kaspersky

Wie gefährlich ist Online-Banking?

Das Halbjahresresümee 2019 für Finanzdienstleister und Verbraucher

Eine Kaspersky-Analyse

20.08.2019

kaspersky

Wie gefährlich ist Online Banking?

Das Halbjahresresümee 2019 für Finanzdienstleister und Verbraucher

Dieser Report beschäftigt sich mit den aktuellen Cybergefahren, denen Finanzdienstleister wie Banken sowie deren Kunden ausgesetzt sind. Dabei beleuchten die Experten von Kaspersky im ersten Teil die Bedrohungslage in puncto Finanz-Malware. Im zweiten Teil der Analyse werden die Gefahr zielgerichteter Attacken gegen die Banken selbst und passende Schutzmaßnahmen aufgezeigt. Abschließend wagen die Cybersicherheitsexperten noch einen Ausblick auf zukünftige Gefahren im Bereich Finanzbedrohungen.

Teil 1: Analyse Finanzbedrohungen im ersten Halbjahr 2019

Der folgende Kaspersky-Report analysiert die Gefährdungslage für Deutschland sowie weltweit bezüglich finanziell motivierter Malware gegen Privatnutzer und Organisationen.

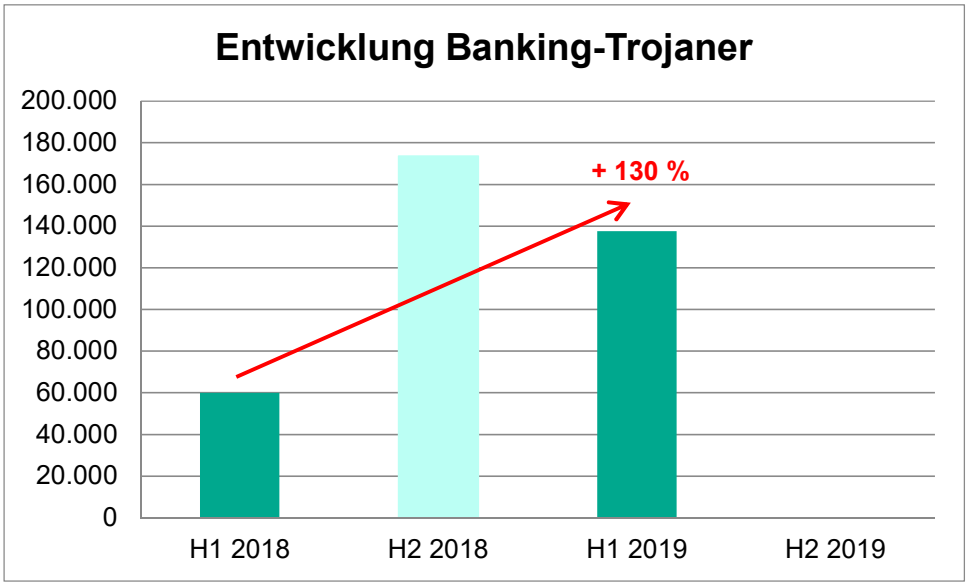
Definition Finanz-Malware

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.

