Staatsanwaltschaft München I
Linprunstraße 25
80097 München

Hiermit erstatten

die Gesellschaft für Freiheitsrechte
Hessische Str. 10
10115 Berlin
vertreten durch den Vorsitzenden Dr. Ulf Buermeyer,
ulf.buermeyer@freiheitsrechte.org

Reporter ohne Grenzen
Potsdamer Str. 144
10783 Berlin
vertreten durch den Geschäftsführer Christian Mihr,
christian.mihr@reporter-ohne-grenzen.de

das European Center for Constitutional and Human Rights e.V.
Zossener Str. 55 – 58,
10961 Berlin
vertreten durch Dr. Miriam Saage-Maaß, Vice legal Director,
saage-maasz@ecchr.eu

Netzpolitik.org
Schönhauser Allee 6/7
10119 Berlin
vertreten durch Andre Meister,
andre@netzpolitik.org

Strafanzeige

wegen Verstoßes gegen § 18 Abs. 2 Nr. 1 und § 18 Abs. 5 Nr. 1 des Außenwirtschaftsgesetzes

gegen

1. Herrn Markus Meiler, Geschäftsführer der Elaman GmbH, geschäftsansässig in der Baierbrunnerstr. 15, 81379 München,
2. Herrn Holger Rumscheidt, Geschäftsführer der Elaman GmbH, geschäftsansässig in der Baierbrunnerstr. 15, 81379 München,
3. Herrn Carlos Gandini, Geschäftsführer der FinFisher GmbH, geschäftsansässig in der Baierbrunnerstr. 15, 81379 München,
4. Herrn Lucian Hanga, Geschäftsführer der Finfisher Labs GmbH, geschäftsansässig in der Baierbrunnerstr. 15, 81379 München,
5. Herrn Holger Tesche, Geschäftsführer der Finfisher Labs GmbH, geschäftsansässig in der Baierbrunnerstr. 15, 81379 München,
6. weitere, namentlich nicht bekannte Mitarbeiter*innen der Elaman GmbH, der Finfisher GmbH und Finfisher Labs GmbH, geschäftsansässig in der Baierbrunnerstr. 15, 81379 München.

Die Verdächtigen geben, soweit sie Angehörige der Firmen FinFisher GmbH und FinFinFisher Labs GmbH sind, postalisch als Geschäftssitz an: Sapporobogen 6-8, c/o Kanzlei hph, 80637 München.

Gliederung

A. EINLEITUNG UND ZUSAMMENFASSUNG

Es bestehen tatsächliche Anhaltspunkte dafür, dass sich die Verdächtigen, die zum anzeigerelevanten Zeitpunkt Geschäftsführer bzw. Mitarbeiter der Elaman GmbH, FinFisher GmbH bzw. FinFisher Labs GmbH waren, des vorsätzlichen Verstoßes gegen Genehmigungspflichten für Dual-Use-Software gem. § 18 Abs. 2 Nr. 1 und § 18 Abs. 5 Nr. 1 Außenwirtschaftsgesetz (AWG) strafbar gemacht haben, in dem sie die Überwachungssoftware FinSpy im Zeitraum zwischen Oktober 2016 bis Juli 2017 in die Türkei exportierten, ohne zuvor die erforderliche Genehmigung der Bundesregierung einzuholen.

Der Strafanzeige liegt zusammengefasst folgender Sachverhalt zugrunde:

Am 29. Juni 2017 wurde auf einer an ein ausschließlich türkischsprachiges Publikum gerichteten Website der Auszug einer Überwachungssoftware gefunden, deren Quellcode dem Quellcode der Überwachungssoftware FinSpy in wesentlichen Punkten entspricht. Die Website war so gestaltet, dass sie ohne Weiteres für die von der türkischen Oppositionsbewegung zu Organisationszwecken genutzte Website – die sogenannte Adalet-Website – gehalten werden konnte.

Die gefälschte Adalet-Website dient ihrer Funktionalität nach einzig dem Zweck, Besucher davon zu überzeugen, eine Überwachungssoftware, getarnt als zur Vernetzung nutzbare Android-Anwendung, auf ihren mobilen Telekommunikationsgeräten zu installieren. Nach dem Herunterladen auf ein mobiles Gerät ermöglichte diese Android-Anwendung, bei der es sich um Malware handelt, dem Angreifer den Zugang zu Telefon- und VoIP-Gesprächen, Datensystemen, Screenshots und anderen Fotos, GPS-Daten, Mikrofonen und Verbindungsdaten sowie zu verschiedenen Anwendungen, u.a. Whatsapp, Line, Viber, Telegram, Skype, Facebook Messenger, Kakao und WeChat.

Von unabhängigen Experten bestätigten Software-Analysen zufolge ist der partiell auslesbare Quellcode der auf der Website gefundenen Malware praktisch identisch mit der von den Firmen FinFisher GmbH bzw. FinFisher Labs GmbH (im Folgenden vereinfachend: FinFisher) hergestellten Malware FinSpy. Auch ein Microsoft-Bericht aus dem Jahr 2016 vermeldet FinSpy Funde in der Türkei.

FinSpy wird von FinFisher hergestellt und gemeinsam mit der Elaman GmbH vertrieben. Von einzelnen, dieser Anzeige zugrunde liegenden und lediglich Teile des FinSpy-Codes abbildenden, Samples abgesehen, ist bis heute kein Daten-Leck („Leak“) des FinSpy-Codes bekannt geworden. Da jene Teile nicht ausreichend sind, um eine vollständige, FinSpy gleichende Malware herzustellen, ist davon auszugehen, dass niemand außer den genannten Unternehmen Zugriff auf den gesamten Quellcode von FinSpy hat.

Aufgrund seiner umfassenden Überwachungsfunktionen bedarf die Ausfuhr von FinSpy einer vorherigen Genehmigung durch die Bundesregierung, § 8 Abs. 1 Nr. 2 Außenwirtschaftsverordnung (AWV) i.V. mit Teil I Abschnitt B,

Code 5D902 lit. a) i.V.m. 5A902 der Ausfuhrliste sowie Art. 3 Abs. 1 der Dual Use Verordnung (2018/1922) i.V.m. Anhang I Code 4A005.

