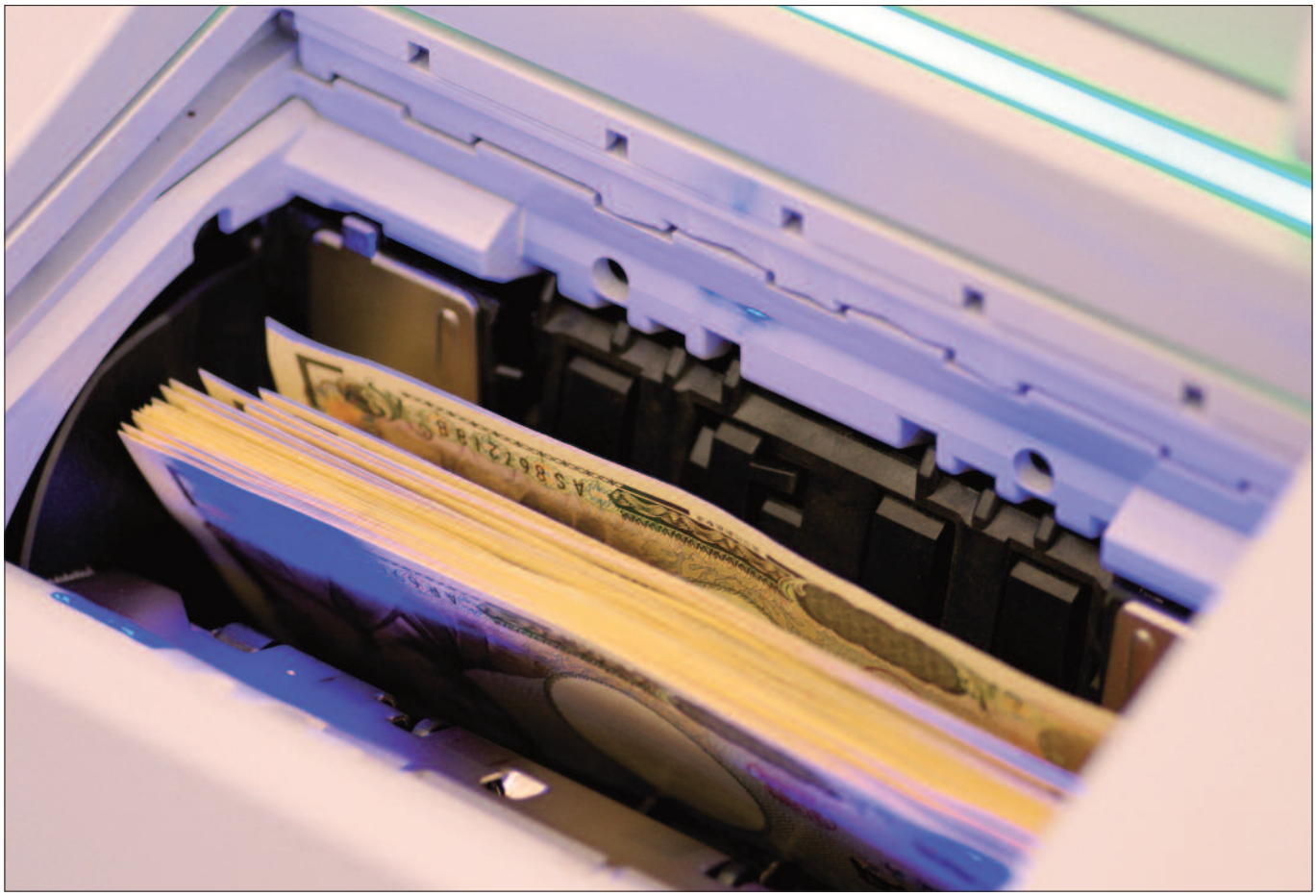

Angriffe auf Geldautomaten: Die Täter manipulieren die Automaten zur Herausgabe von Banknoten mithilfe eines Befehlscodes, der über die Tastatur des Automaten eingegeben wird, oder mit Schadprogrammen.

Online-Angriffe auf Geldautomaten

Laut dem Softwarehersteller *Kaspersky Lab* sollen Banken, Geldautomaten und Online-Bezahlsysteme 2015 vermehrt ins Visier von Cyber-Kriminellen geraten.