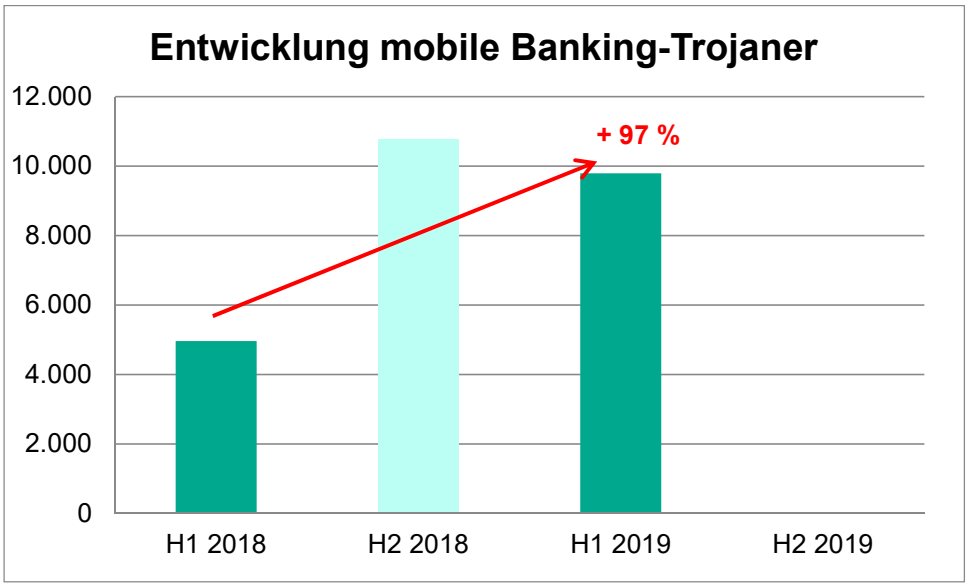
Deutschland – doppelt so viele Attacken gegen PC wie Smartphone-Nutzer

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.

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.



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



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

Die weltweite Bedrohungssituation

Die Malware-Trends für Deutschland entsprechen der weltweiten Entwicklung von Finanzschädlingen [1]:

- So wurden im ersten Halbjahr 2019 weltweit 430.000 Anwender von Finanz-Malware (Banking-Trojaner) attackiert. Betrachtet man die auf den PCs entdeckten Angriffe von digitalen Finanzattacken, stieg im ersten Halbjahr – nahezu analog zu Deutschland – das globale Aufkommen im Vergleich zum Vorjahreszeitraum um 93 Prozentpunkte an.
- Zudem ist die Anzahl neuer Finanz-Malware-Samples in der ersten Jahreshälfte global um 74 Prozent auf über 5 Millionen gestiegen.
- Auch hat sich die Frequenz der Finanz-Angriffe auf die Nutzergeräte merklich erhöht.

Die Einschätzung des Experten

„Wir erwarten, dass die Zahl der angegriffenen Nutzer in der zweiten Jahreshälfte weiter steigt. Da sich die Anwender in den Ferien weniger mit ihren vernetzten Geräten beschäftigen und somit auch in geringerem Umfang Opfer von Cyberattacken werden, ziehen für gewöhnlich nach der Urlaubszeit die Aktivitäten von Cyberkriminellen wieder an. Wir appellieren an alle, gerade nach den Ferien besondere Sorgfalt walten zu lassen. Das gilt für Online-Banking wie alle anderen Finanzdienstleistungen im Internet."

Christian Funk, Leiter des Forschungs- und Analyse-Teams der Region DACH bei Kaspersky

Größte Phishing-Gefahr: Fake-Mails im Namen der Bank

Spam und Phishing bleiben weiter die typischen Angriffsvektoren für Finanz-Malware. So zählten die Kaspersky-Experten in der ersten Jahreshälfte 2019 über 339.000 Phishing-Versuche mit Hilfe 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 [2] wurde jede von Kaspersky entdeckte vierte Phishing-Attacke im Namen einer Bank ausgeführt. Damit liegen die Kunden von Banken im Bereich Phishing auf Rang eins, vor Webportalen und Bezahlsystemen.

Weltweit noch mehr mobile Angriffe als in Deutschland

Auch die mobile Gefährdungslage hat sich in der ersten Jahreshälfte verschärft: In Deutschland hat Kaspersky fast doppelt so viele Erkennungen mobiler Banking-Trojaner festgestellt wie im Vorjahreszeitraum (97,36 Prozentpunkte mehr); weltweit gab es sogar einen Anstieg um 107 Prozentpunkte – mit mehr als 3,7 Millionen mobilen Finanzattacken zwischen Januar und Juni 2019. Hinzu kommt, dass viele Nutzer mobil unter der Ausnutzung großer Brands von Finanzdienstleistern und Bankenattackiert wurden.

Die gefährlichsten Varianten im mobilen Bereich sind die mobilen Banking-Trojaner Asacub und Svpeng.

