Landing Page BSI für Bürger

Botnetzinfrastruktur „Avalanche“ ausgehoben

Eine international agierende Tätergruppierung hat millionenfach private und geschäftliche Computersysteme mit unterschiedlicher Schadsoftware infiziert. Dieses Netzwerk mit dem Namen Avalanche ist derzeit eine der weltweit größten bekannten Botnetzinfrastrukturen. In dieser konnten insgesamt 20 verschiedene Botnetze identifiziert werden, die die Infrastruktur zur Verbreitung von Spam- und Phishing-E-Mails sowie von Schadsoftware wie beispielsweise Ransomware (Erpressungstrojaner) oder Banking-Trojaner, nutzen.

Am 30.11.2016 hat die Staatsanwaltschaft Verden in Zusammenarbeit mit der ZKI Lüneburg und internationalen Partnern Avalanche ausgehoben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist dabei unterstützend tätig. Im Rahmen dieser Zerschlagung werden nun sogenannte Sinkhole-Server eingesetzt, mit deren Hilfe IP-Adressen identifiziert werden, hinter denen sich mit Schadsoftware befallene Geräte verbergen. Diese IP-Adressen werden den jeweilig zuständigen Internetprovidern zur Verfügung gestellt, die dadurch in der Lage sind, ihre Kunden schriftlich über die Infektion ihres Systems zu informieren. Auf diese Weise werden nur Kunden informiert, deren Systeme aktuell infiziert sind und deren IP-Adressen im Verlauf dieser Aktion identifiziert werden können.

Betroffene sollten ihre Geräte auf eine Infektion mit Schadprogrammen überprüfen und Sicherheitslücken schließen. Die Schadprogramme auf den betroffenen Systemen wurden durch die Zerschlagung der Botnetzinfrastruktur nicht gelöscht. Es kann daher nicht ausgeschlossen werden, dass die Täter zu einem späteren Zeitpunkt wieder Kontrolle über die jeweiligen Botnetze erhalten. Betroffene sollten daher möglichst bald handeln. Auch für Nutzer, die kein Schreiben ihres Providers erhalten, empfiehlt sich dieses Vorgehen.

Nach aktuellem Kenntnisstand des BSI sind überwiegend Windows-Systeme und Android-Smartphones Teil der jeweiligen Botnetze gewesen. Dennoch kann eine Infektion bei Smartphones mit Apple iOS, Microsoft Windows Phone oder Betriebssystemen wie Apples OS X oder Linux nicht ausgeschlossen werden. Ebenso sind nach aktuellem Kenntnisstand keine Geräte des Internets der Dinge (Internet of Things, IoT) wie beispielsweise Webcams, Drucker oder TV-Empfänger Teil dieser Botnetze.

Empfehlungen, wie Sie im Fall einer Infektion mit einem Schadprogramm vorgehen sollten, Hintergründe zur Benachrichtigung durch die Provider und viele weitere Informationen finden Sie in unseren FAQ zu Avalanche und Botnetzen.

Weitere Informationen rund um Schadprogramme finden Sie hier auf bsi-fuer-buerger.de sowie auf den Seiten des Anti-Botnet Beratungszentrums.

Häufige Fragen

1. Ich habe von der Abschaltung der Avalanche-Botnetzinfrastruktur gehört. Was bedeutet das?

Eine international agierende Tätergruppierung hat eine Infrastruktur für Botnetze aufgebaut, über die millionenfach private und geschäftliche Computersysteme und Mobilgeräte mit unterschiedlicher Schadsoftware infiziert wurden. Ca. 20 verschiedene Botnetze nutzten diese Infrastruktur, um u.a. Spam- und Phishing-E-Mails zu versenden, Ransomware (Erpressungstrojaner) zu verbreiten und die Nutzer von Online-Banking-Angeboten zu betrügen. Nähere Informationen finden Sie dazu in der gemeinsamen Pressemitteilung der Staatsanwaltschaft Verden (Aller), der Zentralen Kriminalinspektion Lüneburg (ZKI) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

