Digitales Stalking >
< Riskante Spiele-Apps

Cyber-Betrugsmasche „Jackpotting“

Geldautomaten im Visier von Hackern

Ähnlich wie ein Glücksspielautomat, spucken infizierte Automaten den Tätern (fast) ihren kompletten Geldvorrat aus

Um möglichst unerkannt an große Summen Bargeld zu gelangen, lassen sich Kriminelle immer wieder neue Tricks einfallen. Eine ihrer neueste Maschen nennt sich „Jackpotting“. Dabei gelingt es den Tätern, Schadsoftware auf Geldautomaten aufzuspielen und diese im großen Stil leerzuräumen. Allein in Berlin kam es im Jahr 2019 zu rund 50 Fällen. PolizeiDeinPartner sprach mit Oliver Klau, Dezernatsleiter im Bereich Cybercrime beim Landeskriminalamt (LKA) Berlin. Er verrät unter anderem, wie die Täter vorgehen und klärt über den aktuellen Stand der Ermittlungen auf.

Geldregen am Bankautomat

An einem Novembermorgen machte sich in München ein Unbekannter an einem Geldautomaten der Stadtsparkasse zu schaffen. Er versuchte, die Verkleidung des Automaten aufzubrechen, um im Inneren an einen der USB-Anschlüsse heranzukommen. Im Kreis Borken (NRW) hat im Dezember ein Täter im Nikolauskostüm einen Geldautomaten der Volksbank geplündert und dabei Bargeld im fünfstelligen Bereich erbeutet. Bei der so genannten „Jackpotting“-Methode werden Geldautomaten zunächst aufgebrochen und anschließend mithilfe einer Software so manipuliert, dass sie – wie bei einem Jackpot an einem Glücksspielautomaten – fast ihren gesamten Geldbestand ausspucken. „Jackpotting ist so gesehen eine technische Straftat“, bestätigt Oliver Klau vom LKA Berlin. „Die Täter greifen Geldautomaten von Kreditinstituten, aber auch von Zahlungsdienstleistern, an und sorgen dafür, dass

diese Automaten ihren Bargeldbestand teilweise oder sogar vollständig widerrechtlich auszahlen.“

Jeder Automat ist ein Computer

Die grundsätzliche Vorgehensweise der Täter ist immer gleich: Durch mechanische Einwirkung verschaffen sie sich zunächst gewaltsam Zugriff auf den Rechner, der sich im Inneren des Geldautomaten befindet. „Man muss dazu wissen, dass hinter jedem Automatenkorpus ein ganz normaler Computer steckt, der dessen Funktionen steuert und mit der jeweiligen Bank kommuniziert“, erklärt Oliver Klau. Das Geld sei zusätzlich durch einen Tresor geschützt. „Gelangen die Täter jedoch an den Computer im Inneren des Automaten, manipulieren sie diesen so, dass die Auszahlungseinheit das Geld aus diesem Tresor herausholt und ausspuckt.“ Dabei passen sich die Kriminellen immer den neusten technischen Entwicklungen an. „Die Täter gehen nicht wahllos an jeden beliebigen Automaten ran“, weiß der LKA-Experte. „Sie wissen relativ genau, bei welchem Automatentyp welche Schwachstellen vorliegen und picken sich gezielt Geräte raus, wo die Ausbeute erfolgversprechend ist.“ Ein manipulierter Automat lässt sich zum einen daran erkennen, dass er sich ausgeschaltet bzw. in einen Fehlermodus versetzt hat. Wird auf dem Bildschirm eine entsprechende Fehlermeldung angezeigt, sei dies allerdings nur ein potenzieller Hinweis auf einen Angriff. Der Automat könnte genauso gut ein technisches Problem haben oder aus gewöhnlichen Gründen leer sein. Ein sichereres Indiz seien sichtbare Anzeichen, dass der Automat gewaltsam geöffnet wurde, beispielsweise an der Abdeckung.

Der Begriff „Jackpotting“ geht auf den inzwischen verstorbenen neuseeländischen Softwareentwickler und Hacker Barnaby Jack zurück. Er demonstrierte im Jahr 2010 auf einer Konferenz zur Informationssicherheit, wie er eine spezielle Software in einen Geldautomaten einspielte, woraufhin dieser sämtliche Banknoten auswarf.