Die Einschätzung des Experten

„Ein häufig gesehenes Instrument mobiler Schadsoftware ist ein Overlay, das über bekannte und populäre Apps wie dem offiziellen Playstore eingeblendet wird. Dabei wird der Eindruck erweckt, dass periodisch Kreditkarteninformationen zur Zahlung bei In-App Käufen oder anderen Transaktionen zur Überprüfung der Gültigkeit abgefragt werden. Bei Eingabe der sensitiven Information gelangen diese in die Hände der Malware-Autoren."

Christian Funk, Leiter des Forschungs- und Analyse-Teams der Region DACH bei Kaspersky

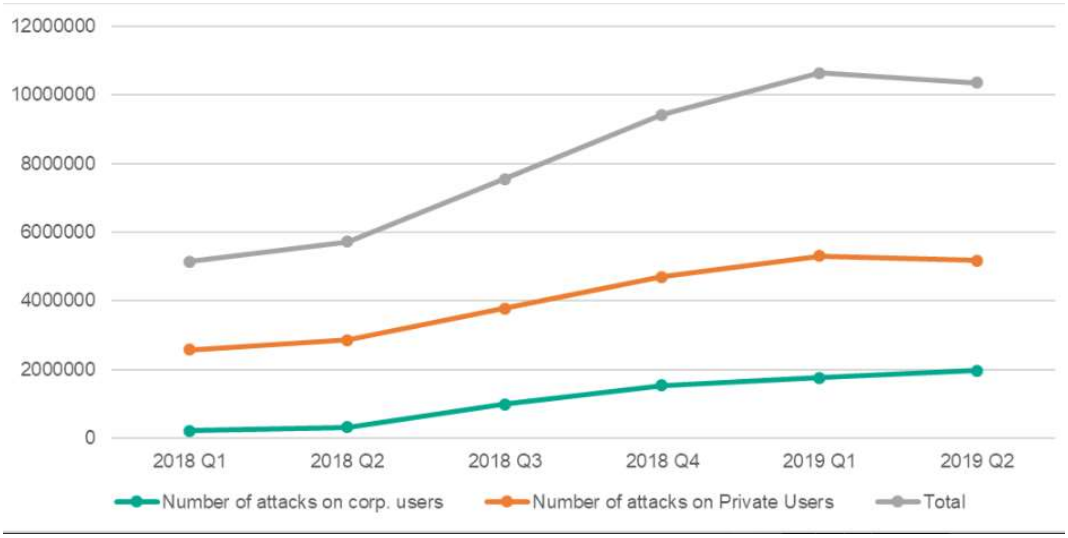
Family	%*
Trojan-Banker.AndroidOS.Asacub	51.39
Trojan-Banker.AndroidOS.Agent	16.75
Trojan-Banker.AndroidOS.Svpeng	14.91
Trojan-Banker.AndroidOS.Faketoken	7.56
Trojan-Banker.AndroidOS.Hqwar	2.56

BU: Die Top mobilen Schädlinge weltweit nach Malware-Familien, die im ersten Halbjahr 2019 eine mobile Finanzattacke ausgeführt haben.

Trend 1: Unternehmen verstärkt im Visier von Finanz-Malware

Ein weiterer gefährlicher Trend: finanziell motivierten Attacken gegen Geräte im Unternehmensumfeld (Corporate Devices) haben sich verstärkt. Auf sie entfallen im ersten Halbjahr dieses Jahres 30,9 Prozent aller von Kaspersky identifizierten 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 der Schädling eine Wurmkomponente, kann er sich, wenn mehrere Geräte miteinander verbunden sind – wie in Organisationsnetzwerken der Fall –, selbstständig ausbreiten und mehr Schaden anrichten.



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

Trend 2: Bisherige Unternehmens-Malware trifft nun auf Privatkunden

Der Blick auf die weltweite Bedrohungslage bezüglich Finanz-Malware zeigt darüber hinaus: Der im Untersuchungszeitraum populärste Banking-Trojaner gegen Anwender im privaten Umfeld ist mit 26 Prozent Zeus beziehungsweise Zbot [3]. Er stiehlt Zugangsdaten und verschafft sich gleichzeitig die Möglichkeit, aus der Ferne auf betroffene Geräte zuzugreifen.

