Banken und Kunden unter Cyberbeschuss

Von Anne Mickler

In Asien entwickelt sich ein neues Epizentrum für Cyberkriminelle, bei denen Banken besonders im Fokus stehen. Das geht inzwischen weit über einfaches Phishing hinaus. Neben Privatkunden wird zunehmend das Online-Banking im Firmenkundengeschäft ins Visier genommen, aber auch die Banken und ihre Infrastruktur selbst. Zu den neuen Bedrohungsszenarien gehören Cyberangriffe auf Geldautomaten, außerdem werden sogenannte digitale Masken, die eigentlich Betrugsmuster aufdecken sollen, für neue Angriffsformen verwendet. Es gab auch erste Proof-of-Concept-Angriffe auf Finanzdienstleister mithilfe gestohlener biometrischer Daten. Als Fazit hält der Autor fest: Verbraucher und Geschäfte, die keine Zwei-Faktor-Authentifizierung verwenden, sind gefährdet. Red.

Aktuelle Zahlen zeigen: Ob über das Smartphone oder den PC – digitale Banking-Nutzer standen in jüngster Zeit verstärkt im Visier von Cyberkriminellen. Laut den Analysen von Kaspersky wurden auf deutschen Windows-Geräten zwischen Januar und Juni 2019 mehr als doppelt so viele Banking-Trojaner (mit einem Zuwachs um 129,74 Prozentpunkte) erkannt und blockiert als noch im selben Zeitraum des Vorjahres.

Finanz-Malware, gemeinhin als Banking-Trojaner bezeichnet, richtet sich gegen Finanzdienstleister wie Banken und deren Kunden. Das Ziel der Hintermänner: finanzielle Ressourcen oder Finanzdaten einzelner Nutzer, wie etwa deren Zugangsdaten für das Online-Banking, Konto- und Kreditkartennummern oder Kryptowährungen, sowie der möglicherweise noch lukrativere Zugriff auf die Infrastruktur und Ressourcen von Finanzdienstleistern, wie beispielsweise Geldautomaten oder Online-Bezahl- beziehungsweise Banking-Systeme.

Auch auf Android – mit nahezu 99 Prozent Ziel Nummer eins im Bereich mobiler Schädlinge – haben sich die Erkennungszahlen mit einem Anstieg um 97,36 Prozentpunkte im Untersuchungszeitraum fast verdoppelt.

Fake-Mails im Namen der Bank sind die größte Phishing-Gefahr

Spam und Phishing bleiben weiter die typischen Angriffsvektoren für Finanz-Malware. So zählte Kaspersky in der ersten Jahreshälfte 2019 weltweit über 339000 Phishing-Versuche mithilfe gefälschter Webseiten, die sich als Startseiten großer Finanzinstitute ausgeben. Unaufmerksame Kunden übergaben dort ihre Zugangsdaten, Konto- und Kreditkartennummern oder andere sensible Finanzdaten direkt an Cyberkriminelle. Die Links auf diese falschen Webseiten werden über Spam-Mails verbreitet.

Im ersten Quartal 2019 wurde jede vierte Phishing-Attacke im Namen einer Bank ausgeführt. Damit liegen die Kunden von Banken im Bereich Phishing auf Rang eins, vor Webportalen und Bezahlsystemen.

Unternehmen verstärkt im Visier von Finanz-Malware

Ein weiterer gefährlicher Trend: finanziell motivierte Attacken gegen Geräte im Unternehmensumfeld (Corporate Devices) haben sich verstärkt. Auf sie entfallen im ersten Halbjahr dieses Jahres 30,9 Prozent der Angriffe, was einer Verdopplung im Vergleich zum Vorjahr entspricht (damals 15,3 Prozent).