Auf parlamentarische Anfragen hin, zuletzt noch am 19. Juni 2019, hat die Bundesregierung bestätigt, dass sie seit Januar 2015 keine solche Genehmigung erteilt hat.

Es ist davon auszugehen, dass die Verdächtigen als Geschäftsführer der mit Herstellung und Vertrieb von FinSpy befassten Unternehmen sowie weitere namentlich nicht bekannte Mitarbeiter*innen, die genehmigungslosen Ausfuhrvorgänge jedenfalls mit vorgenommen bzw. veranlasst haben. Damit haben sie sich gem. § 18 Abs. 2 Nr. 1 und § 18 Abs. 5 Nr. 1 AWG strafbar gemacht.

Wir regen die Einleitung eines Ermittlungsverfahrens wegen des strafbaren Verhaltens der Verdächtigen an.

B. ZU DEN VERDÄCHTIGEN

Die Verdächtigen zu 1 und 2 sind seit dem 23. Oktober 2013 Geschäftsführer der Elaman GmbH, der Verdächtige zu 3 ist seit dem 12. August 2016 Geschäftsführer der FinFisher GmbH, die Verdächtigen zu 4 und 5 sind seit dem 12.02.2014 Geschäftsführer der FinFisher Labs GmbH,

> Elaman GmbH - HRB 153662; FinFisher Labs GmbH - HRB 176385; FinFisher GmbH - HRB 205475, vgl. auch Anhang 3.

C. ZUR ELAMAN GMBH, FINFISHER LABS GMBH, FINFISHER GMBH

Die Elaman GmbH, FinFisher Labs GmbH und FinFisher GmbH haben ihren Hauptsitz an derselben Firmenadresse in München und sind, soweit ersichtlich, auch personell und funktionell eng miteinander verflochten. Gemeinsam produzieren und vertreiben sie nach ihrem registrierten Geschäftszweck Sicherheitsprodukte und -systeme für Regierungsbehörden und regierungsnahe Organisationen,

> Elaman GmbH - HRB 153662; FinFisher Labs GmbH - HRB 176385; FinFisher GmbH - HRB 205475.

Die Elaman GmbH ist ausweislich des Handelsregisterauszugs für den nationalen und internationalen Vertrieb und das Marketing zuständig. Die FinFisher Labs GmbH ersetzte mit Handelsregistereintrag vom 26. September 2013 die Gamma International GmbH und ist für Entwicklung, Produktion, Handel und Vertrieb, Forschung, sowie Durchführung von Schulungen im Bereich der Software- und Nachrichtentechnik verantwortlich. Die Tätigkeitsbeschreibung der FinFisher GmbH, die mit Handelsregistereintrag vom 13. Oktober 2013 die Gamma International Sales GmbH ersetzte, ist fast wortgleich und umfasst Handel und Vertrieb von Software- und Nachrichtensystemen, Forschung und Schulungen,

> FinFisher Labs GmbH - HRB 176385; FinFisher GmbH - HRB 205475; FinFisher Holding GmbH - HRB 205476.

Nicht nur die Aktivitäten der verschiedenen Gesellschaften sind aufeinander bezogen, auch räumlich gibt es Überschneidungen. Die Baierbrunnerstr. 15, 81379 München ist der offizielle Hauptsitz der Elaman GmbH, tatsächlich befinden sich dort auch die Büroräume der FinFisher GmbH und der FinFisher Labs GmbH. Die offizielle Anschrift der FinFisher GmbH und FinFisher Labs GmbH im Sapporobogen 6-8, c/o Kanzlei hph, D-80637 München, ist nur ein Briefkasten bei einer Anwaltskanzlei.

Es gibt verschiedentliche Anhaltspunkte dafür, dass das Firmengeflecht in den letzten Jahren Überwachungssoftware an verschiedene autoritäre Regime verkauft hat. Die Citizen Lab der Universität von Toronto berichtet von FinSpyfunden in Angola, Ägypten, Gabon, Jordanien, der Türkei und Venezuela,

https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#1; zuletzt abgerufen am 02. Juli 2019.

Die ersten Berichte über Lieferungen durch FinFisher an autoritäre Staaten bezogen sich auf Regierungen des Nahen Ostens während des „Arabischen Frühlings". FinFishers Produkte wurden dort wiederholt eingesetzt, um die politische Opposition gezielt zu unterdrücken und zersetzen. Zwischen 2010 und 2012 setzte beispielsweise die Regierung Bahrains FinFisher ein, um Anwaltskanzleien, Journalisten, Aktivisten und politischen Führer der Opposition zu attackieren. Der damalige Geschäftsführer des FinFisher Vorgängers Gamma International Sales GmbH, Martin Münch, bestritt einen Export nach Bahrain zunächst,

https://web.archive.org/web/20120731005707/http:/www.bloomberg.com/news/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy.html; zuletzt abgerufen am 03. Juli 2019,

schließlich belegten von einer Nichtregierungsorganisation publizierte Archiv- und Lizenzunterlagen des hausinternen Kundensupports im August 2014 jedoch, dass Gamma International Sales GmbH seit 2010 Geschäftsbeziehungen mit der bahrainischen Regierung unterhielt,

https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/; zuletzt abgerufen am 2. Juli 2019.

Auch die Kommunikationstechnik äthiopischer Dissidenten wurden in der Vergangenheit mit der FinSpy Software infiziert,

https://www.eff.org/cases/kidane-v-ethiopia; zuletzt abgerufen am 3. Juli 2019.

D. ZU FINSPY

FinSpy ist eine hochentwickelte Spähsoftware, die ausweislich der Eigendarstellung auf der Firmenwebsite ausschließlich an staatliche Regierungen zum Zwecke der strategischen Aufklärung und Strafverfolgung verkauft wird,

Eigendarstellung auf finfisher.com; zuletzt abgerufen am 02. Juli 2019.