2. Ich habe eine Benachrichtigung von meinem Provider erhalten. Woher weiß dieser, dass ich betroffen bin?

Im Rahmen der Zerschlagung werden sogenannte Sinkhole-Server eingesetzt, zu denen die Verbindungsversuche infizierter Systeme umgeleitet werden. Sie dienen dazu, diese Verbindungsversuche aufzuzeichnen. Auf diesem Weg erhält das BSI die IP-Adressen dieser Systeme. Da den Internetserviceprovidern feste Adressbereiche zugeordnet sind, kann das BSI die in ihrem Adressbereich befindlichen IP-Adressen gezielt an die Provider melden. Diese sind dann in der Lage, die betroffenen Kunden zu identifizieren und zu warnen. Dies ist notwendig, da die Identifizierung der Kunden technisch ausschließlich durch die Internetserviceprovider erfolgen kann. Dem BSI liegen keine Kundendaten vor, eine direkte Warnung durch das BSI kann daher nicht erfolgen.

3. Ich habe eine Benachrichtigung von meinem Provider erhalten. Was soll ich tun?

Die Benachrichtigung bedeutet, dass zu dem von Ihrem Provider angegebenen Zeitpunkt an Ihrem Netzwerkanschluss ein Gerät Teil der Avalanche-Infrastruktur war und vermutlich immer noch ist. Das BSI empfiehlt betroffenen Anwendern in diesem Fall, grundsätzlich alle am Netzwerkanschluss genutzten Computer oder Mobilgeräte auf Befall mit Schadsoftware zu überprüfen und Sicherheitslücken zu schließen. Es wurde festgestellt, dass die Täter in der Avalanche-Botnetzinfrastruktur hauptsächlich Schadsoftware auf Rechnern mit Windows-Betriebssystem platziert haben. Daneben wurden aber auch Schadsoftwarefamilien identifiziert, die auf Smartphones und Tablets mit Android zum Einsatz kommen. Dennoch ist nicht auszuschließen, dass Schadsoftware auch unter anderen Betriebssystemen eingesetzt wurde. Sofern Ihr Provider angegeben hat, um welche Schadsoftware es sich handelt, können Sie unter Frage 17 weitergehende Informationen zu den bisher bekannten der bei Avalanche eingesetzten Schadprogramme und einer empfohlenen Vorgehensweise erhalten.

Nach einer Bereinigung der Rechner und Mobilgeräte empfiehlt das BSI alle Passwörter zu ändern, die Sie für Ihren Mail-Account und andere Benutzerkonten bei Online-Shops, Sozialen Netzwerken

oder weiteren Internetdiensten nutzen. Wichtig: Überprüfen und bereinigen Sie zuerst Ihre Systeme und ändern Sie danach Ihre Passwörter! Andernfalls kann eine eventuelle Schadsoftware auch die neuen Passwörter mitlesen.
Achten Sie bei der Änderung darauf, dass Sie ein möglichst sicheres Passwort wählen und nicht für jeden Dienst das gleiche Passwort nutzen. Empfehlungen hierzu gibt das BSI unter www.bsi-fuer-buerger.de/Passwoerter . Zur Prüfung auf Schadsoftwarebefall gibt es eine Reihe von Virenschutzprogrammen. Weitere Informationen rund um die Bereinigung von infizierten Rechnern finden Sie hier auf bsi-fuer-buerger.de sowie auf den Seiten des Anti-Botnet Beratungszentrums. Sollte Ihr Virenschutzprogramm keine Infektion finden, empfiehlt sich der Einsatz einer Virenschutz-Boot-CD, beispielsweise das Antibot Rettungssystem, welches vom Anti-Botnetz-Beratungszentrums angeboten wird. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Betriebssystem neu installieren.

Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Hinweise und Empfehlungen des BSI unter 12 Sicherheitstipps.Tipps zum Schutz Ihres Smartphones oder Tablets finden Sie unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

4. Erkennt mein Virenschutzprogramm die über die Avalanche-Botnetze verteilte Schadsoftware?

In dieser Liste sind die Hersteller aufgeführt, deren Produkte nach Herstelleraussage einen großen Teil der Schadsoftware von Avalanche erkennen können. Das BSI hat nicht überprüft, ob und welchem Umfang dies zutreffend ist. Die Liste erhebt keinen Anspruch auf Vollständigkeit. Durch die ständige Weiterentwicklung der Schadsoftware ist nicht gewährleistet, dass alle Infektionen von den nachfolgenden Herstellern garantiert erkannt werden können.

