Offline Zahlungs-Software im Visier von Hackern - Schweizer Unternehmen betroffen

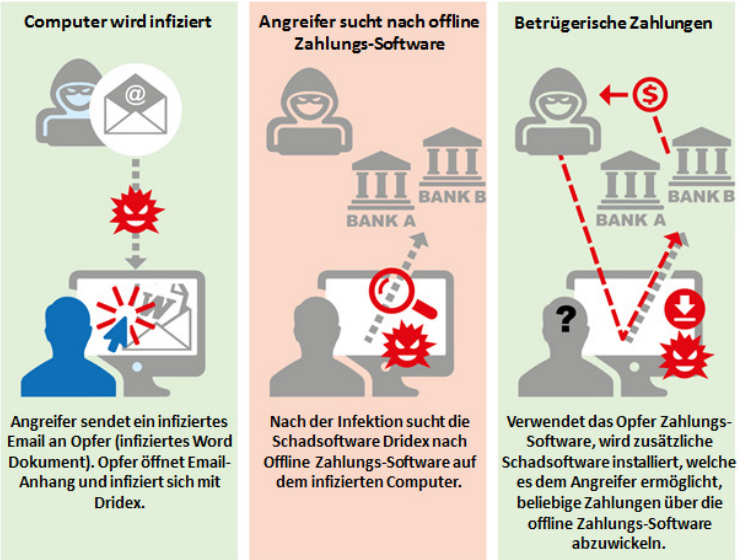
25.07.2016 - In den letzten Tagen hat MELANI mehrere Fälle der Schadsoftware Dridex beobachtet, die sich gegen Offline Zahlungs-Softwarelösungen richtet. Solche Software wird in der Regel von Unternehmen verwendet, um eine grössere Anzahl an Zahlungen via Internet an eine oder mehrere Banken zu übermitteln. Werden Computer, welche solche Software verwenden, kompromittiert, sind die potenziellen Schäden entsprechend hoch. MELANI empfiehlt Unternehmen deshalb dringend, Computer, welche für den Zahlungsverkehr verwendet werden, entsprechend zu schützen.

In den vergangenen Tagen hat die Melde- und Analysestelle Informationssicherung MELANI mehrere Hinweise zu Fällen erhalten, bei denen Angreifer versuchten mittels der Schadsoftware Dridex betrügerische Zahlungen über offline Zahlungs-Software auszulösen. Dabei wird in vielen Fällen versucht, gleich mehrere Zahlungen innert kurzer Zeit an ausländische Empfänger auszulösen. Der potenzielle Schaden ist entsprechend hoch.

Bei der Schadsoftware Dridex handelt es sich um einen bekannten eBanking Trojaner, welcher sich in der Regel über schädliche Microsoft Office Dokumente in Emails von

vermeintlich legitimen Absendern verbreitet. MELANI hat bereits Anfang Juli vor solchen schädlichen Microsoft Office Dokumenten gewarnt.

Vermehrt schädliche Office Dokumente im Umlauf:
https://www.melani.admin.ch/melani/de/home/dokumentation/newsle
(/melani/de/home/dokumentation/newsletter/malicious_office_docum



Modus operandi

Nach der Infektion sucht die Schadsoftware Dridex nach Offline Zahlungs-Software auf dem infizierten Computer. Solche Software wird von vielen Unternehmen verwendet, um grössere Mengen an Zahlungen via Internet an eine oder mehrere Banken zu übermitteln. Auf dem infizierten Computer sucht Dridex aktuell nach folgender offline Zahlungs-Software bzw. Software von untenstehenden Herstellern. Findet Dridex eine solche Zahlungs-Software auf dem Computer, kann weitere Schadsoftware aus dem Internet nachgeladen werden, welche dann für das Erfassen von betrügerischen Zahlungen verwendet wird.