Die Malware wird hierbei vom FinFisher Unternehmensverbund hergestellt und vertrieben, am Vertrieb ist auch die Elaman GmbH beteiligt. FinSpy wird im Verbund mit Servern betrieben, an welche die erhobenen Daten gesendet werden. Diese Server können im Normalfall nicht ohne Zutun des Herstellers konfiguriert und betrieben werden. Nach der Installation der Finspy-Malware auf dem mobilen Endgerät eines Betroffenen ermöglicht FinSpy dem Kunden den verdeckten Zugriff auf Telefon- und VoIP-Gespräche, Dateninfrastrukturen, Screenshots und andere Fotos, GPS-Daten, Mikrofone, Verbindungsdaten sowie auf verschiedene Anwendungen, einschließlich Whatsapp, Line, Viber, Telegram, Skype, Facebook Messenger, Kakao und WeChat,

Bericht „Alert: FinFisher changes tactics to hook critics“, 14.5.2018, Gustaf Björksten und Lucie Krahulcova für Access Now (im Folgenden: “AN Bericht”), S. 8 ff., online abrufbar unter https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf; https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/, zuletzt abgerufen am 04. Juli 2019.

FinSpy ist hierbei besonders effektiv, da es für das ungeübte Auge praktisch unsichtbar bleibt: Nach der erstmaligen Ausführung löscht FinSpy das Symbol aus dem Hauptmenü des Smartphones. Die bislang bekannten FinSpy-Versionen wurden beim Starten des Systems ausgeführt, ohne dass sie dem Nutzer auffallen,

AN Bericht, S. 8.

E. DER SACHVERHALT

I. FINSPY AUF DER GEFÄLSCHTEN ADALET-WEBSITE

Die Türkei ist das Land geworden, in dem im Verhältnis zur Bevölkerungszahl weltweit die meisten Journalisten inhaftiert sind. Zurzeit befinden sich mindestens 34 Journalisten in politischer Gefangenschaft. Hunderte Zeitungen und andere Medienorgane wurden geschlossen. Nach dem gescheiterten Putschversuch vom 15. Juli 2016 wurden mehr als 50.000 Menschen verhaftet; mehr als 140.000 Menschen wurden aus ihren Berufen entfernt,

https://www.tagesschau.de/ausland/putsch-tuerkei-143.html, https://www.reporter-ohne-grenzen.de/tuerkei/, zuletzt abgerufen am 27. Juni 2019.

Im Juni und Juli 2017 zogen die Mitglieder der türkischen Opposition, die noch nicht inhaftiert oder ins Exil gegangen waren, über einen Zeitraum von drei Wochen anlässlich eines „Marsches für Gerechtigkeit“ auf die Straße, um gegen die autoritäre Reaktion der Regierung nach dem gescheiterten Putschversuch vom Juli 2016 zu protestieren. Soziale Medien haben sich weltweit und auch in der Türkei aufgrund ihrer Offenheit, Reichweite und der Möglichkeit zur geschützten Kommunikation zu einem wichtigen Kommunikationsmittel für Aktivist*innen, Menschenrechtsverteidiger*innen und politische Dissident*innen entwickelt. Entsprechend attraktiv ist die Intrusion von sozialen Netzwerken und elektronischen Kommunikationsbeziehungen für autoritäre Regierungen. Die hier verfahrensgegenständliche Malware wurde auf einer Internetseite, welche sich ihrem Inhalt nach an die Teilnehmenden des „Marsches für Gerechtigkeit“ (sog. Adalet-Marsch) wandte, unter Vorspiegelung falscher Tatsachen zum Download angeboten. Bei dieser Website handelte es sich um eine gefälschte Kampagnenseite des Adalet-Marsches. Nachrichten von mehreren gefälschten Twitter-Konten, die in erster Linie mit den Twitter-Profilen der oppositionellen Republikanischen Volkspartei (Cumhuriyer Halk Partisi, CHP) kommunizierten, wiesen die Zielgruppe des Angriffs auf die gefälschte Adalet-Website hin.

Die gefälschte Adalet-Website mit der Domain adaleticinyuru.com wurde am 29. Juni 2017 registriert. Am nächsten Tag wurde jene Malware, die den Gegenstand dieser Anzeige darstellt (im Folgenden: A-Malware), auf diese Website hochgeladen. Die gefälschte Adalet-Website verfügte über die IP-Adresse 178.32.124.175. Diese IP-Adresse wurde von einem sogenannten Share-Hoster betrieben, bei dem sich Kunden Speicherplatz kaufen. Da hinter dieser IP-Adresse ausschließlich türkische Websites lagen, liegt es nahe, dass der Share-Hoster Dienstleistungen für Kunden in der Türkei bereitstellt. Daher liegt es nahe, dass die Website nicht aus dem Ausland, sondern aus der Türkei selbst geschaltet wurde,

AN Bericht, S.5.

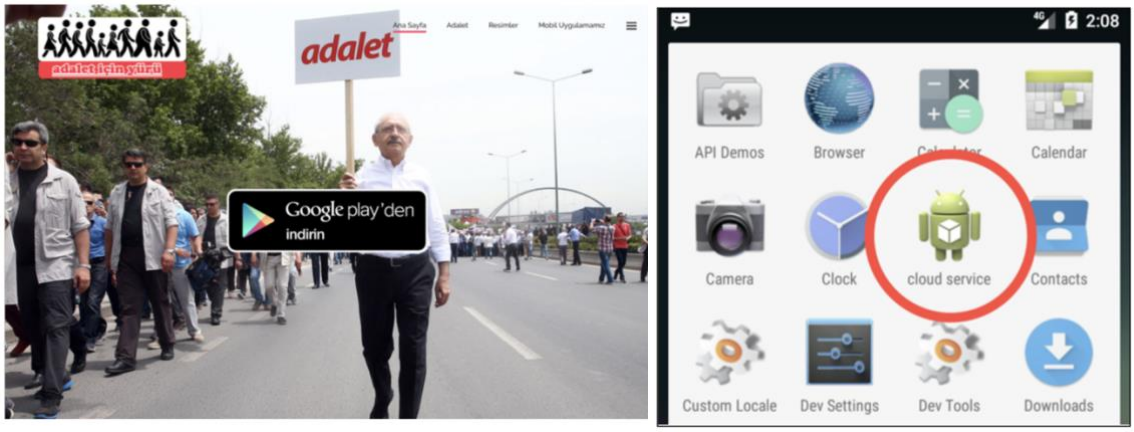
Screenshot von den Twitter-Profilen, die die gefälschte Adalet-Website empfahlen.

