Der große Bankraub: Cybergang „Carbanak“ stiehlt eine Milliarde US-Dollar von 100 Finanzinstituten weltweit

Unter den Opfern sind auch Organisationen aus Deutschland und der Schweiz

Moskau/Ingolstadt, 15. Februar 2015

Kaspersky Lab, INTERPOL, Europol und Institutionen verschiedener Länder haben gemeinsam die Geschichte eines beispiellosen Cyber-Bankraubs aufgedeckt. Dabei wurde bis zu eine Milliarde US-Dollar innerhalb von zwei Jahren von Finanzinstituten weltweit gestohlen. Laut den Experten ist eine internationale Gang von Cyberkriminellen aus Russland, der Ukraine, Teilen Europas sowie China für den Raubzug verantwortlich.

Die so genannte „Carbanak“-Gang nutzte für die Cyberüberfälle Techniken aus dem Arsenal zielgerichteter Attacken. Der Vorgang markiert den Beginn einer neuen Phase in der Entwicklung der Cyberkriminalität, in der Geld direkt von Banken, anstatt von Heimanwendern gestohlen wird.

Seit dem Jahr 2013 haben die Kriminellen Angriffe auf bis zu 100 Banken, E-Payment-Systeme und andere Finanzinstitute in rund 30 Ländern gestartet. Die Attacken sind noch aktiv. Entsprechend den Informationen von Kaspersky Lab liegen die Carbanak-Ziele in Deutschland und in der Schweiz sowie in Russland, den USA, China, Ukraine, Kanada, Hong Kong, Taiwan, Rumänien, Frankreich, Spanien, Norwegen, Indien, Großbritannien, Polen, Pakistan, Nepal, Marokko, Island, Irland, Tschechien, Brasilien, Bulgarien und Australien [1]. .

Es ist davon auszugehen, dass die größten Summen durch das Hacken von Banken erbeutet wurden – bis zu zehn Millionen US-Dollar pro Überfall. Im Durchschnitt dauerte jeder Banküberfall zwischen zwei und vier Monate an, von der Infizierung des ersten Computers im Unternehmensnetzwerk der Bank bis zum eigentlichen Diebstahl.

Kontrolle über Überwachungskameras und Geldtransfersysteme

Anfangs haben sich die Cyberkriminellen über gezielte Spear-Phishing-Attacken Zugang zu einem Angestellten-Computer verschafft und diesen mit dem Carbanak-Schadprogramm infiziert. Anschließend waren sie in der Lage, sich im internen Netzwerk zu bewegen, um die für die Videoüberwachung zuständigen Computer der Administratoren aufzuspüren und zu übernehmen. Die Folge: Die Angreifer konnten alles, was sich auf den Bildschirmen der für die Betreuung der Geldtransfersysteme verantwortlichen Mitarbeiter abspielte, einsehen und aufnehmen. So kannten sie

jedes einzelne Detail über die Arbeit der Angestellten und konnten die Aktivitäten der Angestellten imitieren, um Geld zu überweisen oder bar auszuzahlen.

Wie das Geld gestohlen wurde

Die Carbanak-Gang nutzte mehrere Methoden, um die Banken auszurauben [2]:

1. Sobald die Betrüger aus ihren Aktivitäten Kapital schlagen wollten, nutzen sie Online-Banking- oder internationale E-Payment-Systeme, um Geld von den Konten der Bank auf die eigenen Konten zu überweisen. Zum Teil wurde das gestohlene Geld auch bei Banken in China oder Amerika hinterlegt. Die Experten schließen nicht aus, dass weitere Banken und Länder ebenfalls als Empfänger genutzt wurden.

2. In anderen Fällen sind die Cyberkriminellen direkt in das Herz der Buchhaltungssysteme eingedrungen, um Kontensaldi zu erhöhen und im Anschluss die überschüssigen Geldmittel durch eine Überweisung zu entwenden. Ein Beispiel: Liegen auf einem Bankkonto 1.000 US-Dollar, erhöhen die Kriminellen den Saldo auf 10.000 US-Dollar und überweisen im Anschluss 9.000 US-Dollar auf eigene Konten. Der Kontoinhaber vermutet keine Probleme, weil auf seinem Konto nach wie vor 1.000 US-Dollar liegen.

3. Darüber hinaus hatten die Cyberräuber Kontrolle über die Geldautomaten der Banken und konnten diese anweisen, Bargeld zu einer vorbestimmten Zeit auszuzahlen. Zum Zeitpunkt der Auszahlung wartete ein Handlanger der Gang am betroffenen Geldautomaten und kassierte die Auszahlung ein.

