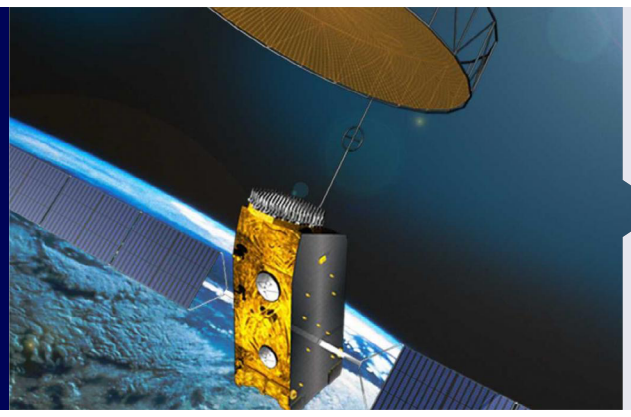
SONDERAUSGABE

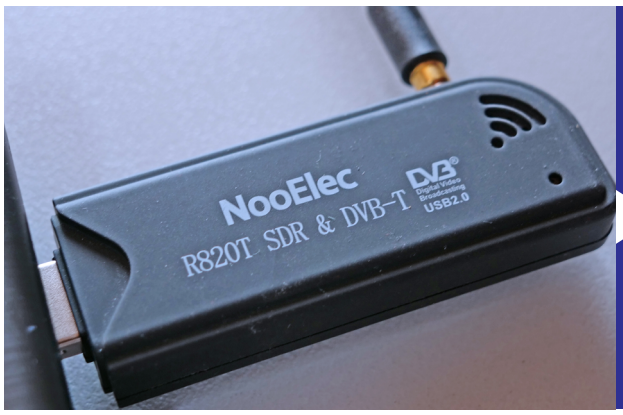
TecTime Magazin

BEST OF 17-19

SPIO



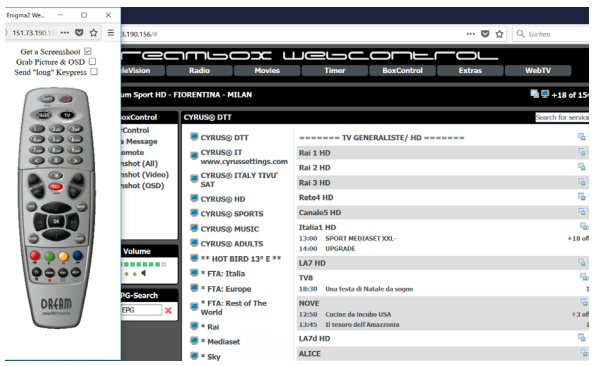
DAS INMARSAT SYSTEM



SDR

Feed-signale mit SDR

Schuldhaftes Verhalten der Verbraucher?



MEDIEN

VORSICHT ABZOCKE!

NOSTALGIE vor 23 Jahren

EDITORIAL

Liebe Leser,

mit dieser kostenlosen Bonus-Ausgabe – ein Rückblick auf Stories, die mir besonders viel Schreibespaß bereiteten - möchten wir uns nochmals bei allen die uns je gesehen oder gelesen haben bedanken. Bedanken dafür, dass so viele von Anfang an ausgeharrt haben und in den schwierigsten Zeiten uns motiviert und unterstützt haben.

Wir bedanken uns bei den vielen neuen Abonnenten, die Technik-Stories nicht aus dem Daten-Überfluss des Internets konsumieren, sondern unsere Sicht auf die Dinge und das Können schätzen.

Einige werden Beiträge aus dieser Sonderausgabe zum ersten Mal lesen, weil sie irgendwann das Abo nicht mehr erneuert haben. An die lautet unser Apell: „kommt bitte zurück zu uns!!! Wir brauchen Euch!“

Und die, die uns noch gar nicht kennen, denen wollen wir guten investigativen Technik-Journalismus bieten.

Herzliche Grüße,
Euer Dr.Dish

VORSICHT ABZOCKE

Wer kennt sie nicht, die teils aggressive Werbung für eine wahre Wunderantenne. Seit einigen Jahren wird sie unter verschiedenen Namen und Preisen vermarktet. Immer wenn die Produktnamen einen mehr als schlechten Ruf bekommen (FreeSeeTV, TV Radius oder TV Fox), wird gibt es schnell einen neuen Namen. Zurzeit ist es die DigiTennaMax. Und um deren Google-Werbung kommt man kaum herum. Selbst auf den Homepages einiger Fachzeitschriften im Bereich Satellit und Kabel tauchen sie regelmäßig auf.