Während es Cyber-Kriminelle bisher vor allem auf Online-Banking-Nutzer abgesehen haben, wird es nach Einschätzung von *Kaspersky Lab* 2015 vermehrt zu Cyber-Angriffen auf die Banken selbst kommen. Zudem geht *Kaspersky Lab* in seinem *Security Bulletin 2014/2015* davon aus, dass Schadprogramme entwickelt werden, die eine Manipulation von Geldautomaten ermöglichen. 2015 sollen auch *Apple*-Geräte vermehrt angegriffen werden sowie mit dem Internet verbundene Geräte – beispielsweise Netzwerkdrucker, über die Kriminelle in Unternehmensnetzwerke eindringen können.

Betrüger manipulierten Geldautomaten bisher mit Kartenlesern, gefälschten Tastaturen und versteckten Videokameras. Auf den Kartenschlitz wurde meist ein zweites Gerät aufgesteckt, das die EC- oder Kreditkartendaten auslas. Über die Videokamera kamen die Betrüger an die Geheimzahl. „In letzter Zeit haben wir eine Zunahme von Angriffen auf Geldautomaten mit Schadsoftware beobachtet“, berichtet Vincente Diaz, Sicherheitsexperte bei *Kaspersky Lab*. Wir raten Banken dringend, die physische Sicherheit ihrer Geldautomaten sowie die Netzwerk-Infrastruktur zu überprüfen und in hochqualitative Sicherheitslösungen zu investieren.“

Trojaner in Geldautomaten. Die erste bekannte Schadsoftware für Geldautomaten wurde „Backdoor.Win32.Skimer“ genannt. Die Schadsoftware speicherte die PIN und die Kartendaten. Die Kriminellen konnten die gespeicherten Daten auf Blankokarten kopieren. Der Hersteller der betroffenen Geldautomaten deaktivierte den Trojaner mit einem Softwareupdate. Die Schadsoftware war nur auf Geldautomaten zu finden, die *Windows XP* als Betriebssystem hatten. Geldautomaten sind meist an geschlossene, interne Netzwerke angeschlossen, auf die von außen kein Zugriff möglich ist. Jeder Versuch, ein solches Gerät zu öffnen und es zu manipulieren, wird normalerweise von Sensoren aufgedeckt. Laut Software-Experten sei die Einschleusung der Schadsoftware mit einem direkten Zugriff auf die Geldautomaten erfolgt und nicht über das Netzwerk. Das sei nur mit Hilfe von Insidern möglich gewesen oder die Schadsoftware sei bereits bei der Herstellung des Geldautomaten installiert worden.

Seit Dezember 2010 treibt der in Brasilien entwickelte Trojaner „Trojan-Spy.Win32.SPSniffer“ sein Unwesen.

FOTO: SHIMA-RISU/FOTOLIA

Angriffe auf Apple-Computer: Schädliche Apple-Programme werden über Torrent-Netze und als Kopien verteilt.

Auch er wird an älteren Geldausgabegeräten angewendet, die über eine USB-Schnittstelle verfügen. Die Kriminellen gelangten an die Kartendaten und PINs, indem sie die Schadsoftware mit USB-Sticks auf das Gerät brachten. Zwar wird die PIN verschlüsselt, doch der Trojaner schöpft am infizierten Rechner die restlichen Kreditkarten-Daten ab, die dann von Cyber-Kriminellen auf gefälschte Blankokarten kopiert werden können.

Ploutus und Tyupkin. 2013 trat in Mexiko erstmals die Schadsoftware „Ploutus" auf. Mittlerweile wurde auch in den USA eine englischsprachige Version der Schadsoftware entdeckt. Den Kriminellen muss es gelungen sein, den Trojaner mit einer CD auf Geldautomaten zu installieren. „Ploutus" weist die Automaten zur Herausgabe von Banknoten mithilfe eines Befehlscodes an, der über die Tastatur des Automaten eingegeben wird. „Ploutus" errechnet anhand der Anzahl der vorhandenen Scheine in den Geldkassetten den maximal auszahlbaren Geldbetrag und gibt ihn nach und nach aus, bis der Automat leer ist. Die neueste Version von „Ploutus" kann den Geldautomaten sogar mit einer SMS dazu bewegen, Geld in den Ausgabeschacht zu transportieren. Dazu muss ein Mobiltelefon mit einer der internen USB-Schnittstellen verbunden werden.