Die gefälschte Adalet-Website tat den Besuchern in der Sache keinen Service, sondern warb nur dafür, eine Android-Anwendung auf ihren mobilen Geräten zu installieren. Diese Android-Anwendung wurde, wie auch bei seriösen Applikationen üblich, zentral platziert über einen vermeintlichen Google Play Link inseriert. Die Tweets und die Website selbst implizierten, dass die Software mit dem Dateinamen „KatilBizeV1.0.apk“ (Übersetzung aus dem Türkischen: „Schließ dich uns an!“) einen Cloud- und Kalenderdienst zu Zwecken der Vernetzung der türkischen Opposition bereithalte.

Nach der Installation erschien die verfahrensgegenständliche Anwendung auf dem Startbildschirm der Benutzer und wurde, gepaart mit einem vertrauenserweckenden Android-Symbol, als „Cloud Service“ angezeigt. Anstatt jedoch der türkischen Opposition organisatorische Cloud-Dienste anzubieten, steckte hinter der Anwendung ein getarnter Malware-Agent. Ausweislich dokumentierter Erfahrungen mit FinSpy-Einsätzen in anderen Ländern entspricht dies dem typischen Verhalten und der Standardkonfiguration von FinSpy.

Sobald der Benutzer dann versuchte, die Anwendung zu öffnen, oder wenn das Gerät zum ersten Mal nach dem Download neu gestartet wurde, entfernte sich das vermeintliche Android-Cloud-Symbol vom Startbildschirm. Die Malware wurde für den Nutzer unsichtbar,

AN Bericht, S.5.



Links: Screenshot der gefälschten Adalet-Website. Über den in der Mitte der Ansicht befindlichen und täuschend echt aussehenden Google Play Link wurde die FinSpy-Malware heruntergeladen. Rechts: So erschien die FinSpy-Malware in den Smartphone-Menüs der Betroffenen Die Malware wurde als „cloud service“ angezeigt.

Die gefälschte Adalet-Website ging kurzfristig nach der Veröffentlichung des AN-Berichts vom Netz. Sie ist online archiviert und kann in ihrer damaligen Version vollständig abgerufen werden; die dort befindliche Malware-Datei, die den Gegenstand der Anzeige bildet, kann dort bis heute heruntergeladen werden,

archive.org unter dem Suchbegriff „adaleticinyuru.com“; zuletzt abgerufen am 29. Juni 2019.

Einmal auf dem mobilen Endgerät installiert, konnte die Malware ihre Überwachungsfunktionen aufnehmen.

Dazu gehört der Zugriff auf Adressbuchinformationen, Kalender- und Telefonanrufaufzeichnungen, Dateisystemen, Screenshots und andere Fotos, die Geolokalisierung, das heimliche Abhören des gesprochenen Wortes durch Aktivierung des gerätinternen Mikrofons, sogenannte „Spycalls“ (versteckte Anrufe zur Ermöglichung der Mikrofonüberwachung), das Sammeln von Kommunikations- und Mediendateien, sowie von Daten aus Messengern wie Line, WhatsApp, Viber, Telegram, Skype, Facebook Messenger, Kakao und WeChat,

AN Bericht, S. 13.

II. ZURECHNUNG ZU FINFISHER

1. FORENSISCHE ANALYSE DER MALWARE

Informatiker der Nichtregierungsorganisation „Access Now“ haben anhand ausführlicher forensischer Analysen der A-Malware und Vergleichen mit älteren bekannten Versionen von FinSpy herausgefunden, dass es sich hierbei aufgrund eklatanter Ähnlichkeiten im Quellcode und in den Metadaten mit an Sicherheit grenzender Wahrscheinlichkeit um FinSpy handeln muss. Verglichen wurden die verfügbaren Quellcode-Samples. Der vollständige Quellcode von FinSpy ist der Software nicht zu entnehmen und bis heute nur dem Hersteller bekannt. Der Quellcode-Sample von FinSpy, der als Vergleich genutzt wurde, stammt von einem Datenleck im Jahr 2014,

> vgl. https://www.pnfsoftware.com/blog/finfisher-finspy-mobile-app-for-android-decompiled/; https://netzpolitik.org/2014/gamma-finfisher-hacked-40-gb-of-internal-documents-and-source-code-of-government-malware-published/, zuletzt abgerufen am 03. Juli 2019.

Folgende Ergebnisse der forensischen Malware-Analyse sprechen eindeutig für eine Identität der von der gefälschten Adalet-Website herunterladbaren A-Malware mit FinSpy. Eine ausführliche technische Analyse ist dem technischen Anhang zu entnehmen,

> vgl. technischer Appendix, Anhang 1.

- **Identische Quellcodes:** Die Konfigurationsoptionen beider Malwares – also jene Teile des Quellcodes, die bestimmen, wie genau die Datei operiert, welche Informationen dem Benutzer des betroffenen Endgeräts verborgen werden, usw. – sind sich extrem ähnlich. Teilweise ist der Quellcode sogar vollständig identisch. Einzelne Funktionen, wie beispielsweise der Programmcode für die Überwachung von telefonischen Gesprächen, sind wortgleich (siehe Technischer Appendix, Teil 1).

- **Sprachliche Hinweise im Quellcode:** Ebenfalls beachtlich sind sprachliche Hinweise im Quellcode der A-Malware. So finden sich im Quellcode mehrfach deutsche Wörter wie „einstellung.html“, was in der internationalisierten Programmiererszene ein eher ungewöhnliches Phänomen darstellt. Noch eindeutiger sind jedoch namentliche Hinweise auf FinFisher. So enthalten bestimmte Kommentare unzweideutige Textfragmente wie „FIN_GIFT“ (siehe Technischer Appendix, Teil 2).

