.
Besonders das Verschicken von **Facebook-Links** wird bei Hackern aktuell immer beliebter, um Ransomware zu verbreiten. Hierbei werden potenzielle Opfer mit sogenannten **Clickbaits** geködert. So kann es sein, dass man von einem Facebook-Freund eine Nachricht erhält „Bist Du das auf dem Bild?“ oder „OMG, guck Dir dieses krasse Video an“. Diese Nachrichten werden unwissentlich versendet. Durch einen Hacker oder eine Schadsoftware wurde sich in diesem Fall Zugang zu einem Profil verschafft. Der Benachrichtigte fällt dann womöglich, durch den bekannten und vertrauten Absender in die **Virusfalle**, indem er den Link anklickt.

DIE HÄUFIGSTEN VERSCHLÜSSELUNGSTROJANER

GVU Trojaner
Wenn der Rechner von einem GVU Trojaner infiziert wurde, wird dem Nutzer vorgeworfen, durch **illegale Raubkopien** das Urheberrecht verletzt zu haben. Unter dem Deckmantel offizieller Behörden, wie zum Beispiel des BKA (Bundeskriminalamt), der GEMA (Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte) oder eben der GVU (Gesellschaft zur Verfolgung von **Urheberrechtsverletzungen**), sollen PC-Nutzer eingeschüchtert und zur schnellen Zahlung erpresst werden.
Ein Sperrbildschirm macht den Nutzer auf Ransomware aufmerksam. Anhand einer Überweisung von 12 bis 100 € via Bitcoin, kann der Nutzer, laut Virus, die Sperre aufheben, sofern man den geforderten Betrag innerhalb von 48 Stunden überweist. Wenn dies nicht passiert, droht Ransomware mit einem angeblichem **Strafverfahren**.

BKA Trojaner
Bei Befall von BKA Ransomware wird der Computer gesperrt. Auf dem Bildschirm erscheint eine Meldung die den Nutzer beschuldigt auf dem Rechner ungesetzliches Material, wie zum Beispiel **Kinderpornografie**, gespeichert zu haben. Die Warnhinweise enthalten oftmals die Worte „Es ist die ungesetzliche Tätigkeit enthüllt!“ oder „Die offizielle Mitteilung des Bundeskriminalamtes“.
Falls der Computer von BKA Ransomware befallen ist, sollen hier die Betroffenen durchschnittlich 100 bis 500 € überweisen, um ihren Computer vermeintlich wieder entsperren zu können. Wenn die Zahlung nicht innerhalb von 24 Stunden erfolgt, droht die Ransomware die **komplette Festplatte zu formatieren.** Sollte der infizierte Rechner zusätzlich mit dem Internet verbunden sein, erscheinen im Nachrichtenfenster Angaben zu der momentan genutzten IP-Adresse, dem Internetserviceprovider und dem ungefähren Standort. Das Ziel von Ransomware ist es den Nutzer so sehr einzuschüchtern, dass er aus Angst vor weiteren Konsequenzen den geforderten Betrag schnellstmöglich zahlt.

WannaCry Trojaner
Vor Malware WannaCry müssen sich in erster Linie **Microsoft-User** fürchten, die Geräte benutzen, die den von Microsoft angebotenen Sicherheitspatch nicht mehr enthalten. Wenn die Ransomware den Computer einmal befallen hat, verschlüsselt der Virus bestimmte **Benutzerdateien** und droht bei nicht bezahlter Lösegeldforderung mit **Datenverlust.** Besonders großen Schaden richtete WannaCry in Unternehmen an, da der Verschlüsselungstrojaner auch als **Computerwurm** fungiert. So hat der Virus die Möglichkeit, sich über das Netzwerk auf weitere Rechner innerhalb einer Firma auszubreiten. Durch die Nutzung der Schnittstelle SMBv1, die unter vielen Windows-Versionen zur Datei- und Druckerfreigabe im Netz benötigt wird, kann sich die Ransomware WannaCry in weitere Computersysteme einhacken. Das heißt, WannaCry nutzt diese **Sicherheitslücke** und infizierte Windowsrechner werden dazu gebracht, beliebige WannaCry Codes auszuführen. Oftmals wird dabei **„DoublePulsar“** installiert. Dabei handelt es sich um eine „Backdoor“, die es WannaCry ermöglicht auf **mehrere Übertragungswege** zurückzugreifen. So kann WannaCry anhand von Mails mit kompromittierenden Anhängen oder Links den Nutzer auf infizierte Websites locken. Eine der gefährlichen Eigenschaften dieser Ransomware ist, dass sich die Malware als **Selbstläufer**

entpuppt. Ohne weiteres Zutun des Nutzers sucht WannaCry nach weiteren Rechnern im gleichen lokalen Netzwerk und versucht sie zu infizieren. Außerdem sendet der Virus zahlreiche IP-Anfragen ins Internet, um auch darüber nicht geschützte Rechner anzustecken.