Der Anstieg von Finanz-Malware sowie die erhöhte Angriffsfrequenz ist vor allem im Unternehmensbereich ein gefährlicher Trend. Der Grund: Beinhaltet

Anne Mickler,
Corporate Communications Manager,
DACH, Kaspersky Labs GmbH, Ingolstadt

der Schädling eine Wurmkomponente, kann er sich, wenn mehrere Geräte miteinander verbunden sind – wie in Organisationsnetzwerken der Fall –, selbstständig ausbreiten und mehr Schaden anrichten.

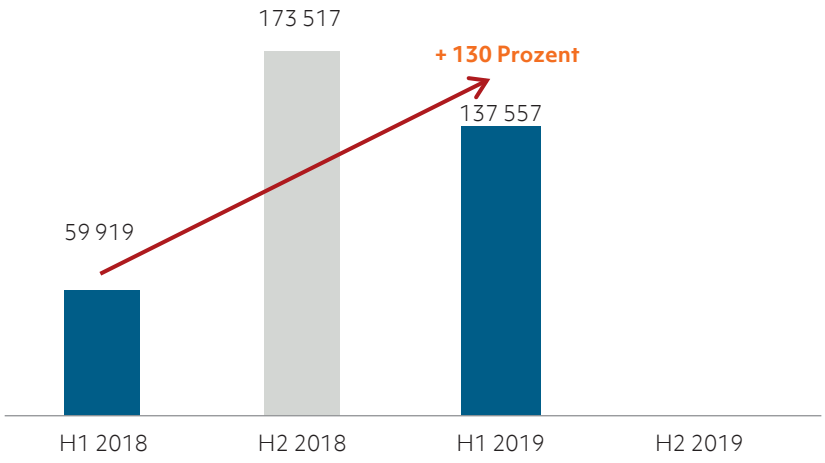
Spezifische Gefahren für Banken

Weltweit mehr als 100 betroffene Finanzinstitute in über 30 Ländern mit einer Beute von bis zu einer Milliarde US-Dollar[1)] – so lautet die Schadenbilanz des größten Cyberraubzugs der Geschichte der sogenannten Carbanak-Gang, deren Aktivitäten von Kaspersky erstmals im Jahr 2015 (am 15. Februar) öffentlich gemacht wurden.[2)] Ein Jahr später (8. Februar 2016) veröffentlichten die Cybersicherheitsexperten eine weitere Analyse, die sich explizit den Aktivitäten der Cyberbankräuber der Gruppen Carbanak, Metel und GCMAN widmete. Die Hauptaussage: Alle drei Gruppen attackierten Finanzinstitute mit vorangehenden, verdeckten APT-typischen Aufklärungsprojekten und maßgeschneiderter Malware. Zudem setzten die Gruppen legale Software sowie neue, innovative Schemata ein, um Barauszahlungen oder Überweisungen zu tätigen. Die Neuauflage der Carbanak-Gruppe (Carbanak 2.0) hatte zudem neben Banken auch Buchhaltungsabteilungen anderer Unternehmen im Visier und manipulierte deren Finanztransaktionen.

Im April 2019 wurde bekannt, dass der Quellcode des berüchtigten Carbanak-Trojaners bereits vor zwei Jahren auf Virus Total hochgeladen wurde, wo er bis dahin offenbar unentdeckt geblieben ist.

Im Mai 2019 zeigte eine Kaspersky-Analyse neue in Verbindung mit Carbanak stehende Erkenntnisse: Eigentlich galt die berüchtigte Fin7- beziehungsweise Carbanak-Cybergang im Jahr 2018 als aufgelöst. Allerdings entdeckten die Experten eine Reihe neuer Angriffe, hinter denen wohl Fin7 stand. Die Gruppe arbeitete eng mit der berüchtigten Carbanak-Gang zusammen, mit der sie auch Tools und Methoden teilte. Während sich Carbanak vor allem auf Banken konzentrierte, hatte Fin7 hauptsächlich Unternehmen im Visier und entwendete vermutlich Millionenbeträge aus den finanziellen Vermögenswerten der Opfer; darunter Zugangsdaten für Kartenzahlungen und Kontoinformationen auf Computern der Finanzabteilungen. Sobald die Bedrohungsakteure die gewünschten Informationen in ihre Hände bekamen, überwiesen sie Geld auf Offshore-Konten.

