Was versteht man unter den Begriff Trojanisches Pferd?

Zu den schwerwiegendsten und gefährlichsten Bedrohungen, gehört das Trojanische Pferd. Sie wird durch eine ausführbare Datei im Windows-Betriebssystem mit verschiedenen spezifischen Eigenschaften dargestellt.

Von allen Arten von Angriffen ist der Trojaner die beliebteste und am weiteste verbreitete Form des Angriffs auf Computer. Der Name deutet darauf hin, dass es die Fähigkeit hat, den Benutzer zu täuschen, dass das verwendete Computerprogramm eine vom Benutzer autorisierte Aktion ausführt, obwohl es tatsächlich dazu bestimmt ist, das System zu manipulieren.

Wie bereits erwähnt, ist das Trojanische Pferd eine ausführbare Datei und kann daher nicht ohne die vorherige Genehmigung des Benutzers des Systems ausgeführt werden. Damit eine Erlaubnis erteilt werden kann, muss diese dem Opfer als legitime Software erscheinen. Sobald der Benutzer die ausführbare Datei startet hat, erhält der Hacker Fernzugriff auf das System.

Abhängig von der schädigenden Wirkung können Trojanische Pferde in fünf Kategorien eingeteilt werden:

1. Trojaner mit Fernzugriff: Bietet dem Angreifer unbegrenzten Zugriff auf das System, so dass er auf private Daten, personenbezogene Daten sowie geistiges Eigentum zugreifen, diese ändern, vernichten und stehlen kann.

2. Daten sendender Trojaner: wurde entwickelt, um sensible Daten wie Finanzinformationen, spezifische Kontoinformationen, Bankverbindung und vieles mehr an den Hacker zu senden.

3. Zerstörerischer Trojaner: wird mit der Absicht erstellt, bestimmte Dateien aus dem System zu zerstören und ist auch für Antivirenanwendungen nicht erkennbar.

4. Security Software Disabler Trojaner: hat den Zweck, das System anfällig zu machen, indem es alle Sicherheitsdienste wie Firewalls und Antiviren auf dem angegriffenen System deaktiviert.

5. Denial-of-Service-Angriff Trojaner: soll das System beschäftigt halten, so dass keine Benutzeranforderungen ausgeführt werden können.

Wie kann man einen solchen Angriff rechtzeitig erkennen?

Die gebräuchlichste Methode, eine bösartige Software zu erkennen, ist die Verwendung von Antivirenanwendungen, die sich jedoch aufgrund der Polymorphie-Eigenschaft als ineffizient erwiesen haben, wenn es darum geht, Trojanische Pferde zu erkennen.

Da diese Dateien dazu bestimmt sind, zu täuschen, ist es schwierig, zwischen bösartigen und legitimen Dateien zu unterscheiden. Auch das Sammeln der Signatur aller Trojanischen Pferde und deren Aktualisierung in einem Verzeichnis ist nicht nur unüberschaubar, sondern aufgrund der Tatsache, dass täglich neue entwickelt werden, weitgehend unmöglich.

Es ist wichtig zu beachten, dass diese schädlichen ausführbaren Dateien bestimmte Eigenschaften besitzen, die es uns ermöglichen, sie von den legitimen zu unterscheiden.

Eine effizientere Methode zur Erkennung infizierter Dateien besteht nicht in der Verwendung von Signaturen, sondern darin, verdächtige Prozesse und Programme aufgrund ihrer Eigenschaften und ihres Verhaltens zu isolieren.

Programme wie ‚Wireshark’ können verwendet werden, um die Aktivitäten und Prozesse im System zu überwachen und uns benachrichtigen zu lassen, wenn eine ausländische Aktivität/Prozess stattfindet.

Wie kann man sich davor schützen?