



Operation Honigbiene: China lädt Späh-App auf Touristen-Handys

Der Bund, Tamedia Espace AG

Donnerstag 4. Juli 2019 11:04 von Lea Deuber, Felix Ebert, Nicolas Richter, Christian Brönnimann

Michael Kummer ahnte, was ihm blühen könnte, als er kürzlich nach China reiste. Der Schweizer, der in Wahrheit anders heisst, löschte alle Daten auf seinem Handy und präparierte seinen Laptop so, dass er beim Aufstarten nicht das normale Betriebssystem mit seinen persönlichen Informationen öffnet. Grund für Kummers Vorsicht: der [chinesische Überwachungsstaat](#) macht auch vor ausländischen Touristen und Geschäftsreisenden nicht Halt.

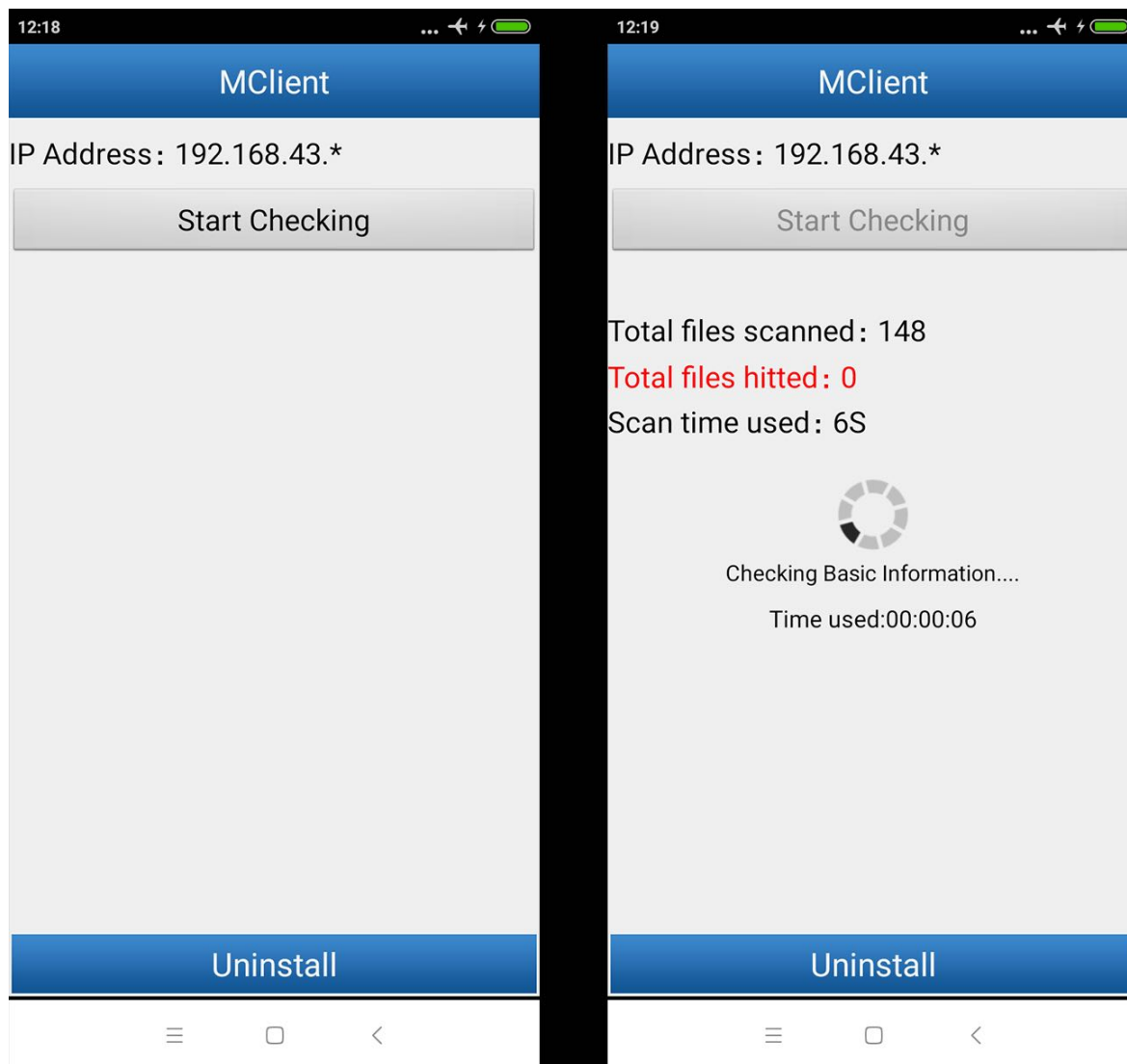
Kummer reiste auf dem Landweg nach China. Der Grenzübertritt von Kirgisistan aus ist ihm in besonderer Erinnerung: Mindestens sechs Grenzkontrollen, verteilt auf rund 150 Kilometer, musste er überwinden. Dazwischen: menschenleeres, karges Gebirgsland.