Kaspersky-Experten entdeckten eine weitere Schadsoftware namens „Tyupkin", mit der die Angreifer Automaten infizierten und ausräumten. Zuerst verschafften sie sich Zugriff zum System des Geldautomaten und legten eine bootfähige CD ein, die die Schadsoftware „Tyupkin" installierte. Nachdem sie das System neu gestartet hatten, befand sich der infizierte Bankautomat unter der Kontrolle der Angreifer. Damit die Manipulation schwerer zu erkennen war, stahlen die Kriminellen Geld aus den infizierten Automaten nur zu bestimmten Zeiten: entweder am Sonntag oder am Montag in der Nacht.

Vorgangsweise der Täter. Videoaufnahmen aus Überwachungskameras an den infizierten Geldautomaten zeigen die Methoden, mit denen die Kriminellen an das Bargeld gelangten. Für jede „Sitzung" wird zunächst eine einzigartige Kombination aus zufälligen Zahlen generiert. Damit wird sichergestellt, dass niemand außerhalb der kriminellen Gruppe versehentlich von dem Betrug profitiert. Anschließend erhält der Täter, der den Diebstahl ausführt, Anweisungen über das Telefon von einem anderen Mitglied der Gruppe. Er kennt den Algorithmus und ist in der Lage, einen Schlüssel für die jeweilige Sitzung auf Basis der angezeigten Nummern zu generieren. Dies stellt sicher, dass die Personen, die das Bargeld stehlen, nicht im Alleingang handeln. Wenn der Schlüssel korrekt eingegeben wurde, zeigt der Geldautomat an, wie viel Bargeld in jeder Geldkassette ist, und fordert die ausführende Person auf, eine Kassette zu wählen. Danach gibt der Geldautomat jeweils 40 Banknoten von der ausgewählten Kassette aus. Die Schadsoftware wurde bisher in Geldautomaten in Europa, Lateinamerika und Asien verwendet.

Banküberfall 2.0. „Wir erwarten 2015 eine Weiterentwicklung bei Angriffen gegen Geldautomaten, die es auf das Herz der Geldautomaten abgesehen haben", sagt Alexander Gostev von *Kaspersky Lab*. „Im nächsten Schritt werden Angreifer Netzwerke von Banken kompromittieren und dadurch Geldautomaten in Echtzeit manipulieren." Gelingt es Angreifern, in das Netzwerk einer Bank einzudringen, können sie mit den erlangten Informationen Geld stehlen. Die Methoden dazu sind Bargeldauszahlung über Befehle aus der Ferne an Geldautomaten, SWIFT-Geldüberweisungen über verschiedene Kundenkonten sowie Manipulation von Online-Banksystemen für Überweisungen im Hintergrund.

Mac-Angriffe. Schädliche Apple-Programme werden über Torrent-Netze und als Kopien verteilt. Das standardmäßig geschlossene *Mac*-System macht es Schadprogrammen schwerer, *Apple*-Computer zu kompromittieren. Es gibt jedoch viele Nutzer, die die Sicherheitsmaßnahmen von *Mac OS X* ausschalten – vor allem, wenn sie dort Raubkopien verwenden. Das bedeutet, dass Kriminelle, die aus verschiedenen Gründen *OS-X*-Systeme infizieren wollen, wissen, dass sie ihre schädlichen Machwerke nur mit einer bestimmten Software verknüpfen müssen, etwa in Form von Key-Generatoren, um die Schädlinge erfolgreich verbreiten zu können. Dank des immer noch weit verbreiteten Glaubens an die Sicherheit der *OS-X*-Plattform ist auf diesen Systemen oft keine Antivirus-Software installiert, die eine Infizierung verhindern könnte. Schädlinge bleiben auf den *Macs* lange unentdeckt und können unbehelligt ihre Aktivitäten ausführen.

Virtuelle Zahlungssysteme. Da die Beliebtheit virtueller Zahlungssysteme steigt, erwarten Sicherheitsexperten, dass Cyber-Kriminelle sie missbrauchen werden. Sie legen Anwender mit Social-Engineering-Tricks herein, greifen Handys an oder hacken Banken. Diese Gefahr besteht auch für das Bezahlsystem *Apple Pay,* das NFC (Near Field Communication) für drahtlose Transaktionen nutzt.

Siegbert Lattacher

FOTO: MARIA REINHOFER-ELBE