Abbildung 1: Entwicklung Banking-Trojaner



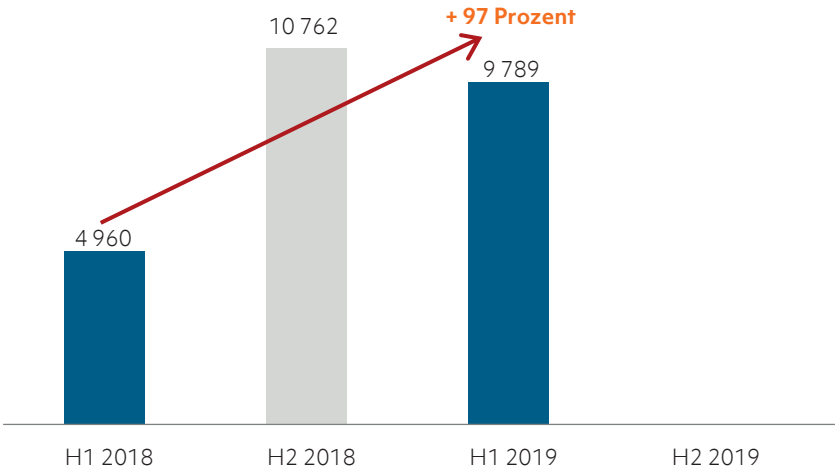
Im ersten Halbjahr 2019 stiegen die Finanz-Malware-Infektionen im PC-Bereich im Vergleich zum Vorjahr um 129,74 Prozentpunkte an. Quelle: Kaspersky

Neue Gefahr: Digitale Doppelgänger

Im April 2019 zeigte eine weitere Untersuchung: Auf der Plattform des im Darknet angesiedelten Untergrund-Online-Shops Genesis werden mehr als 60000 gestohlene, tatsächlich existierende digitale Identitäten gehandelt. Die Gefahr: Mittels der Identitäten ist Kreditkartenbetrug möglich, denn mit dem Marktplatz sowie weiteren schädlichen Tools lässt sich das eigentlich zur Betrugsverhinderung gedachte, auf maschinellem Lernen basierende Konzept digitaler Masken (Digital Masks) missbrauchen.

Wenn Nutzer bei Online-Transaktionen Finanz-, Zahlungs- oder persönliche Informationen auf einer Webseite eingeben, kommen meist fortschrittliche, analytische und auf maschinellem Lernen basierende Anti-Fraud-Lösungen zum Einsatz, um abzugleichen, ob die

Abbildung 2: Entwicklung mobile Banking-Trojaner



Im ersten Halbjahr 2019 stiegen die Finanz-Malware-Infektionen im mobilien Bereich (Android) im Vergleich zum Vorjahr um 97,43 Prozentpunkte an. Quelle: Kaspersky

User-Daten einer bestimmten digitalen Maske entsprechen. Diese Masken sind für jeden Anwender individuell; sie bringen die vom Nutzer normalerweise beim Banking- beziehungsweise Bezahlprozess auf Geräten oder im Browser hinterlassenen digitalen Fingerprints – wie Informationen über den Bildschirm und das Betriebssystem oder Browserdaten, beispielsweise Header, Zeitzone, installierte Plug-ins und Fenstergröße – mit fortschrittlichen Analyse- und maschinellen Lernmethoden zusammen.

Angriffe auf Geldautomaten hinterlassen keine Spuren

Mögliche Angriffsvektoren auf Geldautomaten sind für Banken ein riesiges Problem. Ein Malware-Vertreter, der sich explizit gegen Geldautomaten richtet, ist die Malware ATMitch. Eine Analyse vom April 2017 zeigte folgenden Fall: Als Bankangestellte einen ausgeraubten Geldautomaten vorfanden, ohne erkennbare Spuren physischer Gewaltanwendung oder Malware, standen sie vor einem Rätsel.