- **Fortentwicklung entsprechend strategischer Ziele:** Jene Unterschiede, die zwischen den Quellcodes der A-Malware und älteren Versionen FinSpy bestehen, entsprechen der seit den ersten Leaks von FinFisher verfolgten Strategie der Verbesserung von Geheimhaltung und Verschleierung. Die Veränderung dient gerade der Behebung jener Probleme, die zu dem damaligen Leak führen konnten,

AN Bericht, S. 9, die Befunde der Informatiker von „Access Now“ wurden von einem unabhängigen Expertenteam von „Cure 53“, einem deutschen IT-Sicherheitsunternehmen, fachlich verifiziert, vgl. Anhang V. Genauere forensische Analysen sind dem Technischen Appendix im Anhang 1 zu entnehmen und können bei Bedarf selbst anhand der Software Samples in Anhang 2 durch Sachverständige überprüft werden.

2. WEITERE INDIZIEN

Darüber hinaus sprechen weitere Indizien dafür, dass FinSpy in die Türkei ausgeführt wurde:

- **FinSpy-Funde durch Microsoft:** In seinem Security Intelligence Report für Januar bis Juni 2016 (Band 21) berichtete Microsoft davon, dass über eine systematische Schwachstelle des Betriebssystems viele Microsoft-Nutzer von Malware betroffen waren. Die Malware identifizierte Microsoft eindeutig als FinSpy. Die betroffenen Nutzer kamen zu 84 % aus der Türkei (siehe Technischer Appendix, Teil 3),

  Microsoft Security Intelligence Report, Volume 21, January through June 2016, S. 22-29.

- **Weitere FinSpy Malware in der Türkei:** Auch Access Now stellte neben der A-Malware zusätzliche FinSpy-Aktivität in der Türkei fest. Auf Virus Total, einem von Google betriebenen Online-Virenscanner-Werkzeug, wurde im Zuge des zugrundeliegenden Access Now Berichts aus dem Jahre 2018 eine weitere Malware-Kopie aufgefunden, die von VirusTotal als FinSpy identifiziert wurde (im Folgenden: B-Malware). Diese B-Malware zeichnet sich durch eindeutige Ähnlichkeiten mit der A-Malware aus (siehe Technischer Appendix, Teil 4).

- **Weitere FinSpy Malware in Libyen:** Auch aus Libyen wurde Malware auf VirusTotal hochgeladen, die von dem Dienst eindeutig als FinSpy identifiziert wurde. Auch diese ist der A-Malware, der B-Malware und FinSpy sehr ähnlich. Weil nicht-kommerzielle Akteure in der Regel nicht dazu in der Lage sind, absolut gleichförmige Malware an verschiedensten Orten der Welt zu verteilen, spricht auch dieser Umstand dafür, dass hinter der gefundenen Malware ein professionellen Hersteller steckt (siehe Technischer Appendix, Teil 5).

Diese Anhaltspunkte zeichnen ein eindeutiges Bild: In der Türkei sowie an anderen Orten außerhalb der Europäischen Union tauchte über einen überschaubaren Zeitraum hinweg gleichförmige Malware auf, deren Quellcode weitestgehend den bisherigen Malware-Funden von FinSpy entspricht. Es kann sich dabei nur um eine exportierte Version von FinSpy handeln. Denn es ist nicht nur höchst unwahrscheinlich, dass ein nichtkommerzieller Akteur über die Ressourcen und Expertise verfügt, Malware mit einer Qualität wie FinSpy zu produzieren – der vollständige Quellcode von FinSpy wurde bisher nie außerhalb der Herstellerfirma weitergegeben bzw. gestohlen („geleakt“) – und diese dann weltweit erfolgreich zu vertreiben. Ein solches Vorgehen wäre auch

sinnlos. Für jeden kriminellen Akteur, der darauf abzielt, effektive Spionage-Software zu produzieren, wäre es wesentlich effizienter, diese einfach neu zu konzipieren, anstatt Schritt für Schritt ein hochkomplexes Industrieprodukt zu reproduzieren.

III. ZEITPUNKT DER SOFTWARE-AUSFUHR

Diverse Charakteristika der A-Malware belegen in der forensischen Analyse, dass sie zwischen September und Oktober 2016 erstellt wurde, mithin nach der Einführung der Genehmigungspflichten in die Dual-Use-Verordnung zum 1. Januar 2015 und in die AWV zum 18. Juli 2015.

Der erste Hinweis ist in der Datei "build-data.properties" enthalten, die durch einfaches Entpacken der ursprünglichen Datei überprüft werden kann. Diese Datei enthält Metadaten zur Kompilierung der Androidanwendung, insbesondere einer von ihr verwendeten Bibliothek namens "GMSCore". Dort lässt sich ablesen, dass die Systemkomponente „GMSCore“ aus der A-Malware nicht vor dem 23. September 2016 kreiert worden sein kann.

```
build.time=Fri Sep 23 14\:39\:54 2016 (1474666794)
```

Zwar ist es mit enormem technischen Aufwand möglich, zentrale Metadaten der Grundbestandteile der Malware zu verändern. Hierin läge für den Entwickler keinerlei operativer Vorteil. Vielmehr würde es für die Fortentwicklung der Software erhebliche Verwirrung stiften, wenn diese Bestandteile nicht mehr zeitlich zuordenbar wären.

Außerdem befindet sich in dem Dateibestandteil “META-INF/MANIFEST.MF” ein Hinweis auf eine Android-Entwicklungssoftware namens „Gradle“ in der Version 2.2.1., mit der Android-Programme erstellt werden können.

```
Manifest-Version: 1.0
Built-By: Generated-by-ADT
Created-By: Android Gradle 2.2.1
```

Die Version 2.2.1 wurde jedoch erst im September 2016 veröffentlicht, so dass auch der FinFisher-Trojaner nicht vorher entwickelt worden sein kann,

https://developer.android.com/studio/releases/gradle-plugin; zuletzt abgerufen am 4. Juli 2019.

