F-Alert

Monatliches Threat-Update von

F-Secure

Juni 2023

F-Secure

Lesen Sie die neuesten Threat-Updates. Vollgepackt mit Erkenntnissen der Experten von F-Secure. Jeden Monat neu.

Lesen Sie, wie Sie Ihr digitales Leben im Urlaub absichern können. Erfahren Sie, was Mitarbeiter tun sollten, wenn das Unternehmen, für das sie arbeiten, angegriffen wird. Entdecken Sie, wie man über KI in Begriffen spricht, die jeder versteht. Lernen Sie den neuesten fiesen Android-Malware-Betrug kennen. Und erfahren Sie, warum Sie die Sicherheit von Apple nicht als selbstverständlich ansehen können. Das alles finden Sie in der Sommerausgabe von F-Alert.

Verstöße gefährden Mitarbeiter

Kriminelle nutzen eine Sicherheitslücke in HR-Software, um persönliche Daten zu stehlen. Das können die Opfer tun.

Felix Blank
Senior Solution Consultant
München, Germany

EXPERTEN-TIPP

Wenn dies in Ihrem Land möglich ist, sollten Sie eine Betrugswarnung oder eine Sicherheitssperre für Ihre Kreditakte einrichten. Dies hindert Kriminelle daran, neue Konten in Ihrem Namen zu eröffnen. Und ziehen Sie eine vertrauenswürdige Identitätsschutzlösung in Betracht, wie die in F-Secure Total, um zu verfolgen, wie Ihre gestohlenen Daten gegen Sie verwendet werden könnten.

“Auf die Lösegeldforderung einzugehen, ermutigt nicht nur den Kriminellen, sondern wird wahrscheinlich auch nicht funktionieren”

Die Ransomware-Bande Clop hat sich zu einer Reihe von Angriffen bekannt, bei denen eine bisher unentdeckte Sicherheitslücke in MOVEit Transfer ausgenutzt wurde. Zahlreiche Softwarelösungen, darunter die Personalplattform Zellis, enthalten dieses Tool.

Mitarbeiter der BBC, von Banken, Universitäten und der Regierung von Nova Scotia sowie Tausende von anderen Unternehmen haben eine Vielzahl privater Daten preisgegeben, darunter in einigen Fällen auch Bankdaten.

Clop wird persönlich

Progress Software, der Hersteller von MOVEit Transfer, gab bekannt, dass er im Mai 2023 mit dem Patchen von MOVEit-Schwachstellen begonnen hatte. Clop scheint jedoch bereits seit 2021 Sicherheitslücken in der Software auszunutzen

"Die Bande ging den ungewöhnlichen Schritt, die Unternehmen nicht direkt zu kontaktieren, um ein Lösegeld zu fordern", so Felix Blank, Senior Solution Consultant bei F-Secure. "Stattdessen veröffentlichten sie eine Erpressernachricht auf ihrer eigenen Website und forderten die Opfer auf, sich bis zu einem Termin Mitte Juni, der bereits verstrichen war, direkt mit ihnen in Verbindung zu setzen."

Diese Nachricht teilte den Opfern mit, dass die Bande "eine Menge Ihrer Daten" entwendet habe. Blank wies darauf hin, dass die Kriminellen einem neuen Trend bei Ransomware folgen, bei dem Gruppen versuchen, Daten auf verschiedene Weise zu Geld zu machen, einschließlich der Drohung, Daten öffentlich zu machen.

Handeln Sie, nicht ködern

Leider wies Blank darauf hin, dass es hier keine wirkliche Lösung für die Opfer gibt, selbst wenn sie das Lösegeld bezahlen.

"Auf die Lösegeldforderung einzugehen, ermutigt nicht nur den Kriminellen, sondern wird wahrscheinlich auch nicht funktionieren", sagte er. "Die hier gestohlenen Daten werden wahrscheinlich irgendwann auf die eine oder andere Weise im Dark Web landen.

Diese düstere Realität sollte Opfer motivieren, die notwendigen Schritte zum Schutz ihrer Konten und ihrer Identität zu unternehmen.

"Befolgen Sie die Anweisungen Ihres Arbeitgebers, falls Sie welche erhalten", so Blank. "Überwachen Sie außerdem Ihre Online-Identität und seien Sie besonders vorsichtig beim Anklicken von Links in unaufgeforderten SMS oder E-Mails, die Sie erhalten."

Android-Trojaner lassen Nutzer zahlen.