In einer zeitaufwendigen Untersuchung konnte die Vorgehensweise der Cyberkriminellen aufgedeckt werden: Es handelte sich um einen sogenannten „fileless" Einbruch ins Banknetzwerk. Damit ließ sich der Geldautomat in Sekundenschnelle und ohne wirklich nachzuverfolgende Spuren ausrauben.

Von einfachen Opfern zu schwierigeren Zielen

Echtes Geld und laufende Transaktionen machen den Finanzsektor zu einem der beliebtesten Ziele für einige der gefährlichsten Cyberkriminellen. Und während die Betrugstechnologien sich immer weiterentwickeln, steigen Cyberkriminelle zunehmend von einfachen Opfern auf schwierigere Ziele um, die zwar eine Herausforderung darstellen, bei denen sich ein Angriff jedoch wirklich lohnt – und diese Ziele werden von den Serviceanbietern selbst bereitgestellt.

Ein mehrstufiges Schutzkonzept hilft Unternehmen in der Finanz- und Bankenbranche bei der Implementierung einer flexiblen Sicherheitsstrategie. Die Bausteine hierfür sind:

– Erkennung und Risikominimierung bei zielgerichteten Angriffen und technologisch fortschrittlichen Bedrohungen durch Erkennung unterschiedlichster Kompromittierungsvektoren,

– Umfassende Sicherung von Endpoints und Embedded-Geräten wie Geldautomaten und Kassensystemen sowie anderen, am Point-of-Sale eingesetzten Technologien,

– Sicherheit für virtuelle und physische Server, VDI-Bereitstellung, Speichersysteme und sogar Datenkanäle in Private Clouds sowie erweiterten Workload-Schutz in Public Clouds sowie

– Detaillierte Einblicke in die von Cyberkriminellen eingesetzten Taktiken und Tools.

Erste Attacken mithilfe gestohlener biometrischer Daten

Aussagekräftige Bedrohungsdaten, fortschrittliche Machine-Learning-Technologien und ein Pool weltweit agierender Experten helfen dabei, die Immunität von Banken und Finanzdienstleistern auch gegen bisher unbekannte Cyberangriffe aufrechtzuerhalten.

Biometrische Systeme zur Nutzererkennung und -authentifizierung werden bereits von verschiedenen Finanzunternehmen eingeführt und verwendet. Doch auch erste bedeutende Schwachstellen haben sich bereits gezeigt. Diese beiden Tatsachen haben bereits zu ersten Proof-of-Concept-Angriffen auf Finanzdienstleister mithilfe gestohlener biometrischer Daten geführt.

Die Aktivität von Cyberkriminellen in den Ländern und Regionen Indien, Pakistan, Südostasien und Zentraleuropa steigt konstant: Dafür verantwortlich sind die unausgereiften Schutzprogramme im dortigen Finanzsektor und die rasche Verbreitung verschiedenster elektronischer Zahlungsmittel in Unternehmen und der Bevölkerung. Dadurch wird die Entstehung eines neuen Epizentrums digitaler Bedrohungen im Finanzsektor in Asien begünstigt – zusätzlich zu den bereits bestehenden Hotspots in Südamerika, auf der koreanischen Halbinsel und in der ehemaligen Sowjetunion.

Cyberkriminalität umgeht Anti-Fraud-Lösungen ohne 2FA

Attacken auf die Supply Chain, beispielsweise Softwareanbieter für den Finanzbereich oder Dienstleister für die Bankenbranche, haben sich als besonders effektiv herausgestellt. Kleine Unternehmen, die spezialisierte Finanzdienstleitungen für größere Firmen anbieten, sind neben Anbietern von Geldüberweisungssystemen, Banken und Börsen am stärksten gefährdet. Derartige Kompromittierungen entsprechender Lieferketten werden voraussichtlich auch dieses Jahr noch weiter zunehmen.