Der am zweithäufigsten registrierte Banking-Trojaner ist hingegen eine bislang nur von Angriffen gegen Unternehmen bekannte Malware-Familie: RTM war bereits 2018 die gefährlichste Finanzmalware für Unternehmen [4] und auch in der ersten Jahreshälfte 2019 für 40 Prozent aller Angriffe verantwortlich. Jetzt wird dieser Schädling offenbar zunehmend für Angriffe auf Privatanwender eingesetzt.

Dritthäufigste Gefahr für private Nutzer ist aktuell die Malware-Familie Emotet [5]. Emotet ist ebenfalls im Unternehmensumfeld aktiv und dort mit 15 Prozent der am zweithäufigsten für Angriffe genutzte Banking-Trojaner.

Kaspersky-Tipps zum Schutz gegen Finanzattacken

Um sich vor neuen wie alten Formen finanzieller Cybermalware zu schützen, empfehlen die Kaspersky-Experten privaten Nutzern,

- Sicherheitsupdates immer so rasch wie möglich zu installieren,
- niemals Software von unbekannten Quellen herunter zu laden und diese Option bei mobilen Geräten explizit abzuschalten,
- die von Apps eingeforderten Zugriffsrechte zu überprüfen und gegebenenfalls beim Anbieter nachzufragen,
- niemals Links in Spam-Messages anzuklicken und angehängte Dokumente bei unbekannten E-Mails zu öffnen,
- starke und vor allem einzigartige Passwörter für jeden Account zu nutzen (mindestens 16 Stellen und im besten Fall eine Kombination aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen)
- sowie verlässliche Sicherheitssoftware für stationäre sowie mobile Geräte wie Kaspersky Security Cloud [6] zu installieren. Die plattformübergreifende Kaspersky-Lösung bietet adaptiven Sicherheitsservice und schützt automatisch vor Cybergefahren, beispielsweise sensiblen Zahlungstransaktionen.

Im Unternehmen sollten

- regelmäßig Mitarbeiter-Schulungen zu Fragen der Cybersicherheit [7] durchgeführt werden.
- eingesetzte Software immer auf dem aktuellen Stand gehalten werden,
- die Installation von beliebiger Software durch Mitarbeiter unterbunden werden,
- der Einsatz fortschrittlicher Lösungen wie Kaspersky Endpoint Detection and Response [8] oder Kaspersky Fraud Prevention gesichert sein, um Betrugsversuche in Echtzeit zu erkennen und verhindern zu können;
- Threat Intelligence [9] in das Security Information and Event Management (SIEM) integriert sein.

[1] https://securelist.com/financial-threats-in-h1-2019/91899/

[2] https://securelist.com/spam-and-phishing-in-q1-2019/90795/

[3] https://www.kaspersky.com/resource-center/threats/zeus-virus/

[4] https://www.kaspersky.com/about/press-releases/2019_rtm-banking-trojan-targeting-businesses-hits-more-than-130000-users-in-2018-and-continues-to-attack