Bösartige Apps versprechen coole Tools, zwingen Google Play-Kunden aber zu unerwünschten Abonnements.

Online-Kriminelle drängen in die lukrative Welt der Abonnementdienste - natürlich mit Hilfe von Betrug.

Der Android-Trojaner Fleckpe taucht immer wieder im Google Play Store auf, versteckt in ansprechenden Apps, darunter Beauty-Tools, Fotobearbeitungssoftware und Wallpaper-Pakete. Sobald die Malware installiert ist, abonniert sie die Opfer heimlich für kostenpflichtige Dienste.

Das Vertrauens der Nutzer wird ausgenutzt

Google scheint zwar erfolgreich darin zu sein, mit Fleckpe eingebettete Apps auszusortieren, wenn sie auftauchen, aber der Trojaner hat Berichten zufolge seit 2022 mehr als eine halbe Million Nutzer infiziert.

"Bedrohungsakteure finden immer wieder innovative Wege, das Vertrauen der Opfer zu gewinnen, um sie zur Installation von Malware zu bewegen", sagt Amit Tambe, Forscher bei F-Secure. "Diese Angreifer nutzen das große Vertrauen, das viele Nutzer in den Google Play Store haben, aus".

Der Infektionsprozess ähnelt stark der Installation einer legitimen Anwendung, so dass die Benutzer wahrscheinlich keinen Verdacht schöpfen oder sich der bösartigen Aktivitäten, die Fleckpe im Hintergrund ausführt, gar nicht bewusst sind.

Das übliche Geschäft

Tambe merkt an, dass die App bei der Installation die Erlaubnis zum Zugriff auf SMS-Nachrichten und -Benachrichtigungen anfordert.

"Da sich Fleckpe in echt aussehenden Anwendungen versteckt, scheinen die Anfragen nach SMS- und Benachrichtigungsberechtigungen nichts Ungewöhnliches zu sein", sagte er. "Dieser Zugang gibt Kriminellen die Möglichkeit, die wiederkehrenden Kreditkartenabrechnungen zu veranlassen, die diesen Betrug so profitabel machen.

Über den von der App angeforderten Zugang, den der Benutzer bei der Installation der App erhalten hat, kann die Malware unbemerkt alle für die Dienste erforderlichen Bestätigungen vornehmen.

"Leider aktualisieren die Kriminellen, die hinter dieser App stecken, die Funktionen ständig, um sie sowohl für die Nutzer als auch für Google selbst schwerer erkennbar zu machen", so Tambe abschließend.

Amit Tambe
Wissenschaftlicher Mitarbeiter
Helsinki, Finnland

EXPERTEN-TIPP

Der beste Weg, um bösartige mobile Apps zu vermeiden ist, sich an die offiziellen Stores zu halten. Aber auch die Apps in Google Play können schädlich sein. Achten Sie nicht nur auf die Bewertung einer App, sondern auch auf die Rezensionen. Wenn Sie sich immer noch Sorgen machen, vertrauen Sie auf Ihren Verstand und prüfen Sie auch die Bewertungen d er Entwickler.

“Diese Angreifer nutzen das große Vertrauen aus, das viele Nutzer in den Google Play Store haben."

Ihre digitales Leben sicher im Urlaub

Ihre digitalen Geräte tragen dazu bei, dass Sie Ihren Urlaub in vollen Zügen genießen können. Hier erfahren Sie, wie Sie dafür sorgen können, dass diese geschützt sind.