Bei einem der grösseren Kontrollposten auf chinesischer Seite nehmen ihm die Grenzpolizisten das Mobiltelefon ab. Er muss den Code zum Entsperren eintippen, dann bringen es die Uniformierten in einen anderen Raum. Nach einer Viertelstunde erhält Kummer das Handy zurück. «Was in dieser Zeit mit dem Telefon geschah, konnte ich nicht sehen», sagt er. Als er das Telefon wieder in den Händen hält, ist eine neue App installiert. «Ich versuchte einen Grenzbeamten zu fragen, was das sei. Die Antwort war ein Kopfschütteln und eine abweisende Handbewegung», erzählt Kummer.

Er muss den Code zum Entsperren eintippen, dann wird das Telefon in einen anderen Raum gebracht.

Eine Reporterin der «Süddeutschen Zeitung» erhielt Zugang zum Raum auf dem Grenzposten, in den die Mobiltelefone gebracht werden. Er ist nicht viel grösser als eine Abstellkammer. Auf einem Tisch liegen ein Dutzend Handys, jedes Gerät auf dem Pass seines jeweiligen Eigentümers, europäische und asiatische Touristen, kirgisische LKW-Fahrer, chinesische Unternehmer. Weil der Polizist an vielen Geräten gleichzeitig arbeitet, verwechselt er sie öfters, später muss er Reisende darum bitten, ihm bei der Zuordnung zu helfen.

Ein Grenzbeamter verbindet die Handys mit einem WLAN-Netz und lädt eine App auf die Geräte, 3,9 Megabyte, so gross wie zwei Fotodateien. Auf dem Bildschirm eines Handys erscheint eine weisse Oberfläche mit zwei Feldern. Auf einem steht «Durchsuchung starten», auf dem anderen «deinstallieren». Der Polizist tippt auf «Durchsuchung starten». Der Abfluss persönlicher Daten an den chinesischen Staat beginnt.



So sieht die Anwendung aus, wenn man sie startet.

Teil eines «dystopischen Plans»

Doch wird dieser Staat jetzt selbst ein bisschen durchsichtiger? Denn zum ersten Mal ist es gelungen, die chinesische Überwachungs-App zu durchleuchten. Sie wurde der «Süddeutschen Zeitung» Anfang des Jahres von einem Touristen zugespielt. Die Zeitung begleitete daraufhin weitere Touristen über die Grenze, um herauszufinden, ob die App auf die Handys aller Besucher installiert wird. Zumindest bei den beiden Grenzübergängen zu Kirgisistan scheint das so zu sein.

Gleichzeitig wertete die «Süddeutsche Zeitung» die App zusammen mit Medienpartnern und der Ruhr-Universität Bochum aus. Die Ergebnisse wurden durch den Opentech Fund, ein staatlich finanziertes US-Forschungsprogramm, und das Citizen Lab, ein Institut der Universität Toronto, überprüft und ergänzt.

Ron Deibert vom Citizen Lab in Toronto nennt die App Teil des «dystopischen Plans» Chinas, mit einer Kombination aus «Technologie und politischer und sozialer Kontrolle» die Region Xinjiang in ein «digitales Gefängnis» zu verwandeln. «Solche Apps sind eine grosse Gefahr für zivilgesellschaftliche Freiheiten, die Meinungs- und Versammlungsfreiheit», sagt er.

