integrated solutions IT-CleverNet
IT-CleverNet GmbH
Gehrenweg 2
5103 Möriken
Fon: 062 897 49 59
Fax: 062 897 49 55
it@itclevernet.ch
www.itclevernet.ch

E-Mail mit Erpressungs-Trojaner «GandCrab» zirkuliert

E-Mails mit einer angeblichen Bewerbung auf eine ausgeschriebene Stelle sind verschickt worden. Öffnet man den Anhang, werden die Daten verschlüsselt.

Vor wenigen Tagen wurden E-Mails mit der Ransomware **«GandCrab»** in einer gross angelegten Spamaktion zugestellt. Es handelt sich beim Inhalt um eine angebliche Bewerbung auf eine ausgeschriebene Stelle. Wie Heise Online berichtet, sind die Daten verschlüsselt und mit der Dateiendung **.krab** versehen, wenn GandCrab zugeschlagen hat.
Bei Datarecovery in Leipzig haben sich allein in der letzten Woche über 50 Firmen gemeldet, deren Daten unfreiwillig durch den Trojaner verschlüsselt wurden. Die Spezialisten für Datenrettung empfehlen, auf keinen Fall auf die Lösegeldforderung und die Zahlung mit Bitcoin einzugehen. Das Risiko, dass trotz der Zahlung noch immer die Daten verschlüsselt bleiben ist enorm hoch. In vielen Fällen sind die Zelte der Erpresser bereits abgebrochen, zum Beispiel weil Ermittlungen der jeweiligen Strafverfolgungsbehörden die Fährte aufgenommen haben.
Wenn der Anhang geöffnet wurde oder gar schon wichtige Daten durch den Trojaner verschlüsselt wurden, empfiehlt Lars Müller, technischer Leiter bei Datarecovery folgende Schritte:

1. Trennen Sie Backup-Festplatten schnellstmöglich vom PC.
2. Unterbrechen Sie Netzwerkverbindungen; am besten das Netzwerkkabel aus dem PC entfernen.
3. Informieren Sie die IT-Sicherheitsbeauftragten, damit sofort reagiert werden kann und weitere Mitarbeiter vor der Gefahr gewarnt werden.
4. Bewahren Sie die E-Mail zur späteren Analyse auf. Allerdings: Den Anhang keinesfalls erneut öffnen.
5. Kontaktieren Sie IT-Forensiker bzw. ein spezialisiertes Datenrettungsunternehmen für eine erste Einschätzung des Schadens und den Möglichkeiten der Wiederherstellung der Daten.

IT-CleverNet GmbH
Gehrenweg 2
5103 Möriken
Fon: 062 897 49 59
Fax: 062 897 49 55
it@itclevernet.ch
www.itclevernet.ch

E-Mail mit Erpressungs-Trojaner «GandCrab» zirkuliert

Wie versteckt sich GandCrab in der E-Mail?

Es handelt sich beim Inhalt um eine angebliche Bewerbung auf eine ausgeschriebene Stelle. Die Namen der Fake-Bewerber sowie das jeweilige Foto im Anhang variieren jeweils. Die Gefahr steckt jedoch in der als ZIP-File gepackten Datei, die sich ebenfalls im Anhang der E-Mail befindet. Wird dieses Archiv entpackt und die darin enthaltene .exe-Datei ausgeführt, installiert sich der Crypto-Trojaner und verschlüsselt sämtliche Daten auf dem Windows-Computer und auch auf sämtlichen von diesem PC aus erreichbaren Netzwerkressourcen, also Backup-Datenträgern, zentralen Shares, oder NAS-Systemen. Die verschlüsselten Dateien werden anschliessend mit der Dateiendung .krab versehen.

Auch macOS bedroht

Neben Gandcrab kann das Exploit Kit «Fallout» noch weitere Malware auf Computer schleusen, wie Heise Online schreibt. Auch macOS-Nutzer stehen im Fokus von Fallout. Gandcrab sei für Nutzer dieses Systems aber nicht gefährlich. Surft man als Mac-Nutzer eine damit präparierte Seite an, wird man umgeleitet. Auf dieser Webseite erscheinen Werbeanzeigen, die potenziellen Opfern Fake-Antiviren-Software unterjubeln wollen. GandCrab ist kein neuer Schädling, die Version 3 kursiert bereits seit dem zweiten Quartal 2018 im Netz. Die Malware wurde in zahlreichen Varianten anderer E-Mails gesichtet. So unter anderem auch als getarnte Bestellung mit dem Betreff <Order #00001», wobei eine beliebige Ziffer als Bestellnummer generiert wurde. Die im ZIP File versteckte .exe Datei ist ein VBS-Downloader (Visual Basic Script), welcher den Virus dann auf dem PC installiert. Bei der Bewerbermail-Version haben wir es bereits mit der Version 4 der Ransomware zu tun.

IT-CleverNet GmbH (ho)

Quellennachweis: PCTIPP Ausgabe 10.9.2018