In Berlin wurde im vergangenen Jahr mit rund 50 Jackpotting-Fällen eine große Anzahl an Taten festgestellt, die einen deutlichen Schwerpunkt für ganz Deutschland erkennen ließen. Zwar waren die Angriffe nicht in jedem Fall erfolgreich, dennoch sei insgesamt ein Schaden im siebenstelligen Bereich entstanden. „Wir haben daraufhin aus dem LKA Berlin heraus sehr intensive Ermittlungen angestrengt und eine größere international agierende Bande identifiziert, die wir für den Großteil der Berliner Taten verantwortlich machen konnten“, so Klau. „Gegen die Haupttäter der Bande wurden mittlerweile Haftbefehle erlassen und zum großen Teil bereits vollstreckt.“ In der Regel gehen die Täterbanden streng arbeitsteilig vor und sind international sehr gut organisiert. Die Aufgaben sind genau verteilt und jeder Täter geht seiner Spezialisierung nach. Zum Teil werden die Taten auch aus dem Ausland gesteuert. Klau: „Ein Techniker, der international vernetzt ist, informiert sich steht über die aktuellen Sicherungsmaßnahmen der Geldautomaten, ein weiterer Täter kümmert sich um die Logistik, ein anderer sichert die Taten ab – und so weiter. Es findet quasi ein permanenter krimineller Informationsaustausch statt. Und sobald die alte Masche nicht mehr funktioniert, weil die Geldautomaten-Aufsteller dagegen gesteuert haben, versuchen sie, sich neue technische Tricks einfallen zu lassen.“

Oliver Klau, Dezernatsleiter im Bereich Cybercrime beim Landeskriminalamt (LKA) Berlin

Täterbanden agieren arbeitsteilig

Banken können sich schützen

Um Geldautomaten weniger angreifbar für Jackpotting zu machen, kommt es einerseits auf eine gute physische Sicherung der Automaten an. „Eine dünne Blechabdeckung mit einem kleinen Möbelschloss kriegt man sehr leicht auf. Wenn die Täter hingegen richtig an dem Gerät rumhebeln müssen, steigt für sie automatisch die Gefahr, entdeckt zu werden.“ Noch wichtiger sei allerdings, dass die Geldinstitute sowie auch Dienstleister, welche die Automaten aufstellen, regelmäßig die aktuellsten Sicherheitsupdates der Gerätehersteller installieren. Grundsätzlich seien alle ermittelnden polizeilichen Dienststellen in Deutschland in einem sehr engen Austausch mit den Automatenherstellern wie auch den Sicherheitsbeauftragten der Baken, um genau diese Schwachstellen abzuschaffen. „Wie bei den meisten Straftaten wird man Jackpotting-Angriffe niemals zu 100 Prozent verhindern können“, resümiert Oliver Klau. Man kann es den Tätern aber sehr schwer machen.“
KF (31.01.2020)

Folgende Artikel könnten Sie auch interessieren:

- Manipulierte Geldautomaten
- Die neue Abteilung Cybercrime im BKA
- Mobile Fraud: Vorsicht vor gefälschten Apps
- IT-Sicherheit im Unternehmen

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Internet und Mobil

Wie gut schützen Cyber-Policen vor Internetkriminalität?

Cyberversicherungen

Wer häufig das Internet nutzt, läuft immer auch Gefahr, Opfer von...[mehr erfahren]

Fakeshops in der Hand von internationalen Täterbanden

Bestellt und nichts geliefert

Die Polizei im Rhein-Sieg-Kreis nahm im Frühjahr 2018 vier Betrüger...[mehr erfahren]

„Für wie viele Likes zieht ihr euch aus?“

Umstrittene Live-Streaming Plattform YouNow

Der neueste Trend aus den USA heißt „YouNow“ – ein Dienst, mit dem...[mehr erfahren]

Wer erbt meine Daten?

Der digitale Nachlass

Seit dem 12. Juli 2018 steht fest, dass Facebook-Konten vererbbar...[mehr erfahren]

Tipps und Links zum sicheren Online-Kauf von Medikamenten

Pillen mit Mausklick – aber sicher!

Der Online-Kauf von Medikamenten wird auch in Deutschland immer...[mehr erfahren]