Kalendereinträge, Anruflisten, Kontakte und SMS

Das Logo der App ist unscheinbar, es ist der grüne Roboter mit Antennen auf dem Kopf, der das Google-Betriebssystem Android symbolisiert. Es sieht so aus, als gehöre das chinesische Spionageprogramm zur gewöhnlichen Ausstattung eines Smartphones. Sieht man genau hin, erkennt man unter dem Roboter den Namen der App, Fengcai, was in etwa «sammelnde Honigbienen» bedeutet. Reiseagenturen in Kirgisistan berichten, dass diese Software mindestens seit 2018 auf die Handys von Touristen aufgespielt werde.

Was also sammeln die Honigbienen? Die knappe Antwort: So gut wie alles. Die App fragt 20 Berechtigungen an; tatsächlich nutzt sie dann den Zugriff auf Kalender, SMS, Kontakte, Speicher, Standort, Anruflisten, Telefonnummer. Das sind fast alle wesentlichen Funktionen. Wie ein Bienenschwarm es auf einer Blumenwiese tun würde, fällt die Fengcai-App über das Gerät her und saugt möglichst viel Honig. Die App läuft nur auf Geräten mit dem Google-Betriebssystem Android. iPhones dagegen liest der Staat offenbar aus, indem er ein externes Aggregat an die Ladebuchse des Handys anschliesst, so legen es Beobachtungen am Grenzposten nahe.

Die App sortiert die erlangten Daten, stellt sie in Tabellenform zusammen und sendet diese Übersichten bereits im Grenzposten als Teil eines «Reports» über WLAN an einen Computer. An diesem Rechner können die Sicherheitsbeamten die Erstausswertung studieren. Diese beinhaltet sämtliche Kalendereinträge, Anruflisten, Kontakte und SMS. Übertragen werden auch die Profilbilder aller Kontakte auf dem Smartphone.

PhoneInfo

Manufacturer	Android
Model	SM-G960F(WIFI)
RealModel	SM-G960F(WIFI)
IMEI	9999999999999999,33333333333333
IMSI	111111111111111
ConnectType	WIFI
StartTime	2019/06/26 10:11:52
EndTime	2019/06/26 10:11:52
Date	2019/06/26
TZI	Pacific Standard Time
Version	1.0.0
SN	201901

Message

ID	SmsStorage	SmsType	Folder	CenterNumber	TelePhone	SmsTime	Type	Text
1	N/A	Send	N/A	+49172222222	Facebook	2019/06/25 14:13:01	1	<#> 62000 ist dein Facebook-Code Laz+nxCarLW
2	N/A	Send	N/A	+49171111111	Facebook	2019/06/25 14:09:58	1	<#> 62000 ist dein Facebook-Code Laz+nxCarLW
3	N/A	Read	N/A	+49172333333	Google	2019/06/03 14:59:25	1	G-777777 ist Ihr Google-Best{tigung}code.

Contact

ID	LocalType	Group	Name	Number	MobilePhone	HomeNum	Fax	Work	Email	Internet	Address	Note
1	N/A		Maria Musterfrau		17111111							
2	N/A		Max Mustermann		17444444							

Dialing

ID	CalType	Name	Number	StartTime	Duration
1	Missed		+4961555566677	2019/06/19 18:38:13	0
2	Missed		+4961444444477	2019/06/19 19:37:43	0

Gleichzeitig bereitet die App die erlangten Informationen maschinell lesbar auf und sendet diese Datensätze mit den Informationen über alle auf dem Gerät installierten Apps an den Computer im Grenzposten.

Suche nach «verdächtigen» Daten

Was damit geschieht, ist unklar, womöglich werden die Daten an eine zentrale Polizeidatenbank geschickt und dort systematisch ausgewertet. So liesse sich zum Beispiel feststellen, ob eine Kontaktperson des Reisenden ebenfalls eingereist ist. Ein Teil der App sucht zudem nach Log-ins von chinesischen sozialen Netzwerken sowie Daten einer Navigations-App.

Auf Anfragen für diese Recherche wollten sich weder Chinas Zentralregierung noch die Provinzregierung in Xinjiang äussern. Auch die Firma Nanjing FiberHome StarrySky Communication Development, die die App entwickelt hat, schweigt.