Darüber hinaus wurde auch die digitale Signatur der A-Malware, ausweislich der hierin enthaltenen Informationen erst am 10. Oktober 2016 erstellt:

```
Owner: CN=RMS
Issuer: CN=RMS
Serial number: 36891ece
Valid from: Mon Oct 10 05:17:01 CEST 2016 until: Fri Oct 04 05:17:01 CEST
2041
Certificate fingerprints:
       SHA1: 98:5D:08:CD:5F:1B:B3:30:28:CA:C6:20:AE:D1:93:2D:DD:26:91:E1
       SHA256:
1E:62:1A:88:3B:CD:9D:1B:D6:D5:61:11:C4:88:EE:10:D4:67:1D:2C:A6:64:F7:27:FE:
72:59:47:8A:68:79:67
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

Somit kann die A-Malware nicht vor Oktober 2016 erstmalig exportiert worden sein,

vgl. Technischer Appendix, Teil 6.

Die unter II. 2. beschriebene B-Malware indiziert zudem, dass die türkische Regierung auch weit nach Oktober 2016 mit FinSpy beliefert wurde. Die VirusTotal-Analyse zeigt, dass die B-Malware am 18. Juli 2017 kreiert und am 21. Juli 2017 auf die VirusTotal-Website hochgeladen wurde. Dies bedeutet, dass Finspy-Versionen bis mindestens Juli 2017 in die Türkei exportiert wurden,

vgl. Technischer Appendix, Teil 4.

IV. KEINE GENEHMIGUNG DER AUSFUHR

Weder die FinFisher GmbH, noch die die Elaman GmbH oder die FinFisher Labs GmbH haben eine Genehmigung zur Ausfuhr der Software in die Türkei oder irgendein anderes außereuropäisches Land erhalten. Auf eine parlamentarische sowie mehrere schriftliche Anfragen zu dem oben beschriebenen Sachverhalt antwortete die Bundesregierung, dass sie seit Einführung der Software-Genehmigungspflicht im Jahre 2015 keinem Unternehmen eine Genehmigung zur Ausfuhr von Intrusion-Software wie FinSpy erteilt habe. Hinsichtlich strafrechtlicher Ermittlungen verwies sie auf die örtlich und sachlich zuständigen Staatsanwaltschaften,

BT-Drucksache 19/3334, S. 5 ff.; BT-Drucksache 19/2419, S. 34; bestätigt in BT-Drucksache 19/2610, S. 38; bestätigt in BT-Drucksache 19/3384, S. 56.

Zuletzt bestätigte die Bundesregierung am 19. Juni 2019, dass sie zwar in 13 Fällen Exportgenehmigungen für Technologie zur

Telekommunikationsüberwachung und in 15 Fällen für Ausrüstung für Überwachungszentren erteilt hat. Sie wies hingegen explizit darauf hin, nie eine Exportgenehmigung für „Intrusion Software“ (im Sinne der Güterlistennummer 4D004 der Dual-Use-Verordnung) erteilt zu haben,

> Antwort der Staatssekretärin im Bundesministerium für Wirtschaft und Energie Claudia Dörr-Voß vom 19. Juni 2019 auf die schriftlichen Fragen an die Bundesregierung der FDP-Abgeordneten Gyde Jensen, S. 1.

Bei FinSpy handelt es sich um Intrusions-Software in diesem Sinne.

F. RECHTLICHE WÜRDIGUNG

Es besteht danach der Verdacht, dass sich die Verdächtigen durch die Ausfuhr von FinSpy in die Türkei zwischen Oktober 2016 und Juni 2017 ohne die erforderliche Genehmigung nach § 18 Abs. 2 Nr. 1 sowie § 18 Abs. 5 Nr. 1 des Außenwirtschaftsgesetzes (AWG) strafbar gemacht haben:

Die Ausfuhr von FinSpy war zum Zeitpunkt der Ausfuhr genehmigungspflichtig (dazu unter I). Die Verdächtigen haben FinSpy ausgeführt, ohne die dafür erforderliche Genehmigung zu besitzen (dazu unter II). Es handelt sich dabei um eine, soweit ersichtlich, vorsätzlich begangene Straftat (dazu unter III), die Straftat ist nicht verjährt (dazu unter IV).

I. GENEHMIGUNGSPFLICHT DER AUSFUHR VON FINSPY

Die Ausfuhr von FinSpy war zum Zeitpunkt der Ausfuhr genehmigungspflichtig. Die Genehmigungspflicht resultiert sowohl aus § 8 Abs. 1 Nr. 2 der Außenwirtschaftsverordnung (AWV) i.V. mit Teil I Abschnitt B, Code 5D902 lit. a) i.V. mit 5A902 der Ausfuhrliste (1.), als auch aus Art. 3 Abs. 1 i.V. mit Anhang I Code 4A005 der Dual-Use-Verordnung (2.).

1. GENEHMIGUNGSPFLICHT GEMÄSS § 8 ABS. 1 NR. 2 AWV

Gemäß § 8 Abs. 1 Nr. 2 AWV i.V. mit Teil I Abschnitt B, Code 5D902 lit. a) i.V. mit 5A902 der Ausfuhrliste ist die Ausfuhr von Software, die der Einrichtung von Überwachungssystemen der Kommunikations- und Informationstechnik dient, genehmigungspflichtig. Bei FinSpy handelt es sich um eine Software, die der Einrichtung von Überwachungssystemen der Kommunikations- und Informationstechnik dient. FinSpy ermöglicht den verdeckten Zugriff auf Telefon- und VoIP-Konversationen, Datensysteme, Bildschirm- und andere Fotos, Standortdaten, die Mikrofone und Verbindungsdaten der Mobiltelefone der Betroffenen sowie auf diverse Applikationen. Hierdurch können vielfältige vertrauliche Telekommunikationsdaten der Betroffenen von der Infiltrationssoftware abgefangen werden,

> vgl. Abschnitt E. I.

FinSpy wird auch nicht von den Bereichsausnahmen der, der Ausfuhrliste vorangestellten, „Allgemeinen Software-Anmerkung (ASA)“ erfasst, da sie weder frei erhältlich noch allgemein zugänglich im Sinne der Legaldefinitionen der Begriffsbestimmungen ist. Soweit die A-Malware lediglich als Wartung oder Update einer früheren Fassung von FinSpy zu bewerten sein sollte, unterliegt auch dies der Genehmigungspflicht, da gem. Teil I Abschnitt B, Code 5D902 der Ausfuhrliste die Lieferung von Software zur „Verwendung“ von Überwachungseinrichtungen i.S.v. 5A902 auch Wartungsleistungen erfasst. In den Begriffsbestimmungen der Ausfuhrliste wird „Verwendung“ definiert als „Betrieb, Aufbau (einschließlich Vor-Ort-Aufbau), Wartung (Test), Reparatur, Überholung, Wiederaufarbeitung.“