- Avira
  - PC Cleaner
- Bit Defender
  - Bitdefender Removal Tool (englisch)
- Dr. Web
  - Dr. Web CureIt!
- ESET
  - ESET Online Scanner
- F-Secure
  - F-Secure Online Scanner
- G-Data
- Kaspersky
  - Kaspersky Total Security
  - Kaspersky Rescue Disk
- McAfee
  - McAfee Stinger (englisch)
- Symantec/Norton
  - Norton Power Eraser
- TrendMicro
  - HouseCall

- Diese Liste wird erweitert.
- Weitere Informationen rund um die Säuberung von infizierten Rechnern finden Sie hier auf bsi-fuer-buerger.de sowie auf den Seiten des Anti-Botnet Beratungszentrums.

5. Ich habe keine Benachrichtigung meines Providers erhalten. Bedeutet dies, dass mein Rechner frei von Schadsoftware ist?

Nein, leider bedeutet es das nicht automatisch. Falls Sie keine Benachrichtigung durch den Provider erhalten haben, bedeutet dies nur, dass die IP-Adresse Ihres Netzwerkanschlusses im Rahmen der Abschaltung der Botnetz-Infrastruktur nicht bekannt wurde oder Ihr Provider Sie noch nicht informiert hat. Das BSI informiert die Provider über die ihnen zugeordneten IP-Adressen infizierter Systeme. Die Zuordnung, welcher Kunde des Providers betroffen ist und die Entscheidung wann dieser informiert wird, erfolgt durch den Internet-Serviceprovider.
Es gibt neben der in der Avalanche-Botnetzstruktur eingesetzten Schadsoftware eine Vielzahl von Schadsoftware sowie viele weitere Botnetze, die auch weiterhin aktiv sind. Um eine mögliche Infektion zu erkennen, können Sie eine vollständige Untersuchung ihres Systems mit einem Virenschutzprogramm durchführen. Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Empfehlungen des BSI unter 12 Sicherheitststipps.

6. Wie wurde mein Rechner infiziert?

Die Schadprogramme der Avalanche-Botnetzinfrastruktur wurden typischerweise per E-Mail verbreitet. Diese enthielten oftmals eine persönliche Ansprache (Name und teilweise auch Vorname oder Nickname des E-Mail-Empfängers) und einen infizierten Dateianhang . Im Text dieser Spam-Mails [LINK zu bsi-fuer-buerger SPAM] wurde dem Empfänger z.B. mitgeteilt, dass durch Vertragsabschlüsse, Mitgliedschaften, Onlinekäufe oder ähnliches Kosten in empfindlicher Höhe entstanden seien. In den unaufgefordert übersandten E-Mails befanden sich in der Regel Anhänge im „ZIP-Format“, die eine Rechnung/ Abmahnung für den genannten Kauf, die Mitgliedschaft oder ähnliches enthielten. Im Anhang befand sich dann jedoch meist ein sogenannter Downloader, der Kontakt zu einem Steuerungsserver aufgenommen und von dort Schadsoftware heruntergeladen hat.
Grundsätzlich kann Schadsoftware auch über andere Verbreitungswege [https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme/schadprogramme_node.html] auf Ihr System gelangen.

7. Was bedeutet es, wenn mein Computer oder Smartphone Teil eines Botnetzes ist?

Die Infektiondes Computers oder Smartphones mit Schadsoftware führt oft dazu, dass das System zum Teil eines Botnetzes wird. Mit dem Begriff Bot ist dabei ein Schadprogramm gemeint, welches einem Angreifer die Fernsteuerung des infizierten Gerätes ermöglicht. Von Botnetzen spricht man, wenn sehr viele Geräte (meist mehrere Tausend) per Fernsteuerung zusammengeschlossen werden. Botnetze werden dazu eingesetzt, vertrauliche Daten wie Passwörter, Online-Banking-Daten oder Geschäftsinformationen zu stehlen. Botnetze dienen auch dazu, verteilte Angriffe auf die Verfügbarkeit von Internetsystemen (sogenannte Distributed Denial of Service oder kurz