Die «Honigbienen» können noch mehr, wie ein Test zeigt. An der Ruhr-Universität Bochum legen die Experten ein Smartphone, auf dem die Überwachungs-App gespeichert ist, in eine Metallbox. Dieser Kasten soll das Gerät vom deutschen Mobilfunknetz abschirmen. Im Inneren der Metallbox wurde zugleich ein WLAN-Netz eingerichtet. Dieses Umfeld soll jenem an der chinesischen Grenze entsprechen, die chinesische App dürfte sich dementsprechend so verhalten, wie sie es am Grenzposten tun würde.

Zehntausende potenziell gefährliche Elemente

Nun starten die Techniker den Scan-Modus der App. Und tatsächlich meldet diese sofort ein Ergebnis: eine verdächtige Datei, die auf dem Handy gespeichert wurde. Die App meldet den Fund mit einer Anzeige auf dem Bildschirm und einem Piepton, der von einem Computerspiel stammen könnte.

So offenbart sich eine weitere Eigenschaft des chinesischen Überwachungsprogramms. Die «Sammelnde Honigbienen»-App durchsucht das Smartphone nämlich auch nach Inhalten, die aus Sicht der chinesischen Regierung verdächtig sind. Dazu nimmt die App eine Art Fingerabdruck von Dateien, die auf dem Smartphone gespeichert wurden. Diese sogenannten «Hashwerte» gleicht sie mit einer Datenbank innerhalb der App ab, die 73'315 Einträge enthält.

```
<string name="sending_result">Sending check results...</string>
<string name="checking_contacts">Checking phone contacts</string>
<string name="checking_sim_contacts">Checking SIM card contacts</string>
<string name="checking_call_logs">Checking call logs</string>
<string name="testing_sms">Checking SMS</string>
<string name="checking_calendar">Checking calendar information</string>
<string name="checking_sim_sms">Checking SIM card SMS</string>
```

So sieht der Code der Überwachungs-App «Fengcai» aus.

Alle diese 73'315 Dateien sind aus Sicht der chinesischen Regierung dubios. Dazu gehören Inhalte, die klar terroristisch sind: Pamphlete der Organisation Islamischer Staat oder jihadistische Gewaltvideos. Die App sucht etwa nach Ausgaben des Jihadisten-Magazins «Inspire», das unter anderem erklärt, wie man zu Hause eine Bombe baut. Es finden sich auch Videos mit Enthauptungen aus dem Irak und Aufnahmen des deutschen Islamisten Denis Cuspert, der wohl vor mehr als einem Jahr in Syrien getötet wurde. Andere Videos zeigen Enthauptungen durch Mitglieder mexikanischer Drogenkartelle.

Einige Dateien, in denen Arabisch gesprochen wird oder die auf Arabisch verfasst wurden, beinhalten aber auch harmlose Aufnahmen von Koran-Suren, die gläubige Muslime auf dem Handy speichern. Eine andere Datei, nach der die App sucht, ist die Aufnahme einer japanischen Metalband, eines ihrer Alben heisst: «Taiwan – another China».

Andere Dateien haben mit Tibet und dem Dalai Lama zu tun, etwa eine Biografie, die eine Organisation in Taiwan herausgegeben hat. Tibet gehört aus Pekinger Sicht zu China, der Status ist aber umstritten. Taiwan ist ein unabhängiger Staat, auf den Peking Anspruch erhebt.

Xi Jinpings Paranoia

Folglich sucht die chinesische App auch nach Material, das in einem europäischen Land als völlig harmlos gelten würde, sowie nach Inhalten, die auch in China zumindest offiziell von der Religionsfreiheit abgedeckt sein sollten. Es ist eine Sammlung, die belegt, wie gross die Paranoia im neuen China unter Präsident Xi Jinping inzwischen geworden ist, und wie sie sich gegen immer mehr Aspekte des gesellschaftlichen und kulturellen Lebens des Landes richtet.

Michael Kummer hat die App schon einen Tag nach seiner Einreise nach China wieder gelöscht. Ob das vom Staat bemerkt wurde, kann er nicht sagen. Sein Handy hat Kummer nach der Rückkehr in die Heimat ausgetauscht. Ob er jemals wieder nach China reisen wird, weiss er noch nicht.

Mitarbeit: Katharina Brunner, Frederik Obermaier und Vanessa Wormer.