30.10.2023 – 14:01 Uhr

Halloware - die Malware aus der Hölle

Jena (ots) -

Die Nächte werden länger und bald schon wird man überall Zombies, Gespenster und Vampire durch Straßen und Gassen streifen sehen. Halloween ist auch in Deutschland innerhalb der letzten Jahre beliebter geworden. Der Grusel beschränkt sich nicht nur auf die physische Welt: Auch im virtuellen Raum gibt es allerhand schaurige Wesen und Phänomene, die sich scheinbar nicht erklären lassen. ESET erzählt heute eine Geschichte, wie sie jeden Tag vorkommen kann - und die Internetnutzern das Blut in den Adern gefrieren lässt.

Wer von Halloween nicht genug bekommen kann, findet im neuen Blogpost auf WeLiveSecurity weitere schaurige Zahlen und Fakten zur Cybersecurity - Gänsehaut garantiert.

Post für Dich

Alles begann mit einer einfachen E-Mail: Jonas, ein Computer-Nerd, saß wie so häufig vor seinem PC. "Neue Mail", teilte sein Thunderbird ihm mit, der Betreff: "Halloween-Horror-Gewinnspiel". Neugierig, was es wohl zu gewinnen gab, öffnete er die Nachricht.

Die E-Mail enthielt eine Einladung zu einem Online-Gewinnspiel namens "Halloween-Challenge". Das Konzept klang faszinierend und unheimlich zugleich: Die Teilnehmer wurden aufgefordert, verschiedene knifflige Horror-Rätsel zu lösen, um am Ende des Wettbewerbs einen Preis zu gewinnen. Jonas konnte sich bereits vorstellen, wie er den grandiosen Hauptpreis, einen schwarz verzierten Computer mit Kürbis-Design, in sein Zimmer stellen würde. Natürlich nahm er teil.

"Ich möchte ein Spiel spielen"

Die Regeln der Challenge waren einfach: Jeden Tag erhielt er eine neue E-Mail mit einem Rätsel, das er innerhalb von 24 Stunden lösen musste. Die Rätsel waren harmlos und drehten sich um klassische Halloween-Themen wie Geistergeschichten und Horrorfilme: "Wie hieß die Hauptfigur in 'Nightmare on Elmstreet?'" und "Wie nennt man Untote noch?". Auch Suchbilder in Form von PDF-Dokumenten musste er lösen. Bei Erfolg durfte er weiter machen und sich als Teil der nächsten Aufgabe ein kleines Puzzle-Spiel installieren.

Eines Abends als Jonas ein besonders schwieriges Puzzle zu lösen versuchte, begann der Albtraum: Der Bildschirm flackerte in gruseligen Mustern und aus den Lautsprechern ertönten mysteriöse Geräusche. Von einem normalen Software-Fehler ausgehend, tat Jonas das, was jeder in diesem Moment getan hätte: Er schaltete seinen Rechner aus und wieder ein.

Sie sind hier

Die Festplatten summten vor sich hin, als Jonas seinen Rechner wieder hochfuhr. "Nur ein Bug", redete er sich ein. Doch es war kein Bug: Dutzende Male versuchte der immer panischer werdende Computer-Nerd, auf seine Bilder und Dokumente zuzugreifen. Das Ergebnis war immer dasselbe: Zugang verweigert. Nur sein Mail-Programm und der Internet-Browser funktionierten noch. "Neue Mail", poppte es auf seinem Bildschirm auf.

"Komm und spiel mit uns, Jonny. Gewinne alle Challenges und Deine Daten überleben. Du hast 24 Stunden Zeit. Viel Glück." Es folgte ein Link zum nächsten Rätsel.