DDoS-Angriffe) durchzuführen. Aufgrund ihrer vielfältigen Einsatzmöglichkeiten und der wirtschaftlich motivierten kriminellen Energie, welche die Täter aufbringen, stellen Botnetze derzeit eine der größten Gefahren im Internet dar. Über gefälschte/ manipulierte Internetseiten oder wie im Fall Avalanche, über Phishing-Angriffe mit gefälschten E-Mails, können Daten in falsche Hände gelangen oder auch Identitäten gestohlen werden.
Wie ein Botnetz funktioniert haben wir für Sie in einem kurzen Video erklärt.
[https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/botnetze_node.html]
Ist mir bereits ein Schaden entstanden, ohne dass ich es bemerkt habe?
Das ist möglich. Die von den Tätern eingesetzte Schadsoftware eröffnet eine Vielzahl von Möglichkeiten, auf den infizierten PC zuzugreifen. Etwa zur Ausspähung weiterer Daten auf Ihrem Computer oder zur Manipulation von Online-Transaktionen, die Sie bei Online-Shops oder im Rahmen des Online-Bankings durchführen.
Deshalb sollten Sie in regelmäßigen Abständen anhand eines Kontoauszugs etwa in Papierform prüfen, ob Ihnen verdächtige Kontobewegungen auffallen. Beispielsweise ist die in Avalanche eingesetzte Schadsoftware URLzone in der Lage, die Anzeige des Bankkontostandes im Internet-Browser zu manipulieren, so dass eine Prüfung per Internet-Browser kein verlässliches Ergebnis liefert. Wir haben für Sie Informationen zu sicherem Online-Banking zusammengestellt.
[https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/onlinebanking_node.html]

8. Mein Virenschutzprogramm zeigt nach einem Scan oder einer Bereinigung keine Infektion an. Ist mein System nun sicher?

Eine 100%-ige Garantie für eine erfolgreiche Bereinigung durch ein Anti-Virenprogramm ist nicht möglich, da die Angreifer regelmäßig die eingesetzte Software anpassen. Untersuchungen zeigen, dass befallene Systeme häufig mit mehreren Schadprogrammen infiziert sind. Es ist daher wichtig, nach einer Benachrichtigung durch den Provider Ihre Geräte anhand eines geeigneten Virenschutzprogramms sorgfältig auf Befall zu prüfen.
Sollten Sie Zweifel haben, dass die Bereinigung erfolgreich war, empfiehlt es sich sicherheitshalber, nach einem Backup der Daten das System zu löschen und neu aufzusetzen. Beachten Sie bitte dabei, dass Sie aus dem Backup keine ausführbaren Programme wiederherstellen, da diese mit der Schadsoftware befallen sein könnten. Ziehen Sie im Zweifel einen Computer-Spezialisten hinzu.
Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Hinweise und Empfehlungen des BSI unter 12 Sicherheitstipps.

9. Sind Geräte des Internets der Dinge (Internet of Things, IoT) wie beispielsweise Webcams, Drucker oder TV-Empfänger betroffenen?

Bei der analysierten Botnetz-Infrastruktur konnten keine IoT-Botnetze identifiziert werden. Nach aktuellem Kenntnisstand des BSI sind vorrangig Windows-Systeme und Android-Geräte betroffen.

10. Was ist der Unterschied zwischen einer Botnetzinfrastruktur und einem Botnetz?

Eine Botnetzinfrastruktur wird von Kriminellen als redundante Infrastruktur zum Betrieb von Botnetzen angeboten. Sie ermöglicht es den Tätern, ihre auf vielen tausend Geräten verteilten Bots (das Botnetz) zu steuern ohne eine Vielzahl von eigenen Servern betreiben zu müssen.

11. Warum könnten einzelne Botnetze trotz des Aushebens der Infrastruktur wieder aktiv werden?

Die Botnetzinfrastruktur wurde zwar abgeschaltet, die Bots selbst bleiben aber bis zu einer Bereinigung durch den Nutzer auf den Geräten. Falls es den Tätern gelingt, eine alternative Botnetzinfrastruktur aufzubauen, könnten diese Bots erneut ferngesteuert werden. Daher ist es wichtig, diese Bots zügig von betroffenen Geräten zu entfernen

12. Mein Provider hat in seinem Anschreiben den Namen einer Schadsoftware genannt, mein Virenschutzprogramm findet aber nur Schadsoftware mit anderem Namen. Was bedeutet das?