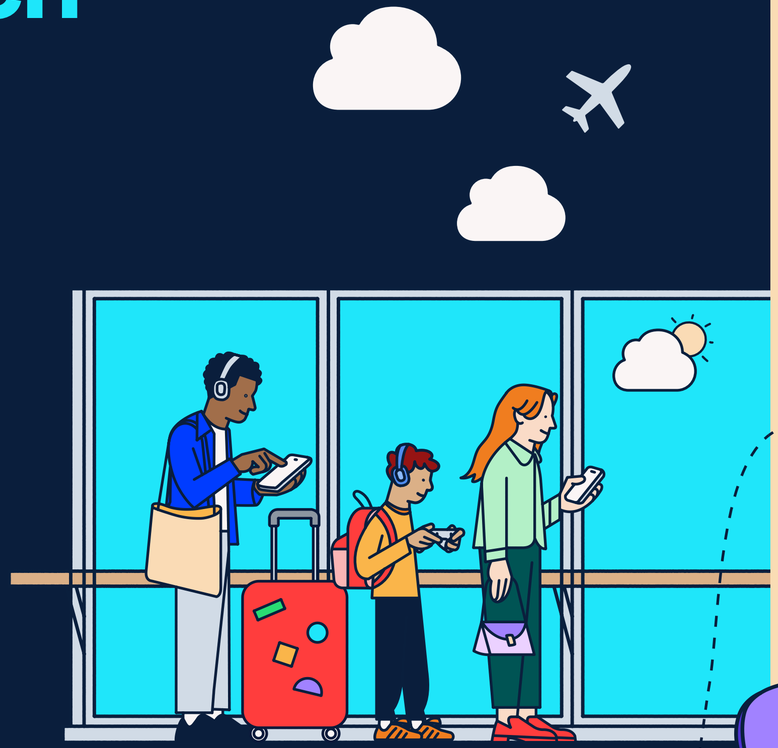
Bevor Sie abreisen 1

Intelligentes Zuhause

Stellen Sie Ihre intelligente Beleuchtung so ein, dass es so aussieht, als ob Sie zu Hause wären. Und gehen Sie nicht weg, ohne Ihrem WLAN und all Ihren intelligenten Geräten ein sicheres, eindeutiges Passwort zuzuweisen.

Geräte

Machen Sie Backups von Ihren Geräten. Vergewissern Sie sich auch, dass Sie Ihre Passwörter aus Ihrem Passwort-Manager auf mehreren Geräten synchronisiert haben, damit Sie auch im Urlaub Zugang zu Ihren Diensten haben.



2 Unterwegs

Flughäfen und öffentliche Verkehrsmittel

Benötigen Sie kostenloses öffentliches WiFi? Verwenden Sie VPN, wenn Sie sich auf Reisen mit einem beliebigen Netzwerk verbinden.

3 An Ihrem Reiseziel

Stellen Sie sicher, dass Ihr Gerät und Ihre SIM-Karte mit einem starken PIN-Code geschützt sind, falls Ihr Gerät verloren geht oder gestohlen wird. Deaktivieren Sie außerdem den Flugzeugmodus für Ihre SIM-Karte ohne PIN-Code. Dadurch wird es Taschendieben erschwert, das Gerät offline zu nehmen, und ein Fernlöschen verhindert.

4

Der schlimmste Fall

ein verlorenes Telefon

Wenn Sie Ihr Gerät verlieren oder glauben, dass es gestohlen wurde, müssen Sie schnell handeln:

Gehen Sie auf ein anderes Gerät und versuchen Sie, Ihr Telefon mit Find My Device für Android oder iCloud.com/find für iOS-Geräte zu **orten**.

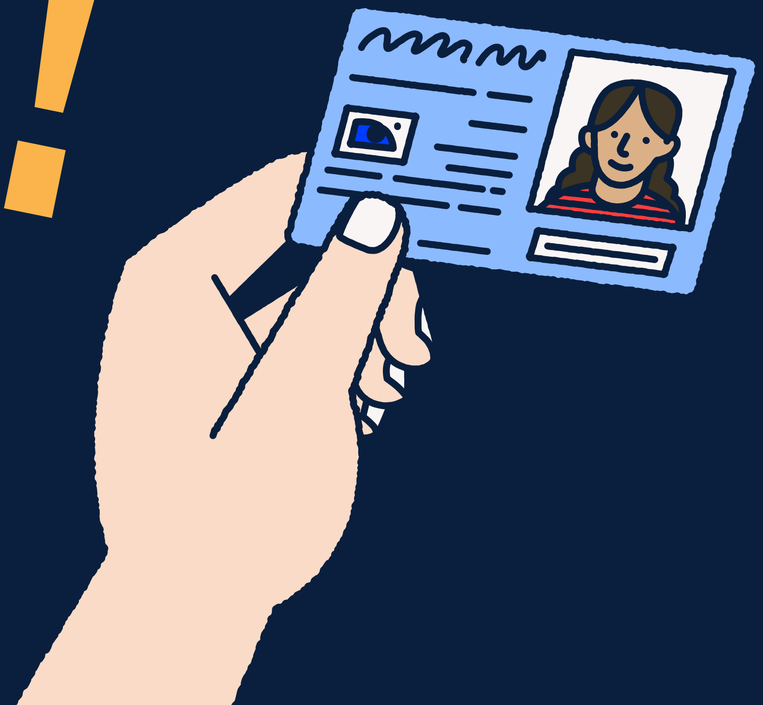
Sperren Sie Ihr Telefon mit der Funktion "Sicheres Gerät" von Android oder dem "Verlorenen Modus" von iOS.

