NACHRICHTEN AG

30. Januar 2021

Die Emotet-Gefahr wurde noch nicht abgewendet

Wahrscheinlich hat sich keine andere Malware schneller verbreitet und in den letzten Jahren mehr Schaden angerichtet als Emotet. Das Erfolgsgeheimnis bestand beispielsweise darin, sich in bestehende E-Mail-Gespräche einzubinden. Die neuen Opfer glaubten dann, sie hätten Post von einem bekannten Kontakt erhalten und infizierte Anhänge oder gefährliche Links in gutem Glauben geöffnet. Danach hatten die Cyberkriminellen freie Hand. Sie könnten Passwörter stehlen, Online-Banking nutzen, den entführten Computer in ein Bot-Netzwerk integrieren oder Daten verschlüsseln, um Lösegeld zu erpressen. Der Zugang zu infizierten Computern wurde oft tatsächlich an andere Kriminelle verkauft. Emotet ist nutzlos In den letzten Januartagen hat eine internationale Gruppe …

Wahrscheinlich hat sich keine andere Malware schneller verbreitet und in den letzten Jahren mehr Schaden angerichtet als Emotet. Das Erfolgsgeheimnis bestand beispielsweise darin, sich in bestehende E-Mail-Gespräche einzubinden.

Die neuen Opfer glaubten dann, sie hätten Post von einem bekannten Kontakt erhalten und infizierte Anhänge oder gefährliche Links in gutem Glauben geöffnet. Danach hatten die Cyberkriminellen freie Hand.

Sie könnten Passwörter stehlen, Online-Banking nutzen, den entführten Computer in ein Bot-Netzwerk integrieren oder Daten verschlüsseln, um Lösegeld zu erpressen. Der Zugang zu infizierten Computern wurde oft tatsächlich an andere Kriminelle

verkauft.

Emotet ist nutzlos

In den letzten Januartagen hat eine internationale Gruppe von Ermittlern die Infrastruktur hinter Emotet zerstört und den Trojaner unter Kontrolle gebracht. Nach Angaben des Bundeskriminalamtes könnte die Malware auf vielen Computern für die Täter unbrauchbar gemacht werden.

Die IP-Adressen der betroffenen PCs werden an das Bundesamt für Informationssicherheit (BSI) gesendet, das sie wiederum an den zuständigen Internetprovider weiterleitet. Diese sollten dann ihre betroffenen Kunden informieren.

Da dies in den allermeisten Fällen per E-Mail erfolgt, warnt die Verbraucherberatungsstelle Nordrhein-Westfalen, dass andere Cyberkriminelle diese Tatsache für Phishing-Angriffe nutzen könnten.

Emotet-Benachrichtigungen können Phishing sein

Sie können also gefälschte E-Mails verwenden, um den Eindruck zu erwecken, dass Sie eine Emotet-Benachrichtigung von Ihrem Internetprovider erhalten haben – und so den Empfänger dazu verleiten, auf einen Link zu klicken und vertrauliche Daten offenzulegen. Es ist jedoch auch möglich, dass die nächste Malware-Bedrohung in einem Anhang wartet, der geöffnet werden soll.

Wenn sich eine solche E-Mail in der Mailbox befindet, sollten Sie zunächst herausfinden, ob sie wirklich vom Anbieter stammt, und die Verbrauchervertreter beraten. Normalerweise senden Kriminelle die gefälschten E-Mails von Adressen, die nichts mit dem betreffenden Unternehmen zu tun haben. Wenn Sie sich nicht sicher sind, sollten Sie sich direkt beim Internetprovider erkundigen, ob und von welcher Adresse die Nachricht gesendet wurde.

Emotet ist viel Arbeit

Und was machen Sie, wenn Sie Emotet wirklich auf Ihrem Computer haben? Das BSI empfiehlt den Betroffenen, alle auf den infizierten Computern gespeicherten Kennwörter zu ändern, z. B. in Browsern.

Darüber hinaus empfiehlt die Behörde den Betroffenen, ihren Computer erneut einzurichten. Emotet und möglicherweise andere heruntergeladene Malware führten manchmal tiefgreifende und sicherheitsrelevante Änderungen am System durch. Die einzige Möglichkeit, absolut sicher zu sein, dass keine schädlichen Überreste mehr auf der Festplatte vorhanden sind, besteht darin, das Betriebssystem neu zu installieren.

Die niederländische Polizei hat außerdem eine Emotet-Abfrage für E-Mail-Adressen eingerichtet. Dort können Sie überprüfen, ob Ihre eigene Adresse in den Datensätzen mit gestohlenen Benutzernamen und Passwörtern erscheint, die vor den Cyberkriminellen geschützt wurden.

dpa

.

Inspiriert vom LVZ Newsticker -> Zum kompletten Artikel

Details