Software-Hersteller
Abacus
Abrantix
Alphasys
Argo-Office
Bellin
Cashcomm
CoCoNet
Crealogix
Epsitec
financesuite
Financesuite
Macrogram
Mammut
Mmulticash
Moneta
Multiversa
Myaccessweb
Omikron
Quatersoft
Softcash
Softcrew
Starmoney
Trinity

Auszug von Zahlungs-Software Herstellern, die in der Konfigurationsdatei von Dridex enthalten sind.

Um sich vor solchen Angriffen zu schützen, empfiehlt MELANI Computer, welche für den Zahlungsverkehr verwendet werden, entsprechend abzusichern:

- **Verwenden Sie für offline Zahlungs-Software und eBanking einen dedizierten Computer, auf welchem Sie nicht im Internet surfen oder Emails empfangen.**
- **Verwenden Sie für die Visierung von Zahlungen eine Kollektivunterschrift über einen Zweitkanal (z.B. eBanking). Erkundigen Sie sich bei Ihrer Bank über entsprechende Möglichkeiten.**
- **Falls Sie einen Hardware-Token (z.B. Smart Card, USB-Dongle) verwenden, entfernen Sie diesen nach Gebrauch der Zahlungs-Software.**
- Speichern Sie Zugangsdaten (Vertragsnummer, Passwort, etc.) für eBanking und Zahlungs-Software nicht auf dem Computer bzw. in der Software.
- Erkundigen Sie sich beim Hersteller Ihrer Zahlungs-Software über zusätzliche Sicherheitsmassnahmen und aktivieren Sie die automatischen Softwareupdates.
- Melden Sie verdächtige Zahlungen umgehend Ihrer Bank.

Um eine Infektion mit Dridex und anderer Schadsoftware in Ihrem Unternehmen zu verhindern, empfiehlt MELANI zudem folgende Massnahmen:

- Stellen Sie sicher, dass potenziell schädliche Email Anhänge bereits auf Ihrem Email-Gateway bzw. Spam-Filter blockiert bzw. gefiltert werden. Gefährliche Email Anhänge verwenden unter anderem folgende Dateieendungen:

  .js (JavaScript)
  .jar (Java)
  .bat (Batch file)
  .exe (Windows executable)
  .cpl (Control Panel)
  .scr (Screensaver)
  .com (COM file)
  .pif (Program Information File)
  .vbs (Visual Basic Script)
  .ps1 (Windows PowerShell)
  .wsf (Windows Script File)
  .docm (Microsoft Word mit Makros)
  .xlsm (Microsoft Excel mit Makros)
  .pptm (Microsoft PowerPoint mit Makros)

- Versichern Sie sich, dass solche gefährlichen E-Mail-Anhänge auch dann blockiert werden, wenn diese in Archiv-Dateien wie Beispielsweise ZIP, RAR oder aber auch in geschützen Archiv-Dateien (z.B. in einem passwortgeschützten ZIP) an Empfänger in Ihrem Unternehmen versendet werden.
- **Zusätzlich sollten sämtliche E-Mail-Anhänge blockiert werden, welche Makros enthalten (z.B. Word, Excel oder PowerPoint Anhänge mit Makros).**

Weitere Massnahmen zur Erhöhung der IT-Sicherheit in KMUs finden Sie in unserem Merkblatt.

Merkblatt IT-Sicherheit für KMUs:
https://www.melani.admin.ch/it-sicherheit-fuer-kmus (/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html#par_text)

10-Punkte Programm zur Erhöhung der IT-Sicherheit:
https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it/fachgerechte-it-infrastruktur/it-sicherheit.html

Informationen von Herstellern
mammut soft computing ag, 12. Juli 2016:
https://www.mammut-soft.ch/images/Doku/Dringender_Sicherheitshinweis.pdf

Fachkontakt (mailto:info@melani.admin.ch)
Letzte Änderung 25.07.2016

https://www.melani.admin.ch/content/melani/de/home/dokumentation/newsletter/offline-payment-software.html

---

Melde- und Analysestelle Informationssicherung MELANI