Die Hersteller von Virenschutzprogrammen benennen Schadsoftware von Botnetzen nicht einheitlich. Eine Zuordnung von Schadprogrammen zu Botnetznamen ist zudem sehr aufwändig und nicht immer eindeutig, da manche Schadprogramme als sogenannte Downloader nur zum Nachladen weiterer Schadprogramme genutzt werden. Häufig ist auf infizierten Rechnern zudem Schadsoftware für mehrere Botnetze zu finden. Daher werden bei Funden häufig generische Namen wie z.B. „Downloader.XYZ“ angezeigt.

13. Was hat dies mit gestohlenen Identitäten zu tun?

Beim dem aktuellen Takedown der Avalanche-Botnetzinfrastruktur handelt es sich nicht um einen Datenfund gestohlener Identitäten. Beim der Zerschlagung der Avalanche-Botnetzinfrastruktur werden die Bürger direkt von Ihren Providern informiert, sofern ihre Rechner aktuell infiziert sind.

14. Ich habe mein System bereinigt oder neu aufgesetzt, erhalte nun aber eine zweite Benachrichtigung durch meinen Provider. Muss ich erneut tätig werden?

Ja. Erhalten Sie eine erneute Meldung durch Ihren Provider ist Ihr System oder Ihr Smartphone erneut oder immer noch mit Schadsoftware infiziert. Dies kann beispielsweise folgende Gründe haben:

- Ihre Bereinigung war nicht erfolgreich oder nicht vollständig. Es empfiehlt sich, das System neu aufzusetzen. Im Zweifel sollten Sie einen Computer-Spezialisten hinzuziehen.
- Ihr System wurde erneut mit Schadsoftware infiziert. Bitte beachten Sie unsere Tipps zum

Schutz Ihres Systems [https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html] und unsere Hinweise zum sicheren Surfen im Internet.

- Ein anderes System an Ihrem Netzwerkanschluss ist immer noch oder erneut mit Schadsoftware infiziert.

15. Erhalte ich nun jedes Mal, wenn mein System mit Schadsoftware infiziert ist, eine Benachrichtigung?

Nein. Sie erhalten nur dann eine Benachrichtigung, wenn Ihr System mit Schadsoftware infiziert ist, die mit Sinkholes der abgeschalteten Avalanche-Botnetzinfrastruktur oder mit anderen Sinkholes kommuniziert, deren Informationen das BSI erhält. Schadsoftware, die aus anderen Quellen stammt, wird davon nicht erfasst, daher erhalten Sie darüber auch keine Benachrichtigung.
Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Hinweise und Empfehlungen des BSI unter 12 Sicherheitstipps.

16. Was ist ein Sinkhole-Server?

Ein gängiges Verfahren zur Identifikation mit Schadprogrammen infizierter Systeme ist die Umleitung von Steuerungsdomänennamen auf sogenannte "Sinkholes". Dabei werden die durch Analyse von Schadprogrammen ermittelten Domainnamen, mit denen die Schadprogramme kommunizieren, in Zusammenarbeit mit den zuständigen Domain-Registrierungsstellen auf Sinkhole-Server umgeleitet. Die Sinkholes protokollieren anschließend die Zugriffe auf die schädlichen Domainnamen mit Zeitstempel und der Quell-IP-Adresse sowie Quell-Port, von welcher der Zugriff erfolgte. Solche Sinkholes werden von zahlreichen Analysten und IT-Sicherheitsdienstleistern weltweit betrieben.
Da sich unter den Domainnamen keine legitimen Internetangebote befinden, werden diese üblicherweise nicht angesteuert. Ein Zugriff auf einen solchen Domainnamen ist daher ein gutes Indiz, dass sich unter der Quell-IP-Adresse, von welcher ein Zugriff erfolgt, mit hoher Wahrscheinlichkeit ein mit einem entsprechenden Schadprogramm infiziertes System befindet.
Die von den Sinkhole-Betreibern gelieferten Daten enthalten üblicherweise zu jedem protokollierten Zugriff einen Zeitstempel, die Quell-IP-Adresse, den aufgerufenen schädlichen Domainnamen und eine Bezeichnung des damit verbundenen Schadprogramms, welches den Domainnamen für die Kontaktaufnahme zu einem Kontrollserver verwendet. Häufig sind auch die IP-Adressen der Sinkholes sowie die Quell- und Ziel-Portnummern der Verbindung in den Daten enthalten.