Die Genehmigungspflicht besteht bereits seit dem 18. Juli 2015, und damit auch zum mutmaßlichen Zeitpunkt der Ausfuhr zwischen Oktober 2016 und Juni 2017,

> 4. Verordnung zur Änderung der AWV vom 13.07.2015, Bundesanzeiger AT 17.07.2015 V1.

Es existieren keine Übergangsvorschriften. Selbst etwaige bestehende Vertragspflichten, die bereits vor dem 18. Juli 2015 eingegangen wurden und zukünftige Updates oder Wartungen beinhalten könnten, stünden der Genehmigungspflicht nicht entgegen. § 1 Abs. 1 AWV differenziert zwischen genehmigungsbedürftigen Rechtsgeschäften und genehmigungsbedürftigen Handlungen. In § 2 Abs. 3 AWG wird die Ausfuhr als rein tatsächliche Handlung legaldefiniert.

2. GENEHMIGUNGSPFLICHT GEMÄSS DUAL-USE-VERORDNUNG

Die Genehmigungspflicht aus der Dual-Use-Verordnung resultiert aus Art. 3 Abs. 1 i.V. mit Anhang I Code 4A005. Bei FinSpy handelt es sich aufgrund der o.g. umfassenden Überwachungsfunktionen um „Intrusion-Software“, die im Sinne der Legaldefinition „besonders entwickelt oder geändert wurde, um die Erkennung durch ‘Überwachungsinstrumente’ zu vermeiden, oder ‘Schutzmaßnahmen’ eines Rechners oder eines netzfähigen Gerätes zu umgehen“ und die Operation der „Extraktion von Daten oder Informationen aus einem Rechner oder einem netzfähigen Gerät oder Veränderung von System- oder Benutzerdaten“ auszuführen.

Die Genehmigungspflicht für Intrusions-Software aus der Dual-Use-Verordnung bestand bereits zum mutmaßlichen Zeitpunkt der Ausfuhr zwischen Oktober 2016 und Juni 2017, denn sie wurde mit der Delegierten Verordnung (EU) Nr. 1382/2014 der Kommission mit Wirkung zum 1. Januar 2015 in die Dual-Use-Verordnung eingeführt. Übergangsvorschriften existieren nicht,

> https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R1382.; zuletzt abgerufen am 02. Juli 2019.

II. AUSFUHR OHNE ERFORDERLICHE GENEHMIGUNG

Die Verdächtigen haben FinSpy mutmaßlich zwischen Oktober 2016 und Juni 2017 in die Türkei ausgeführt. Die Ausfuhr von Software ist in § 2 Abs. 3 Nr. 2 AWG legaldefiniert als die Übertragung von Software und Technologie aus dem Inland in ein Drittland einschließlich ihrer Bereitstellung auf elektronischem Weg für natürliche und juristische Personen in Drittländern. Die Dual-Use-Verordnung versteht gemäß Art. 2 Nr. 2 lit. iii) unter Ausfuhr die „Übertragung von Software oder Technologie mittels elektronischer Medien wie Telefax, Telefon, elektronischer Post oder sonstiger elektronischer Träger nach einem Bestimmungsziel außerhalb der Europäischen Gemeinschaft; dies beinhaltet auch das Bereitstellen solcher Software oder Technologie in elektronischer Form für juristische oder natürliche Personen oder Personenvereinigungen außerhalb der Gemeinschaft. Als Ausfuhr gilt auch die mündliche Weitergabe von Technologie, wenn die Technologie am Telefon beschrieben wird“.

Wie unter Abschnitt E beschrieben liegen zahlreiche Belege für die Verwendung von FinSpy durch einen türkischen Abnehmer vor. Die auf der falschen Adalet-Webseite gefundene Malware A ist mit an Sicherheit grenzender Wahrscheinlichkeit die FinSpy-Malware, wie sie von den Verdächtigen produziert und vertrieben wird,

> vgl. Abschnitt E. II.

Eine Analyse der Software zeigt, dass die Malware A frühestens im Oktober 2016 hergestellt wurde,

> vgl. Abschnitt E. III.

Es spricht vieles dafür, dass die Entwicklung und der Vertrieb von FinSpy und anderen FinFisher-Produkten in München stattfindet. Insbesondere wird FinSpy nicht mehr in England produziert und vertrieben. Im OECD Verfahren gegen Gamma International UK LTD vor dem UK National Contact Point for the OECD Guidelines for Multinational Enterprises (Referenznummer BIS/15/93), in dem die britische Kontaktstelle Verstöße von Gamma International UK LTD gegen die OECD-Leitsätze für multinationale Unternehmen festgestellt hat, hat der Unternehmensvertreter von Gamma darauf hingewiesen, dass Exporte von FinFisher-Produkten aus Großbritannien im April 2012 eingestellt wurden,

> “Gamma has declined to tell the UK NCP whether any supply was made (for customer confidentiality reasons), but has told the UK NCP that Gamma International UK Limited ceased any exports of Finfisher software in April 2012 and soon after that (around July 2012) ceased any exports of hardware components of the system (some components continued to be shipped to Germany later in 2012 but not as exports)”, UK National Contact Point for the OECD Guidelines for Multinational Enterprises: Privacy International & Gamma International UK Ltd: Final statement after examination of complaint, December 2014, online abrufbar unter https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International

_and_Gamma_International_UK_Ltd.pdf, zuletzt abgerufen am 27. Juni 2019.

Die FinFisher Labs GmbH mit Sitz in München ersetzte mit Handelsregistereintrag vom 26. September 2013 die Gamma International GmbH. Die FinFisher GmbH mit Sitz in München ersetzte mit Handelsregistereintrag vom 13. Oktober 2013 die Gamma International Sales GmbH. Die Finfisher Limited mit Sitz in Winchester, Hampshire, United Kingdom ist am 24. Februar 2014 aufgelöst worden,