"Wir alle werden manchmal ein bisschen verrückt"

Der Gedanke an all die Daten, die verloren gehen würden, schnürte Jonas die Kehle und ließ ihn zittern. Doch dann fiel ihm ein, dass seine gute Freundin Marion IT-Security-Spezialistin war. Er rief sie an und schilderte ihr die Situation. Sofort fuhr sie zu ihm und analysierte seinen Computer. Ihre Untersuchung bestätigte ihren Anfangsverdacht: Jonas hatte seinen Computer mit der Halloware infiziert, einer hochentwickelten Ransomware, die sich auf die Manipulation der Daten eines Opfers spezialisiert hat. Sie verbreitete sich in der Regel über schädliche E-Mail-Anhänge, zum Beispiel PDFs und Programme, die gezielt darauf abzielen, Opfer in die "Halloware Challenge" zu locken. Die Malware ging dabei immer gleich vor:

- **Infektion**: Die Malware wird durch infizierte Dateianhänge oder Downloads aktiviert. Nach der Aktivierung verschafft sich Halloware Zugriff auf das Opfersystem. Aktiv wird sie aber erst nach einigen Tagen.
- **Verschlüsselung**: Halloware verwendet eine starke Kryptografie, um die Dateien auf dem Opfersystem zu

kodieren.
- **Rätsel** und Countdown: Nach der Verschlüsselung präsentiert Halloware dem Opfer eine weitere Reihe von Rätseln und Herausforderungen, die gelöst werden müssen, um den privaten Entschlüsselungsschlüssel zu erhalten. Ein Countdown erzeugt zusätzlichen Druck, da das Opfer eine begrenzte Zeit hat, um die Rätsel zu lösen.
- **Kommunikation mit den Drahtziehern**: Die Malware setzt verschlüsselte Kommunikationskanäle zu den Drahtziehern auf, die in der Regel anonym bleiben. Die Drahtzieher senden Anweisungen und drängen das Opfer, die Rätsel zu lösen und den "Challenge" fortzusetzen. Wurden alle Rätsel gelöst, bleiben die Daten allerdings verschlüsselt. Nur gegen Bezahlung erhalten Opfer wieder Zugriff.

Die schlechte Nachricht für Jonas: Marion konnte die Verschlüsselung der Daten nicht rückgängig machen. Die Gute: Sie kannte die Neugier und Sorglosigkeit ihres Freundes und hatte ihm zuvor ein regelmäßiges Back-up eingerichtet. Somit konnte sie seinen Computer ohne nennenswerte Datenverluste neu aufsetzen. Was bei Jonas übrig blieb, war ein gehöriger Schrecken - und die Gewissheit, dass er nie wieder an solch einer Challenge teilnehmen würde.

Reale Gefahren

In der echten Welt treten solche Attacken häufig auf. Allerdings gehen Cyberkriminelle hier deutlich direkter vor. Sie wollen selten, dass ihr Opfer einfach nur Fragen beantwortet und Puzzles löst: Ein Klick auf einen Mail-Anhang und schon sind die eigenen Daten verschlüsselt. Der einzige Ausweg, um an seine Daten zurückzukommen ist, ein Lösegeld zu zahlen.

Um vor solchen Gefahren sicher zu sein, empfiehlt sich eine Grundskepsis bei allen Mails, die zu Gewinnspielen, Challenges usw. einladen. Sobald eine Mail zum Download einer ausführbaren Datei auffordert, ist höchste Vorsicht geboten. Regelmäßige Back-ups sorgen dafür, dass die Datenverluste im Ernstfall im Rahmen bleiben. Noch sicherer sind Nutzer, die eine aktuelle IT-Sicherheitslösung wie ESET Smart Security Premium nutzen.

Weitere Informationen, wie sich Nutzer vor den Gefahren im Internet schützen können, gibt es auf unserem Blog WeLiveSecurity.

Pressekontakt:

ESET Deutschland GmbH

Christian Lueg
Head of Communication & PR DACH
+49 (0)3641 3114-269
christian.lueg@eset.de

Michael Klatte
PR Manager DACH
+49 (0)3641 3114-257
Michael.klatte@eset.de

Philipp Plum
PR Manager DACH
+49 (0)3641 3114-141
Philipp.plum@eset.de

Folgen Sie ESET:
http://www.ESET.de

ESET Deutschland GmbH, Spitzweidenweg 32, 07743 Jena, Deutschland