Melden Sie den Verlust den zuständigen Behörden und kontaktieren Sie Ihren Mobilfunkanbieter, um sicherzustellen, dass das Gerät für denjenigen, der es hat, unbrauchbar ist..

5

Wenn Sie nach Hause kommen

Prüfen Sie genau alle Abrechnungen von Kredit- oder Bankkarten, die Sie im Urlaub benutzt haben – persönlich oder online.



Reisen Sie unbesorgt.

F-Secure Total bietet vollständige Online-Sicherheit, Datenschutz und ID-Schutz - wo immer Sie auch sind, mit einer einzigen App.

Was müssen Sie über KI wissen?

Experten warnen immer wieder vor den Risiken der künstlichen Intelligenz, aber was bedeutet das für Sie?

KI-Tools, die in der Lage sind, Texte und Bilder zu generieren, wie ChatGPT und Midjourney, werden von Hunderten von Millionen Menschen genutzt. Einige Experten schlagen jedoch wegen der Zunahme von Maschinen, die zu denken scheinen, Alarm.

Dinge werden intelligenter als wir

Der so genannte "Godfather of AI" hat im Mai bei Google gekündigt, um frei über das "existenzielle Risiko, was passiert, wenn diese Dinge intelligenter werden als wir", sprechen zu können. Und im Juni nannte Singapur sechs Risiken der generativen KI: "Halluzinationen", Bedenken hinsichtlich des Datenschutzes, Desinformation, Urheberrechtsfragen, inhärente Verzerrungen und die Herausforderung, Sicherheitsmechanismen in diese Modelle einzubauen. Deshalb haben wir Khalid Alnajjar, Threat Data Researcher bei F-Secure, gebeten, einige Grundlagen, die jeder über KI wissen sollte, zu erklären.

Was sind große Sprachmodelle (LLMS)?

Sprachmodelle zielen darauf ab, Texte zu generieren, indem sie den Kontext verstehen und Wort für Wort die wahrscheinlichste Reaktion darauf vorhersagen.

Stellen Sie sich den LLM als einen erfahrenen Assistenten vor, der alle Daten durchgelesen hat und Ihnen sofort relevante Ratschläge für den aktuellen Fall, an dem Sie arbeiten, geben kann, indem er ihn analysiert und mit den Fällen vergleicht, über die er im Hintergrund gelesen hat.

Machen Sie jedoch nicht den Fehler zu glauben, dass alles, was ein LLM Ihnen erzählt, wahr ist, wie es ein Anwalt in den Vereinigten Staaten tat. Er reichte einen Schriftsatz ein, der sechs Fälle enthielt, die ChatGPT scheinbar aus dem Nichts "halluziniert" hatte. Leider hat das der Richter bemerkt.

Welche Sicherheitsrisiken birgt KI?

KI ist ein zweischneidiges Schwert und wenn sie in die Hände von Cyberangreifern gerät, sind unerwünschte Ergebnisse vorprogrammiert. Diese Angriffe können darin bestehen, bösartige Inhalte in die KI-Modelle selbst zu injizieren. Das kann von bösartigem Code bis hin zu Propaganda alles sein.

Generative KI kann leicht dazu verwendet werden, Phishing und Betrug zu automatisieren und Menschen zu imitieren indem ihr einzigartiger Stil nachgeahmt wird, um irreführende Inhalte zu produzieren, wie z. B. Deep Fakes von Politikern, die provokante Reden halten. Es ist wichtig sich dieser Angriffe bewusst zu sein und Online-Inhalten nicht blind zu vertrauen - heute mehr denn je.

Khalid Alnajjar
Threat Data Researcher
Helsinki, Finnland

EXPERTEN-TIPP

Generative KI kann leicht dazu verwendet werden, Phishing und Betrug zu automatisieren und Menschen zu imitieren indem ihr einzigartiger Stil nachgeahmt wird, um irreführende Inhalte zu produzieren, wie z. B. Deep Fakes von Politikern, die provokante Reden halten.

Es ist wichtig sich dieser Angriffe bewusst zu sein und Online-Inhalten nicht blind zu vertrauen - heute mehr denn je.

“Betrachten Sie den LLM als einen erfahrenen Assistenten.”