Verbraucher und Geschäfte, die bei Finanztransaktionen noch immer keine Zwei-Faktor-Authentifizierung oder Karten ohne Chips verwenden, sind gefährdet. Mit komplexen Methoden werden Computer- und Browsereinstellungen kopiert, sodass Anti-Fraud-Systeme zum Schutz vor Betrugsaktivitäten umgangen werden können. Dies führt dazu, dass Angriffe auf Terminals am Point-of-Sale wahrscheinlich abnehmen und Attacken sich stattdessen auf Online-Zahlungsplattformen verlagern werden.

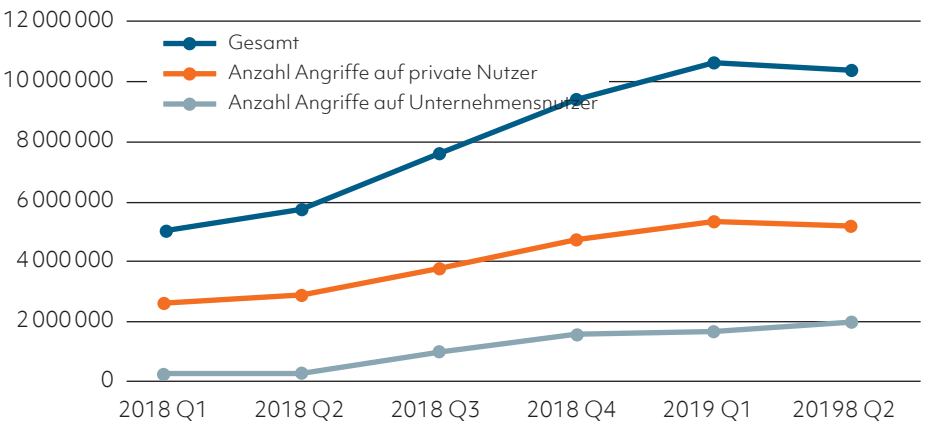
Angriffe auf das Mobile Banking von Geschäftskunden

Mobile Unternehmensanwendungen gewinnen zunehmend an Popularität. Dies wird vermutlich die ersten entsprechenden Angriffe im Mobile Banking auf ihre Benutzer zur Folge haben. Das vorhandene Instrumentarium der Cyberkriminellen ist reichhaltig und die Verluste, die Unternehmen zugefügt werden können, um ein Vielfaches höher, als wenn Einzelpersonen anvisiert werden. Die wahrscheinlichsten Angriffsvektoren sind hierbei Attacken auf Web-API-Ebene und über die Supply Chain.

Social-Engineering, also die Manipulation von Menschen zur Durchsetzung krimineller Machenschaften, ist nach wie vor ein entscheidender Faktor bei Angriffen. Cyberkriminelle gehen gezielt einzelne Personen in Unternehmen und Kreditinstituten an und verleiten sie, große Geldsummen zu überweisen. Dabei wird das adressierte Opfer von der Echtheit einer finanziellen Forderung, etwa durch seriös und authentisch anmutende, gefälschte E-Mails von Geschäftspartnern oder Subunternehmen überzeugt. Diese Art von Angriff ist bereits als CEO-Fraud bekannt. Dafür ist keine Malware nötig.

Verschiedene Social-Engineering-Taktiken werden 2019 zunehmen und etwa in Form von SIM-Swapping zum Einsatz kommen. Unter SIM-Swapping versteht man den Prozess, bei dem die Telefonnummer eines Nutzers auf eine SIM-Karte übertragen wird, die einem Cyberkriminellen gehört. Einmal im Besitz der persönlichen Nummer, können alle Passwörter zurückgesetzt und der Zugriff auf dessen Konten deutlich vereinfacht werden.

Abbildung 3: Entwicklung Banking-Trojaner



Gefährlicher Trend für Unternehmen – sie stehen verstärkt im Kreuzfeuer von Finanz-Malware

Quelle: Kaspersky

Fußnoten

1) www.heise.de/security/

2) Die Analyse von damals ist inklusive einem Video und Infografiken unter https://securelist.com/ verfügbar.