Locky Trojaner
Locky ist eine Malware, die **Microsoft und Mac OS** Nutzer gleichermaßen angreift. Der Verschlüsselungstrojaner infiziert nicht ausreichend gesicherte Rechner und verschlüsselt ausschließlich **Nutzerdaten**. Einen besonderen Wiedererkennungswert hat die Ransomware, da nachdem die Dateien von Locky befallen sind, alle Files auf .locky enden. Um sich von Locky wieder zu befreien, fordern die Erpresser ein Lösegeld, in Höhe von ca. 200 €. Nach Bezahlung des Lösegelds kann sich das Opfer über diverse Internetadressen sowie einem Tor-Netzwerk-Zugang zu einer Software namens **Locky Decryptor** zum Entschlüsseln der Dateien kaufen. Allerdings stehen die Chancen zur Entschlüsselung der Dateien nach Erwerbs des Programms reichlich schlecht. Locky verbreitet sich über Rechnungen und gepackte JavaScript Dateien im Anhang von E-Mails oder durch E-Mails, die den Anschein erwecken, als wären sie von einem Scanner mit Mail-Funktion verschickt worden.

Dridex
Die Ransomware Dridex versteckt sich meist in E-Mails aus Vietnam, Taiwan, Südkorea, China oder Indien und ist größtenteils gefährlich für **Microsoft-User**. Nachdem der Anhang einer E-Mail geöffnet wurde, fängt der darin enthaltene **Makro-Code** an, die eigentliche Malware von bestimmten Webseiten auf den Computer herunterzuladen, um dann den Krypto Trojaner zu starten. Da Microsoft Makros durchgehend deaktiviert hat, um Ransomware zu umgehen, bittet der Virus den PC-Nutzer Makros in Microsoft Word zu aktivieren. Wenn das vermeintliche Opfer dies tut, hat Dridex die Möglichkeit weitere schädliche Malware herunterzuladen. Dridex ist besonders gefährlich, wenn ihr **Onlinebanking** nutzt. Sobald ihr Euch in Eurem Onlinebanking Portal einloggt, kreiert der Trojaner eine zusätzliche in HTML-Code programmierte Website, die den User bittet, weitere Daten preiszugeben.

(Quelle: https://www.youtube.com/watch?v=80nIdaQrq9I&start=92&autoplay=1 Stand: 02.06.2017)

WAS TUN, WENN RANSOMWARE DEN RECHNER BEFALLEN HAT?

Ganz wichtig ist, dass ihr **NICHT einfach so** auf die Lösegeldforderung eingeht. In der Vergangenheit hat sich gezeigt, das Opfer, die Ransomware gezahlt haben, nach wie vor vor einem verschlüsselten Rechner saßen. Die Polizei rät, den Bildschirm zu fotografieren und **Anzeige** zu erstatten. Sucht Euch am besten Rat bei der Polizei, wir können Euch lediglich Tipps geben. Je nach Trojaner hilft eine **Notfall CD**, die die Malware wieder entfernt, die Nutzung der Funktion **„Systemwiederherstellung“** von Windows, eine **manuelle Bereinigung** (GVU Trojaner) oder im Fall Dridex, die Unterlassung von Makro Ausführungen in Microsoft-Word. In ganz schwerwiegenden Fällen hilft leider nur noch ein **komplettes neu Aufsetzen** des Rechners, mit anschließendem Aufspielen eines **Daten-Backups.**

WIE KANN ICH MICH VOR RANSOMWARE SCHÜTZEN?

Um Malware zu vermeiden, empfehlen wir Euch unsere Security Experten der Media Company zunächst einmal einen **leistungsstarken Antivirenschutz**. So macht ihr es der Ransomware so schwer wie möglich, Euren PC überhaupt infizieren zu können. Auch helfen regelmäßige **Backups** um sicherzustellen, dass, auch wenn der Rechner von einem Trojaner befallen ist, Eure Fotos, Videos, die Arbeit der letzten Monate und alles was Euch wichtig ist, sicher aufbewahrt wird. Um unsere Rechner vor Malware zu schützen, haben wir unseren Partner IT-ON-NET an der Seite. Wenn es um **Virenschutz** bei E-Mails geht, solltet ihr auf Software von Sicherheitsexperten setzen. Unsere Mailserver schützen wir beispielsweise mit **Hornetsecurity** vor Phishing E-Mails und DdoS-Angriffen. Bis zu 99,9% Spam und Virenangriffe werden so gefiltert und verhindert. Verdächtige Mails werden in einer virtuell abgeschlossen Umgebung getrennt vom Server geöffnet und erst weitergeleitet, wenn sie sich als unauffällig erweisen. So erreicht ihr wirklich das **Maximum an Schutz** vor Spam und Ransomware.
Wenn ihr weitere Fragen habt zum Thema Hornetsecurity, Ransomware, Malware oder ihr auf der Suche nach einem Partner seid, der die Sicherung der Daten Eurer Webseite, Eures Online-Shops oder Eurer Firmenmails übernimmt, dann meldet Euch bei uns oder hinterlasst einen Kommentar – Team Webweisend der Media Company hilft Euch gerne weiter!