[5] https://threats.kaspersky.com/en/threat/Trojan-Banker.Win32.Emotet/

[6] https://www.kaspersky.de/security-cloud

[7] https://www.kaspersky.de/enterprise-security/security-awareness

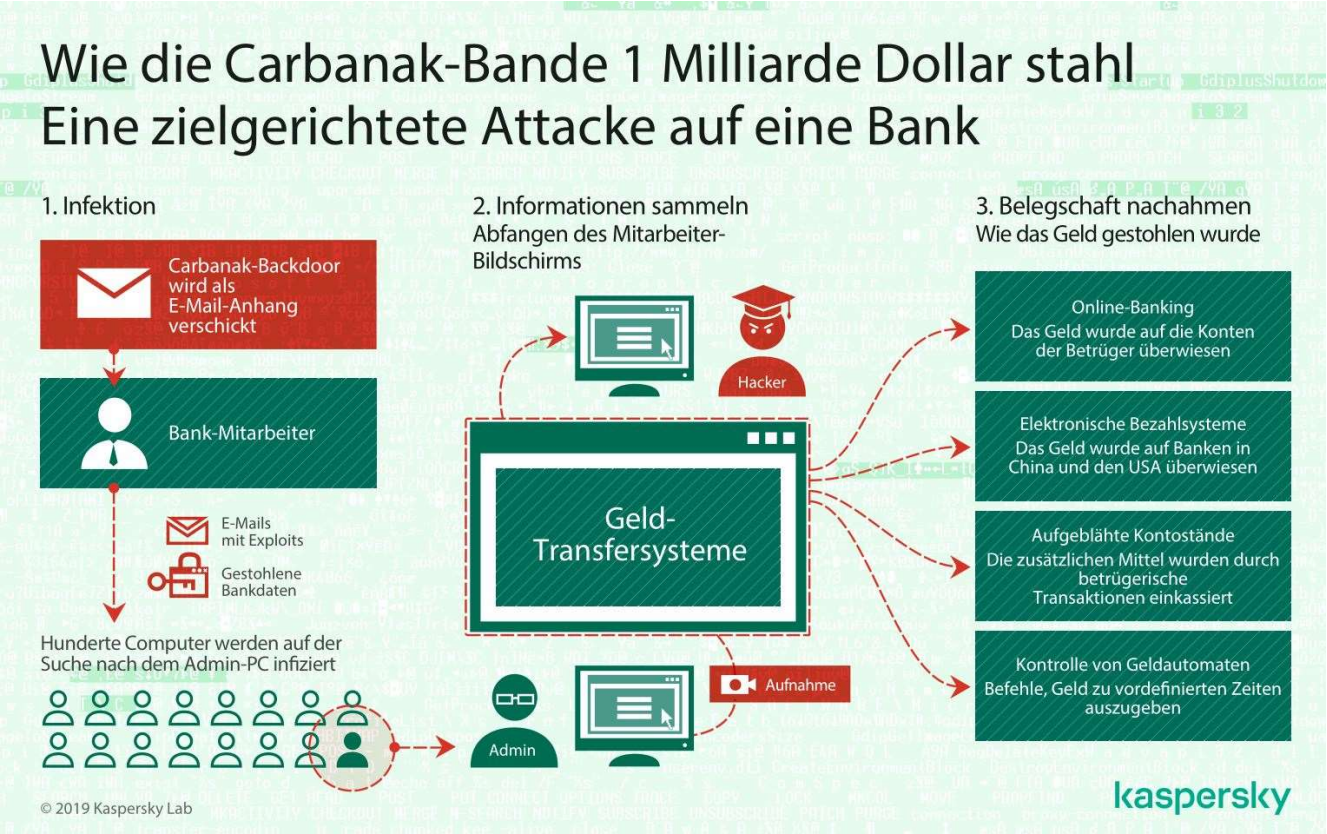
[8] https://www.kaspersky.de/enterprise-security/endpoint-detection-response-edr

[9] https://www.kaspersky.de/enterprise-security/threat-intelligence

Teil 2: Die spezifischen Gefahren und Lösungen für Banken

Carbanak – eine Chronologie der berüchtigten Cyberräuber

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. Die Analyse von damals ist inklusive einem Video und Infografiken unter https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/ verfügbar.



Ein Jahr später (8. Februar 2016) veröffentlichten die Cybersicherheitsexperten von Kaspersky 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: https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

Im April 2019 wurde bekannt, dass der Quellcode des berüchtigten Carbanak-Trojaners bereits vor zwei Jahren auf VirusTotal [https://www.virustotal.com/de/] 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 von Kaspersky 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: https://www.kaspersky.de/about/press-releases/2019_in7-gruppe