ADVANCE ALERT :
Infostealer und die MacOS-Goldmine

Die Sicherheit von Apple ist nicht mehr selbstverständlich

MacOS galt lange Zeit als eine Festung gegen Cyberangriffe. Jüngste Entwicklungen haben diese Vorstellung jedoch erschüttert, denn Infodiebe haben sich als wachsende Bedrohung für das Apple-Ökosystem - und seine Nutzer - entpuppt.

Ein heimlicher Angriff auf Ihre wertvollsten Daten

Infostealer können vertrauliche Informationen stehlen, z. B. Passwörter für Ihren Schlüsselbund oder Anmeldedaten für Ihre E-Mails, Konten bei sozialen Medien, Streaming-Dienste und Messaging-Anwendungen.

Diese Bedrohung kann über Phishing-Techniken auf Ihren Mac gelangen, bei denen die Opfer manipuliert werden. Gefälschte Reinigungs- oder Hilfsprogramme sowie raubkopierte oder geknackte Software führen ebenfalls zu Infostealer-Infektionen.

Das Ausbeutung von guten Absichten

Apple hat zahlreiche Sicherheitsfunktionen wie Datei-Quarantäne, Gatekeeper, Notarization und XProtect eingeführt, um Benutzer vor Phishing-Angriffen und bösartigen Anwendungen zu schützen. Die Sicherheitskontrollen von Apple bieten dem Benutzer jedoch auch die Möglichkeit, den Schutz zu umgehen.

Es überrascht daher nicht, dass bösartige Anwendungen inzwischen Social-Engineering-Techniken einsetzen, um überzeugende Szenarien zu schaffen, die die Benutzer dazu bringen, die bösartigen Anwendungen trotzdem zu öffnen. Der AMOS-Infostealer (Atomic MacOS Stealer) beispielsweise zeigt ein Fenster an, in dem das Opfer aufgefordert wird, die Fehlermeldung der Sicherheitskontrollen zu ignorieren, und überzeugt die Benutzer, mit der rechten Maustaste auf die bösartige Anwendung zu klicken und sie dann zu öffnen. Auf diese Weise werden die Sicherheitsmaßnahmen von Apple effektiv umgangen. ▶▶

Außerdem verfügt MacOS, wie andere Betriebssysteme auch, über einen mächtigen Administrator, der auf alle Dateien und Programme auf dem Rechner zugreifen kann. Infostealer verleiten Benutzer oft dazu, ihr Administrator-Passwort preiszugeben, indem sie einen ähnlich aussehenden Dialog für ein Systempasswort anzeigen. Auf diese Weise kann die Malware auf versteckte Bereiche des Systems zugreifen und sensible Informationen abgreifen. Der Dieb kann sich sogar im System halten und den Zugriff aufrechterhalten, indem er so genannte Persistenztechniken einsetzt.

Das große Ganze

Malware, die auf MacOS abzielt, hat sich zwischen 2020 und 2022 fast verdoppelt. Die Zahl der einzigartigen, neuen Malware-Familien ist mit 13 immer noch gering. Am wichtigsten ist jedoch, dass Malware-Gruppen begonnen haben, MacOS-Versionen ihrer Angriffe zu entwickeln. Dies zeigt eine Verlagerung hin zu MacOS, die dem Anstieg seines Marktanteils folgt. ■

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finnland

EXPERTEN-TIPP

Um sich vor Datendieben zu schützen, sollten Sie proaktive Maßnahmen ergreifen. Es ist wichtig, alles auf dem neuesten Stand zu halten. Verpassen Sie also keine Updates für Ihr Betriebssystem und Ihre Anwendungen, die alle aus dem offiziellen Apple App Store stammen sollten. Darüber hinaus kann eine vertrauenswürdige Anti-Malware-Software wie F-Secure Total Ihren Schutz erheblich verbessern.

Über F-Secure

F-Secure macht jeden digitalen Moment sicherer, für jeden. Wir bieten brillant einfache, reibungslose Sicherheitserlebnisse, die das Leben für die Millionen von Menschen, die wir schützen, und unsere 180 Partner einfacher machen.

Seit mehr als 30 Jahren sind wir führend in der Cybersicherheitsbranche, inspiriert von einem Pioniergeist, der aus der gemeinsamen Verpflichtung erwächst, durch Zusammenarbeit mehr zu erreichen.

Besuchen Sie gleich unsere Website f-secure.com/de für weitere Informationen.

F-Secure