NACHRICHTEN AG

23. August 2024

Neue Android-Malware NGate: So schützen Sie Ihr Geld vor Betrügern

ESET deckt gefährliche Android-Malware auf, die Bargeldabhebungen am Geldautomaten ermöglicht. Schützen Sie sich vor Betrug!

Jena (ots)

In der digitalen Welt ist Sicherheit ein wichtiges Thema, das immer wieder ins Rampenlicht rückt. Aktuelle Entwicklungen zeigen, dass Cyberkriminalität eine neue Dimension erreicht hat. ESET-Forscher haben nun eine neuartige Android-Malware entdeckt, die speziell darauf abzielt, Bankdaten von Nutzern auszuspionieren und unautorisierte Geldabhebungen zu ermöglichen.

Die betreffenden Angriffe konzentrieren sich auf Kunden mehrerer tschechischer Banken. Die Malware, bekannt als NGate, verwendet innovative Techniken, um Daten von kontaktlosen Zahlungskarten auszulesen und direkt an die Kriminellen zu übermitteln. Diese Methode, die als NFC-Relay-Technik bezeichnet wird, stellt eine signifikante Bedrohung für die Online-Sicherheit dar und könnte weitreichende Folgen für die Betroffenen haben.

Aufbau und Funktionsweise der Malware

NGate ermöglicht es den Angreifern, die NFC-Daten von Bankkarten zu erfassen. NFC steht für Near Field Communication und beschreibt eine Technologie, mit der Geräte über sehr kurze Distanzen kommunizieren können. Diese Funktion wird häufig

beim kontaktlosen Bezahlen verwendet. In diesem speziellen Fall haben Cyberkriminelle eine bösartige App entwickelt, die unbemerkt auf den Smartphones der Opfer installiert wird. Diese App hat die Fähigkeit, Kartendaten sowie PIN-Nummern auszulesen und an die Angreifer zu übertragen.

Lässt sich ein Geldautomat auf herkömmliche Weise nicht erreichen, haben die Betrüger einen weiteren Plan: Sie können die erbeuteten Gelder direkt auf Konto anderer Banken transferieren. Dies zeigt die vielseitige Gefährlichkeit der NGate-Malware und ihre potenziellen Auswirkungen auf die Finanzen der Opfer.

Der Betrug im Detail

Um an die Installationen der bösartigen Software zu gelangen, bedienen sich die Angreifer bewährter Techniken wie Social Engineering und Phishing. Potenzielle Opfer erhalten betrügerische SMS, die angeblich von ihrer Bank stammen. In diesen Nachrichten wird dringlich empfohlen, eine App herunterzuladen, um angebliche Probleme zu lösen. Wenn die Opfer auf diesen Trick hereinfallen und die App installieren, sind sie dem Zugriff der NGate-Malware hilflos ausgeliefert.

Aktuell konzentrieren sich die Angriffe vor allem auf Kunden von drei großen Banken in Tschechien. ESET hat die Malware erstmals im November 2023 entdeckt, nachdem die Angreifer systematisch gefälschte Nachrichten an zufällig ausgewählte Mobilfunknummern geschickt hatten. Dies bedeutet, dass nicht nur ein spezifischer Personenkreis gefährdet ist, sondern dass potenziell viele weitere Kunden von Banken denselben Risiken ausgesetzt werden können.

Schutzmaßnahmen gegen digitale Bedrohungen

Angesichts dieser neuen Gefahr ist es unerlässlich, dass Nutzer

präventive Maßnahmen ergreifen, um sich zu schützen. Experten empfehlen verschiedene Strategien, um sicherzustellen, dass man nicht Opfer solcher Machenschaften wird:

- Überprüfen Sie Links und Apps gründlich, bevor Sie sie herunterladen oder öffnen.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen wie dem Google Play Store.
- Bewahren Sie Ihre PIN-Nummern geheim und teilen Sie diese niemals über unsichere Kanäle.
- Setzen Sie Sicherheitsanwendungen ein, um Ihr Gerät gegen Schadsoftware abzusichern.
- Deaktivieren Sie die NFC-Funktion, wenn Sie diese nicht brauchen, um unbefugten Zugriff zu erschweren.

Diese präventiven Maßnahmen sind von entscheidender Bedeutung, denn Cyberkriminalität entwickelt sich ständig weiter, und es ist wichtig, wachsam zu bleiben.