Die Einschätzung des Experten

„Die Tatsache, dass der Quellcode der berüchtigten Carbanak-Malware auf einer Open-Source-Website verfügbar war, ist ein schlechtes Zeichen. Tatsächlich wurde die Carbanak-Malware selbst zunächst auf dem Quellcode der Carberp-Malware aufgebaut, nachdem sie online veröffentlicht wurde. Wir haben allen Grund zu der Annahme, dass sich dieses Szenario nun wiederholen wird und wir uns in Zukunft mit gefährlichen Modifikationen von Carbanak konfrontiert sehen werden. Die gute Nachricht ist, dass sich die Cybersicherheitsbranche seit dem Carberp-Leck stark weiterentwickelt hat und den geänderten Code heute leicht erkennen kann. Wir fordern Unternehmen und Einzelpersonen auf, sich gegen diese und zukünftige Bedrohungen mit einer robusten Sicherheitslösung zu schützen."

Sergey Golovanov, Sicherheitsforscher bei Kaspersky

Die Lazarus-Gruppe

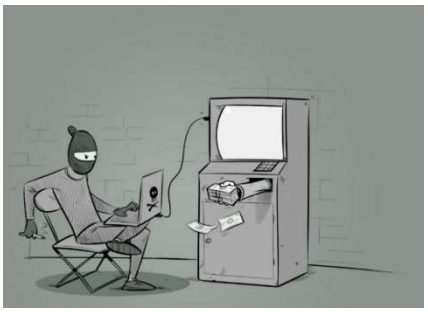
Kaspersky hat im April 2017 eine einjährige Untersuchung zu der so genannten Lazarus-Gruppe veröffentlicht. Die Hackergruppe wird für den Diebstahl von 81 Millionen US-Dollar von der Zentralbank in Bangladesch im Jahr 2016 verantwortlich gemacht. Über eine forensische Analyse von Artefakten, die die Gruppe in den Systemen südostasiatischer und europäischer Banken hinterlassen hatte, konnte Kaspersky tiefe Einblicke darüber gewinnen, welche Werkzeuge die Gruppe verwendet und wie ihre Angriffe auf Finanzinstitutionen, Spielcasinos, Software-Entwickler für Anlagegesellschaften sowie Unternehmen im Kryptowährungsbereich weltweit ablaufen. Mit Hilfe dieser Erkenntnisse wurden mindestens zwei weitere Operationen und damit der Diebstahl hoher Geldsummen bei Finanzinstituten vereitelt. Laut den Erkenntnissen von Kaspersky ist die Gruppe nach wie vor aktiv: https://www.kaspersky.de/about/press-releases/2017_jadg-auf-lazarus-gruppe-verhindert-groben-cyberbankuberfall

Neue Gefahr: Digitale Doppelgänger

Im April 2019 veröffentlichte Kaspersky die Ergebnisse einer weiteren Untersuchung des im Darknet angesiedelten Untergrund-Online-Shops ‚Genesis'. Auf der Plattform werden mehr als 60.000 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 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 maschinelle Lernmethoden zusammen: https://securelist.com/digital-doppelgangers/90378/ und https://www.kaspersky.de/about/press-releases/2019_perfide-kartenbetrugsmasche

Angriffe auf Geldautomaten (ATMs) – eine Chronologie der Kaspersky-Entdeckungen

Kaspersky beobachtet seit Jahren mögliche Angriffsvektoren auf Geldautomaten. Seit Carbanak ist klar: die Bedrohung ist nicht nur real, sondern für Banken ein riesiges Problem. Wie Cyberkriminelle mit und ohne Malware ATMs angreifen, beschreibt eine Kaspersky-Analyse aus 2016 sehr detailliert: https://de.securelist.com/malware-and-non-malware-ways-for-atm-jackpotting-extended-cut/71316/