17. Welche Schadsoftware wurde in der Avalanche-Botnetzinfrastruktur identifiziert?

Nachfolgend werden bekannte Botnetzfamilien (Schadsoftware) dargestellt, die in der Botnetzinfrastruktur Avalanche aufgefunden wurden. Bitte beachten Sie, dass die Hersteller von Virenschutzprogrammen die Botnetzfamilien nicht einheitlich benennen. Häufig werden bei Funden auch generische Namen wie z.B. „Downloader.XYZ“ angezeigt.

Andromeda/Gamarue

Andromeda/Gamarue ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Andromeda/Gamarue können dies z.B. die Banking-Trojaner Citadel, Rovnix oder UrlZone/Bebloh sein. Des Weiteren ist Andromeda/Gamarue mit Hilfe von Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Andromeda/Gamarue infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Andromeda/Gamarue wird von den Tätern, getarnt als Rechnung, per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken im Browser durch präparierte Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Andromeda/Gamarue weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Durchsuchung ihres Systems mit einem Virenscanner durch. Nutzen Sie gegebenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Andromeda/Gamarue zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten Systemalle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

Bolek

Bolek ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Bolek zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Bolek infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch.Es kann sich zusätzlich zu Bolek auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Citadel

Citadel ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Citadel zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto,

abfangen.

Wie habe ich mich mit Citadel infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Citadel auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann

Corebot

Corebot ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Corebot zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Corebot infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Corebot auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Dofoil/Smokeloader

Dofoil/Smokeloader ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Dofoil/Smokeloader kann dies z.B. die Schadsoftware Matsnu sein. Des Weiteren ist Dofoil/Smokeloader mit Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Dofoil/Smokeloader infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Dofoil/Smokeloader wird von den Tätern getarnt als Rechnung per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken in Browsern durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Dofoil/Smokeloader weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Nutzen Sie gegebenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Dofoil/Smokeloader zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

Gozi2

Gozi2 ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Gozi zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Gozi2 infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Gozi auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

KINS/VMZeus

KINS/VMZeus ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann KINS/VMZeus zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit KINS/VMZeus infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu KINS/VMZeus weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen

Marcher

Marcher ist ein Banking-Trojaner für Android-Geräte . Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Im Fall von Marcher werden SMS mit smsTAN/mTAN bgefangen und an die Täter weitergeleitet.

Wie habe ich mich mit Marcher infiziert?

Ein möglicher Infektionsweg ist über eine weitere Schadsoftware, z.B. einen Banking-Trojaner wie URLZone/Bebloh, die bereits Ihren Windows-PC infiziert hat. Diese Schadsoftware öffnet z.B. beim Besuch einer Banking-Seite ein Pop-Up-Fenster in ihrem Browser, mit der Aufforderung eine zusätzliche Sicherheitsanwendung auf ihrem Smartphone zu installieren. Alternativ kann Ihnen auch ein Link zu dieser Schadsoftware in einer SMS zugeschickt worden sein.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Smartphone oder Tablet durch. Nutzen Sie einen Virenscanner für Android oder setzen Sie ihr Smartphone auf die Werkseinstellungen zurück. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Matsnu

Matsnu ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Matsnu können dies z.B. die Banking-Trojaner Citadel und UrlZone/Bebloh sein.

Wie habe ich mich mit Matsnu infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Matsnu wird von den Tätern getarnt als Rechnung per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken in Browsern durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Matsnu weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

Nymaim

Nymaim ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Nymaim können dies z.B. die Banking-Trojaner Citadel und UrlZone/Bebloh sein. Des Weiteren ist Nymaim mit Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Nymaim infiziert?
Ein möglicher Infektionsweg ist E-Mail-Spam. Nymaim wird von den Tätern, getarnt als Rechnung, per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken in Browsern durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.
Was muss ich jetzt machen?
Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Nymaim weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Nutzen Sie gegebenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Nymaim zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

Pandabanker

Pandabanker ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Pandabanker zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.
Wie habe ich mich mit Pandabanker infiziert?
Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.
Was muss ich jetzt machen?
Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Pandabanker auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Ranbyus

Ranbyus ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Ranbyus zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.
Wie habe ich mich mit Ranbyus infiziert?
Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.
Was muss ich jetzt machen?
Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch.Es kann sich zusätzlich zu Ranbyus auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine

vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Rovnix

Rovnix ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Rovnix zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen. Rovnix kann sich sehr tief im System verstecken, sodass eine Erkennung vom infizierten System aus nicht mit Sicherheit festgestellt werden kann.