Die Bedrohung im digitalen Zeitalter

Die Entdeckung der NGate-Malware verdeutlicht, wie fortschrittlich und raffiniert die Methoden von Cyberkriminellen im 21. Jahrhundert geworden sind. Erkennbar ist, dass diese Malware keine Root-Rechte benötigt, was sie für viele Benutzer gefährlicher macht. Dies könnte eine neue Ära der Cyberkriminalität einläuten, in der immer häufiger Anwendungen verwendet werden, die selbst ohne tiefere Eingriffe in das System funktionieren. Nutzer müssen ständig am Puls der Zeit sein und sich über aktuelle Bedrohungen informieren.

Die Ergebnisse dieser Ermittlungen verdeutlichen die Wichtigkeit von Technologiewissen innerhalb der Gesellschaft und unterstreichen die Notwendigkeit, digitale Sicherheitsstandards ständig zu verbessern.

Hintergrundinformationen zur Cyberkriminalität

In der heutigen digitalisierten Welt hat die Cyberkriminalität stark zugenommen. Die Verbreitung von Smartphones und Online-Banking hat es Kriminellen erleichtert, an persönliche Daten von Nutzern zu gelangen. Besonders in den letzten Jahren haben sich präparierte Apps und Phishing-Techniken weiterentwickelt, und Sicherheitslücken in Betriebssystemen und Anwendungen bieten immer wieder neue Angriffsmöglichkeiten. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind insbesondere Banken und Finanzinstitutionen häufig Ziel solcher Angriffe, da sie oft große Geldbeträge verwalten.

Die NGate-Malware ist ein neues Beispiel für diese gefährlichen Entwicklungen. Kriminelle nutzen nicht nur technische Schwächen aus, sondern kombinieren auch psychologische Manipulationen, um ihre Opfer zu täuschen. Es stellt sich die Frage, wie solche Software entwickelt wird und welche rechtlichen Maßnahmen zur Bekämpfung dieser Cyberbedrohungen vorhanden sind. Cyber-Sicherheitsbehörden in vielen Ländern haben begonnen, diesem Problem aktiv entgegenzuwirken, jedoch bleibt der Bereich der Cyberkriminalität dynamisch und schwer fassbar.

Aktuelle Statistiken zur Cyberkriminalität

Laut einer Studie der europäischen Strafverfolgungsbehörde Europol hat die Cyberkriminalität in Europa in den letzten Jahren erheblich zugenommen. Eine Umfrage des BSI aus dem Jahr 2022 ergab, dass etwa 60 % der Unternehmen in Deutschland von Cyberangriffen betroffen waren oder sich bedroht fühlten. Besondere Aufmerksamkeit erhielt der Bereich des Online-Bankings; über 40 % der Nutzer geben an, bereits einmal Opfer eines Phishing-Angriffs gewesen zu sein.

Zusätzlich zeigt eine Erhebung der Statista, dass im Jahr 2021 weltweit über 30 Milliarden Euro durch Cyberkriminalität verloren gingen, und die Schäden heben sich jedes Jahr um mehrere Prozent. Diese Zahlen verdeutlichen das Ausmaß, in dem solche Betrugsversuche, ähnlich wie die mit der NGate-Malware, in der digitalen Gesellschaft verbreitet sind.

Maßnahmen gegen Cyberkriminalität

Um der wachsenden Bedrohung durch Cyberkriminalität entgegenzuwirken, sind sowohl Nutzer als auch Unternehmen gefordert. Regelmäßige Schulungen über Sicherheitsvorkehrungen und der Einsatz von modernen Sicherheitsmaßnahmen, wie Multifaktor-Authentifizierung, werden empfohlen. Darüber hinaus ist es wichtig, Software aktuell zu halten und regelmäßig Sicherheitsüberprüfungen durchzuführen.

Die koordinierten Maßnahmen von Behörden, wie Interpol und nationalen Cyberabwehrzentren, sind entscheidend zur Bekämpfung solcher Phänomene. Die Schaffung eines globalen Bewusstseins über diese Risiken ist ebenfalls notwendig, um die Benutzer auf potenzielle Gefahren frühzeitig zu sensibilisieren und ihnen Tools an die Hand zu geben, die ihre Geräte und finanziellen Informationen schützen.

Details