Ein Malware-Vertreter, der sich explizit gegen Geldautomaten richtet ist die **Malware ATMitch**. Eine Analyse von Kaspersky (April 2017) zeigte folgenden Fall: Als Bankangestellte einen ausgeraubten Geldautomaten vorfanden ohne erkennbare Spuren physischer Gewaltanwendung oder Malware, standen sie vor einem Rätsel. Die Experten von Kaspersky konnten in einer zeitaufwendigen Untersuchung die Vorgehensweise der Cyberkriminellen aufdecken: es handelte sich um einen ‚fileless' Einbruch ins Banknetzwerk. Damit ließ sich der Geldautomat in Sekundenschnelle und ohne wirklich nachzuverfolgende Spuren ausrauben: https://www.kaspersky.de/about/press-releases/2017_cyberbankuberfall-40-erst-dateiloser-bankeinbruch-dann-spurlose-plunderung-von-geldautomaten

Weitere aktuelle Vorfälle in puncto Geldautomaten seit dem Jahr 2018:

- 2019: https://securelist.com/criminals-atms-and-a-cup-of-coffee/91406/
- 2019: https://securelist.com/atm-robber-winpot/89611/
- 2018: https://securelist.com/koffeymaker-notebook-vs-atm/89161/
- 2018: https://securelist.com/atm-malware-from-latin-america-to-the-world/83836/

Kaspersky Finance Services Cybersecurity – das Lösungsportfolio für Finanzinstitute

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.

Das mehrstufige Schutzkonzept Finance Services Cybersecurity von Kaspersky hilft Unternehmen in der Finanz- und Bankenbranche bei der Implementierung einer flexiblen Sicherheitsstrategie: https://www.kaspersky.de/enterprise-security/finance

Die Bausteine hierfür sind:

- Erkennung und Risikominimierung bei zielgerichteten Angriffen und technologisch fortschrittlichen Bedrohungen durch Erkennung unterschiedlichster Kompromittierungsvektoren:https://www.kaspersky.de/enterprise-security/resources/white-papers

- Umfassende Sicherung von Endpoints und Embedded-Geräten wie Geldautomaten und Kassensystemen sowie anderen, am Point-of-Sale eingesetzten Technologien: https://www.kaspersky.de/enterprise-security/embedded-systems

- Kaspersky Hybrid Cloud Security bietet Sicherheit für virtuelle und physische Server, VDI-Bereitstellung, Speichersysteme und sogar Datenkanäle in Private Clouds sowie erweiterten Workload-Schutz in Public Clouds: https://www.kaspersky.de/enterprise-security/cloud-security

- Kaspersky Threat Intelligence ermöglicht detaillierte Einblicke in die von Cyberkriminellen eingesetzten Taktiken und Tools. Aussagekräftige Bedrohungsdaten, fortschrittliche Machine-Learning-Technologien und ein

einzigartiger Pool weltweit agierender Experten hilft dabei, die Immunität von Banken und Finanzdienstleistern auch gegen bisher unbekannte Cyberangriffe aufrechtzuerhalten: https://www.kaspersky.de/enterprise-security/threat-intelligence

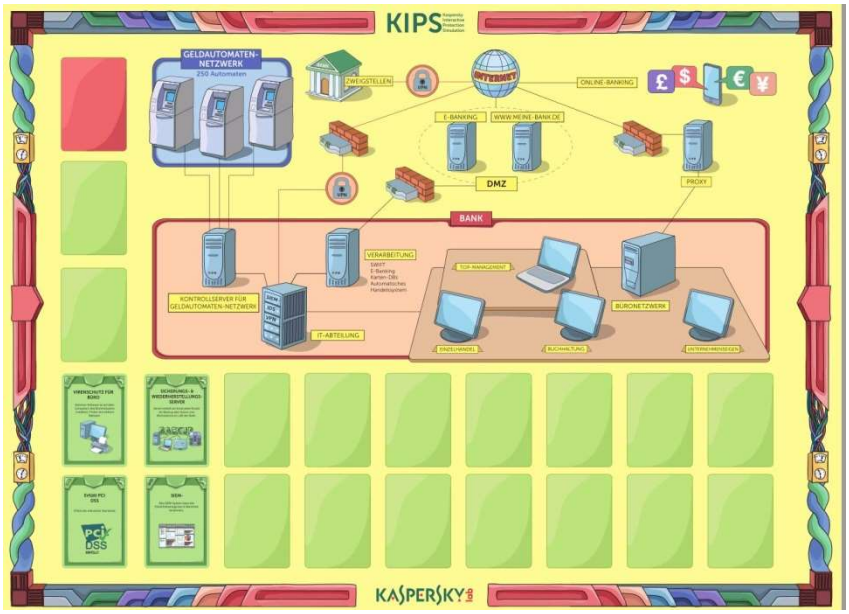
Kaspersky Security Awareness unterstützt dabei zusätzlich bei der Entwicklung einer sicheren Cyberumgebung in Unternehmen. Denn mehr als 80 Prozent aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. Klassische Schulungsprogramme sind häufig nicht geeignet, Mitarbeitern die erforderlichen Verhaltensänderungen und die nötige Motivation vermitteln zu können. Kaspersky hat deshalb eine Reihe von computerbasierten Schulungsprodukten auf den Markt gebracht, die auf den neuesten Lerntechniken basieren und an sämtliche Unternehmensebenen gerichtet sind: https://www.kaspersky.de/enterprise-security/security-awareness