vgl. https://beta.companieshouse.gov.uk/company/07346435, zuletzt abgerufen am 27.06.2019.

Die Elaman GmbH, die FinFisher GmbH und die FinFisher Labs GmbH befassen sich nach den Einträgen im Handelsregister mit Handel und Vertrieb einschlägiger Softwareprodukte. Keines der drei Unternehmen besaß eine Genehmigung für eine Ausfuhr nach Januar 2015,

BT-Drucksache 19/3334, S. 5 ff.; BT-Drucksache 19/2419, S. 34; bestätigt in BT-Drucksache 19/2610, S. 38; bestätigt in BT-Drucksache 19/3384, S. 56.

III. STRAFRECHTLICHE VERANTWORTLICHKEIT DER VERDÄCHTIGEN

Durch die ungenehmigte Ausfuhr von FinSpy zwischen Oktober 2016 und Juni 2017 haben sich die Verdächtigen gemäß § 18 Abs. 2 Nr. 1 AWG sowie § 18 Abs. 5 Nr. 1 AWG strafbar gemacht. Der Sachverhalt legt nahe, dass die Verdächtigen vorsätzlich gegen die Ausfuhrbestimmungen verstoßen haben (und nicht lediglich eine Ordnungswidrigkeit gemäß § 19 Abs. 1 AWG begangen wurde).

Die Verdächtigen waren im besagten Zeitraum Geschäftsführer der Elaman GmbH, der FinFisher Labs GmbH bzw. der FinFisher GmbH. Da die Firmen nur an den überschaubaren Kundenkreis von Regierungen und regierungsnahe Organisationen liefern, besteht kein Zweifel, dass sie Kenntnis von allen laufenden Lieferbeziehungen mit ausländischen Regierungen - wie in diesem Fall der Türkei – haben müssen. Weder sind die Unternehmen so groß noch die Zahl der potentiellen Abnehmer von FinSpy so hoch, dass es naheliegen würde, Ausfuhrentscheidungen ohne Kenntnis der Geschäftsführer zu treffen und durchzuführen. Die Tatsache, dass die Bundesregierung, ausweislich ihrer Auskunft vom 19. Juni 2019, seit Januar 2015 keine Ausfuhrgenehmigung für genehmigungspflichtige Intrusions-Software erteilt hat, deutet zudem entweder darauf hin, dass die Ausfuhr von entsprechender Software kein alltägliches Geschäft ist, was umso mehr für eine Kenntnis der Geschäftsführer spräche, oder aber darauf, dass in den letzten Jahren über die Geschäfte mit der Türkei hinaus auch zahlreiche weitere Ausfuhren unter Verstoß gegen die Ausfuhrbestimmungen stattgefunden haben.

Der Tatverdacht richtet sich auch gegen die jeweiligen Verantwortlichen auf den ausführenden Ebenen im Unternehmen, die hier wegen fehlender Kenntnis der Unternehmensstrukturen nicht namentlich benannt werden können.

IV. ZUR VERJÄHRUNG

Da nahe liegt, dass die Verdächtigen FinSpy bis Juli 2017 in die Türkei ausgeliefert haben,

vgl. Anhang 1, Teil 4,

verjährt die Strafbarkeit gem. § 18 Abs. 2 Nr. 1 und § 18 Abs. 5 Nr. 1 AWG nicht vor Juli 2022, § 78 Abs. 3 Nr. 4 StGB.

G. MÖGLICHE ERMITTLUNGSMASSNAHMEN

Wir regen an, den Sachverhalt durch die nachfolgenden Ermittlungsmaßnahmen weiter aufzuklären:

Vernehmung folgender sachverständiger Zeugen:

- Gustaf Björksten, Chief Technologist bei Access Now, gustaf@accessnow.org

  Der Zeuge Björksten ist Mitautor der Acces-Now-Studie und wird die Validität der technischen Analyse bezeugen.

- Dr.-Ing. Mario Heiderich, Cure53, Bielefelder Str. 14, 10709 Berlin

  Der Zeuge Heiderich arbeitet bei dem IT-Unternehmen Cure53 und hat die Validität der Aussagen der Access Now Studie überprüft, vgl. Anhang 6.

- Matt Miller; Microsoft Security Response Center

  Der Zeuge Miller ist Mitautor des Microsoft Security Intelligence Reports, Volume 21. Der Zeuge wird die Richtigkeit der in diesem Bericht getroffenen Aussagen zu FinSpy-Funden in der Türkei bestätigen.

Durchsuchungen und Beschlagnahmen:

Durchsuchung der Unternehmensräume der vorbezeichneten Unternehmen in München und Beschlagnahme von Unterlagen und Datenträgern, Sicherstellung von

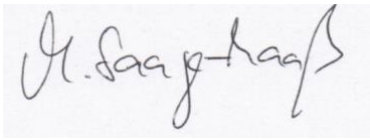
- Kopien der FinSpy Schadsoftware; dabei werden voraussichtlich Kopien aufgefunden werden können, die mit der verfahrensgegenständlichen A-Software identisch sind,

- Kundenkorrespondenzen mit der türkischen Regierung oder anderen einschlägigen Akteuren sowie interne Korrespondenz, welche Aufschluss über die Handlungen und das Wissen der Verdächtigen und weiterer Unternehmensangehöriger geben,

- andere Unterlagen, die auf den oben angeführten Sachverhalt hindeuten, insbesondere zu den Erlösen aus ungenehmigten Exporten, was für die Abschöpfung der so erzielten Vermögenswerte wesentlich sein dürfte.

Mit freundlichen Grüßen

Ulf Buermeyer, Vorsitzender der Gesellschaft für Freiheitsrechte e.V.



Miriam Saage-Maaß, Vice Legal Director des European Center for Constitutional and Human Rights

Christian Mihr, Geschäftsführer bei Reporter ohne Grenzen

Andre Meister, Netzpolitik.org

H. **ANHÄNGE**

1. Technischer Appendix

2. USB-Stick mit
- Sample der A-Malware
- Sample der B-Malware
- Sample der FinSpy-Malware 2014
- digitale Fassung der Strafanzeige und der Anhänge

3. Relevante Handelsregisterauszüge

4. Ausdruck des Access Now Berichts: FinFisher changes tactics to hook critics, Mai 2018

5. Ausdruck des Microsoft Security Berichts, Seiten 22-29

6. Ausdruck der von der IT-Firma Cure53 durchgeführten Überprüfung der Aussagen des Access Now Berichts, März 2018