Wie habe ich mich mit Rovnix infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Rovnix weitere Schadsoftware auf Ihrem System befinden. Nutzen Sie eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Rovnix zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem mit ihrer Bank in Kontakt, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Smart App

Smart App ist ein Banking-Trojaner für Android-Geräte. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Im Fall von Smart App werden SMS mit smsTAN/mTAN abgefangen und an die Täter weitergeleitet.

Wie habe ich mich mit Smart App infiziert?

Ein möglicher Infektionsweg ist über eine weitere Schadsoftware, z.B. einen Banking-Trojaner wie URLZone/Bebloh, die bereits Ihren PC infiziert hat. Diese Schadsoftware öffnet z.B. beim Besuch einer Banking-Seite ein Pop-Up Fenster in Ihrem Browser, mit der Aufforderung eine zusätzliche Sicherheitsanwendung auf ihrem Smartphone zu installieren. Alternativ kann Ihnen auch ein Link zu dieser Schadsoftware in einer SMS zugeschickt worden sein.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Smartphone oder Tablet durch. Nutzen Sie einen Virenscanner für Android oder setzen Sie Ihr Smartphone auf die Werkseinstellungen zurück. Sichern Sie vor einer Bereinigung Ihre persönlichen Daten. Ändern Sie auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

TeslaCrypt

TeslaCrypt ist ein Ransomware-Trojaner. Ransomware-Trojaner verschlüsseln Teile Ihrer Daten auf der Festplatte und erpressen dann Lösegeld für die Entschlüsselung dieser Daten.

Wie habe ich mich mit TeslaCrypt infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu TeslaCrypt auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann. Ein TeslaCrypt-Entschlüsselungswerkzeug wird von dem Europol-Projekt "No-More-Ransom" bereitgestellt (https://www.nomoreransom.org).

Tiny Banker/Tinba

Tiny Banker/Tinba ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab um, an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Tinba zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Tiny Banker/Tinba infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Tinba weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Trusteer App

Trusteer App ist ein Banking-Trojaner für Android-Geräte . Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Im Fall von Trusteer App werden SMS mit smsTAN/mTAN abgefangen und an die Täter weitergeleitet.

Wie habe ich mich mit Trusteer App infiziert?

Ein möglicher Infektionsweg ist über eine weitere Schadsoftware, z.B. einen Banking-Trojaner wie URLZone/Bebloh, die bereits Ihren PC infiziert hat. Diese Schadsoftware öffnet z.B. beim Besuch einer Banking-Seite ein Pop-Up Fenster in ihrem Browser, mit der Aufforderung eine zusätzliche

Sicherheitsanwendung auf ihrem Smartphone zu installieren. Alternativ kann Ihnen auch ein Link zu dieser Schadsoftware in einer SMS zugeschickt worden sein.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Smartphone durch. Nutzen Sie einen Virenscanner für Android oder setzen Sie ihr Smartphone auf die Werkseinstellungen zurück. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

URLzone/Bebloh

URLZone/Bebloh ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann URLZone/Bebloh zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit URLZone/Bebloh infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu URLZone/Bebloh weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

Vawtrak

Vawtrak ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Vawtrak zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Vawtrak infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Vawtrak auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung Ihre persönlichen Daten. Ändern Sie auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese

entsprechende Sicherheitsmaßnahmen treffen kann.

Xswkit

Xswkit ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Xswkit können dies z.B. die Banking-Trojaner Citadel, Rovnix oder UrlZone/Bebloh sein. Des Weiteren ist Xswkit mit Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Xswkit infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Xswkit wird von den Tätern, getarnt als Rechnung, per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken im Browser durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Xswkit nun auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Nutzen Sie gegenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Xswkit zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.