„Das Überraschende an diesen Banküberfällen war, dass es den Kriminellen egal war, welche Software die Bank nutzte. Daher sollten Banken sich nicht in Sicherheit wiegen, selbst wenn sie eine einzigartige Software verwenden. Die Angreifer mussten nicht einmal die Services der Bank hacken. Sobald sie ein Netzwerk geentert hatten, lernten sie, ihren gefährlichen Komplott hinter legitimen Aktionen zu verstecken. Alles in allem ein sehr geschickter und professioneller Cyberraub“, so Sergey Golovanov, Principal Security Researcher beim Global Research und Analysis Team von Kaspersky Lab.

„Diese Attacken unterstreichen wieder einmal, dass Kriminelle jede Schwachstelle in jedem System ausnutzen werden. Klar wird zudem: Es gibt keine Branche, die immun gegen Attacken ist. Sicherheitsabläufe müssen ständig überprüft werden. Das Identifizieren von neuen Trends im Bereich Cyberkriminalität ist ein Schlüsselbereich, in dem INTERPOL mit Kaspersky Lab zusammenarbeitet, um sowohl den öffentlichen als auch den privaten Sektor beim Schutz vor aufkommenden Gefahren besser helfen zu können“, sagt Sanjay Virmani, Director des INTERPOL Digital Crime Centre.

Kaspersky Lab rät allen Finanzorganisationen dazu, ihre Netzwerke sorgfältig nach einer Präsenz von Carbanak zu prüfen. Bei einem Fund sollten umgehend die Strafverfolgungsbehörden eingeschaltet werden.

Weitere Details zur Carbanak-Operation werden in den kommenden Tagen unter http://viruslist.com/de/ abrufbar sein.

[1] siehe Grafik
http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KL_infographic_carbanak_map_of_targets.png

[2] siehe Grafik http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KL_inographic_carbanak_how_the_money_was_stolen.png

Nützliche Links:

- Infografik “How the money was stolen”: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KL_inographic_carbanak_how_the_money_was_stolen.png
- Infografk: “Map of Carbanak targets”: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KL_infographic_carbanak_map_of_targets.png
- Infografik: “Traces of the infection”: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KL_infographic_traces_of_carbanak.png
- Kaspersky Fraud Prevention: http://www.kaspersky.com/de/business-security/fraud-prevention
- Kaspersky-Prognose Überfälle auf Banken: http://www.viruslist.com/de/analysis?pubid=200883875#p1
- Pressemitteilung “Kaspersky-Report zu finanziellen Cyberbedrohungen“: http://newsroom.kaspersky.eu/de/texte/detail/article/version-deutschland-fast-jede-zweite-phishing-attacke-auf-deutsche-nutzer-zielt-auf-finanzdaten
- Pressemitteilung „Virtuelle Banküberfälle”: http://newsroom.kaspersky.eu/de/texte/detail/article/virtuelle-bankueberfaelle-attacken-auf-apple-angebote-und-das-internet-der-unsicheren-dinge

Über Kaspersky Lab

Kaspersky Lab ist der weltweit größte privat geführte Anbieter von Endpoint-Sicherheitslösungen. Das Unternehmen zählt zu den vier erfolgreichsten Herstellern von Sicherheitslösungen für Endpoint-Nutzer. In seiner über 17-jährigen Unternehmensgeschichte hat Kaspersky Lab zahlreiche Innovationen im Bereich IT-Sicherheit auf den Weg gebracht und bietet effektive digitale Sicherheitslösungen für Großunternehmen, KMU und Heimanwender. Kaspersky Lab, mit Holding in Großbritannien, ist derzeit in rund 200 Ländern auf der ganzen Welt vertreten und schützt über 400 Millionen Nutzer weltweit.*

Weitere Informationen zu Kaspersky Lab finden Sie unter http://www.kaspersky.com/de/. Kurzinformationen erhalten Sie zudem über www.twitter.com/Kaspersky_DACH und www.facebook.com/Kaspersky.Lab.DACH. Aktuelles zu Viren, Spyware, Spam sowie Informationen zu weiteren IT-Sicherheitsproblemen und -Trends sind unter www.viruslist.de und auf dem Kaspersky-Blog auf http://blog.kaspersky.de/ abrufbar.

** The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.*

Redaktionskontakt:

essential media GmbH
Florian Schafroth
florian.schafroth@essentialmedia.de
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-17
Landwehrstraße 61
80336 München

Kaspersky Labs GmbH
Stefan Rojacher
stefan.rojacher@kaspersky.com
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100
Despag-Straße 3
85055 Ingolstadt

© 2015 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.