Kaspersky Interactive Protection Simulation

Kaspersky Interactive Protection Simulation (KIPS) ist ein Übungsszenario, bei dem IT-Sicherheitsteams aus Unternehmen und Behörden im Rahmen eines Planspiels in eine simulierte Geschäftsumgebung versetzt werden, in der sie einer Reihe unerwarteter Cyberbedrohungen ausgesetzt werden, während die Teams versuchen, den Gewinn zu maximieren und das Vertrauen der Kunden zu erhalten.

Die Idee besteht darin, durch Auswahl der besten verfügbaren vorausschauenden und reaktionsschnellen Kontrollmöglichkeiten eine Cyberverteidigungsstrategie zu entwickeln. Jede Reaktion der Teams auf die eintretenden Ereignisse verändert den Verlauf des Szenarios und damit den Gewinn bzw. den Verlust des Unternehmens.

Mit einem ausgewogenen Verhältnis von Entwicklungs-, geschäftlichen und Sicherheitsprioritäten sowie den Kosten eines realistischen Cyberangriffs analysiert das Team Daten und trifft strategische Entscheidungen auf Basis unsicherer Informationen und begrenzter Ressourcen. Dieser Realitätsgrad ist beabsichtigt, da alle Szenarien auf realen Ereignissen basieren.



BU – Bankszenario bei KIPS: Schutzmaßnahmen von Finanzinstitutionen vor neuen, übergeordneten APTs wie Tyukpin und Carbanak sind hier gefragt.

[1] https://www.heise.de/newsticker/meldung/Eine-Milliarde-Euro-Beute-mit-Malware-Carbanak-und-Cobalt-Polizei-schnappt-mutmasslichen-4005558.html und https://de.wikipedia.org/wiki/Carbanak

kaspersky

Teil 3 - Kaspersky-Prognosen Cyberbedrohung im Finanzbereich

Ende 2018 prognostizierten die Kaspersky-Experten die folgenden Cyberbedrohungsprognosen für den Finanzbereich:

Erste Attacken mit Hilfe gestohlener biometrischer Daten

Biometrische Systeme zur Nutzererkennung und -authentifizierung werden bereits von verschiedenen Finanzunternehmen eingeführt und verwendet. Doch auch erste bedeutende Schwachstellen haben sich bereits gezeigt [10]. Diese beiden Tatsachen haben bereits zu ersten Proof-of-Concept-Angriffen auf Finanzdienstleister mit Hilfe gestohlener biometrischer Daten geführt.

Neue Angriffe auf Kreditinstitute und Finanzbehörden

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.

Supply-Chain-Attacken gehen weiter

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.

Cyberkriminalität umgeht Anti-Fraud-Lösungen

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, so dass 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.

Fortschrittliche Social-Engineering-Kampagnen

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 Emails 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 werden und der Zugriff auf dessen Konten deutlich vereinfacht.

[10] https://www.heise.de/security/meldung/Sicherheitsforscher-kritisieren-Standard-fuer-passwortloses-Login-4169294.html

www.kaspersky.de
www.securelist.com