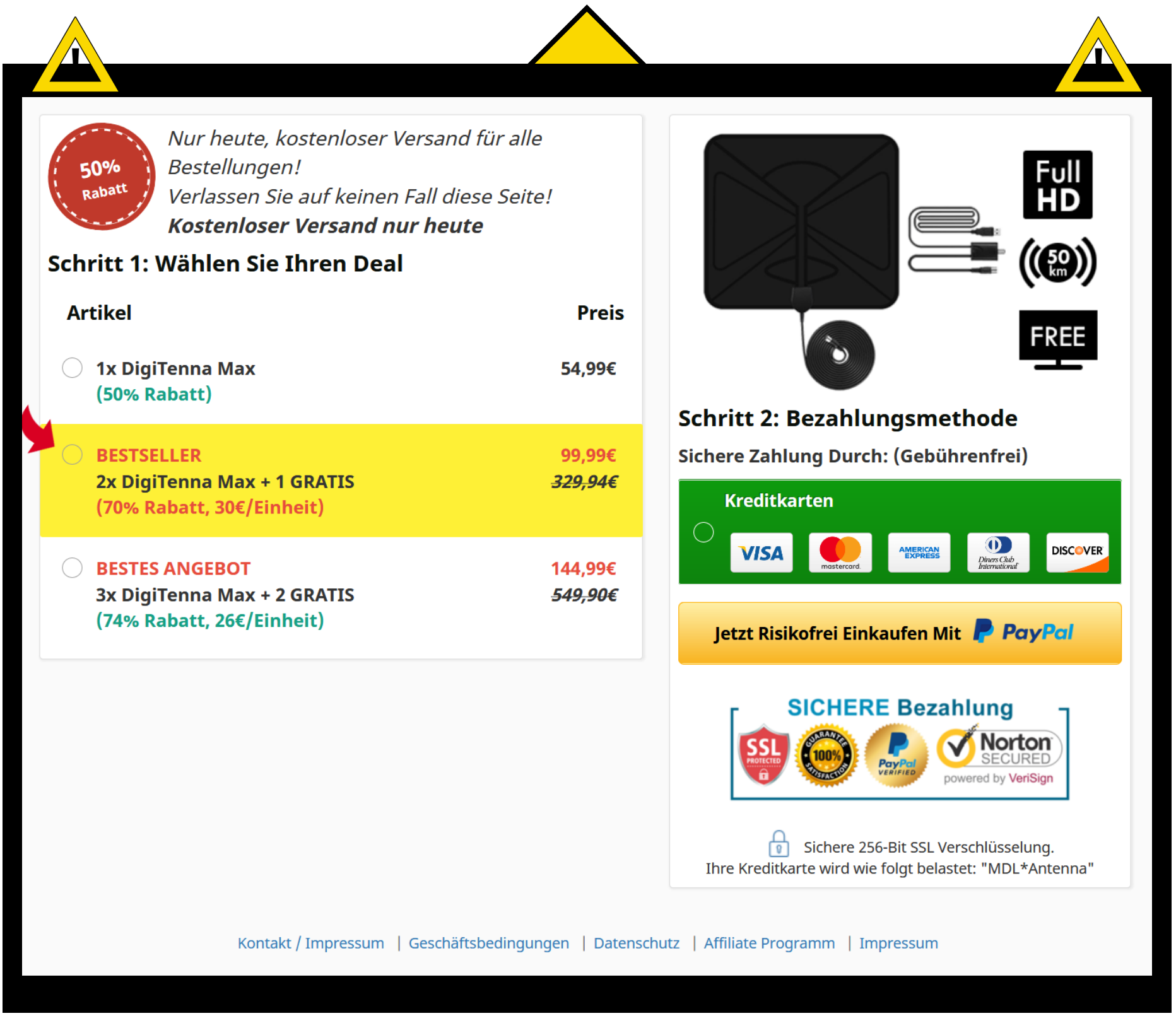
Dem Laien wird vorgegaukelt, das Produkt sei das Ergebnis geheimer Militärtechnik und es sei langlebig, kraftvoll und von hoher Qualität. Aber vor allen Dingen heißt es der freie Empfang von hunderten HD Sendern überall auf der Welt sein gesichert. Ohne

Abo oder Kabelgebühren. Das alles Dank der Offenlegung geheimer Frequenzen auf denen die Kabelanbieter verpflichtet sind Ihr Programm terrestrisch zusätzlich abzustrahlen. Diese niedrigen Frequenzen mache sich die DigiTennaMax zunutze. Das mit den geheimen Frequenzen der Kabelgesellschaften ist natürlich Blödsinn. Es gibt sie nicht! Die hochgelobte Antenne greift einfach auf den DVB T2-Empfang zurück. Soll heißen, sie versucht es zumindest. Und damit die ganze Sache glaubhafter erscheint, listet der Anbieter eine ganze Reihe von Zuschriften glücklicher Besitzer dieser Wunderantenne.

Lässt sich nun ein Interessent von all dem blenden und schreitet zur Bestellung, dann wird Zeitdruck aufgebaut, denn auf der Seite erscheint eine Zeitanzeige, die ihm sagt in xx Minuten sei der Sonderpreis ungültig und somit werde die Antenne teurer. Im Bestellformular ist vom Anbieter schon einmal die Bestellung von zwei Antennen eingekreuzt und so mancher fällt in der Eile darauf hinein. Bezahlt werden die rund 55 Euro pro Stück mit Kreditkarte oder mit PayPal. Bei PayPal wird mit dem Käuferschutz geworben.

Das Geld ist erst einmal weg und nun beginnt die Wartezeit. Und irgendwann kommt eventuell (es gibt Fälle da kam überhaupt nichts) ein Paket an. Der stolze Besitzer der DigiTennaMax macht sich an die Installation. Alle Kabel liegen bei und die Passiv-Antenne entpuppt sich als Folienantenne für die Fensterscheibe. In Deutschland erhältlich für 8,99 Euro bei Amazon. Die Antenne ist passiv, das heißt, sie hat keinen integrierten Verstärker.

Unser Käufer hat zwar einen etwas älteren Flachbildschirm, jedoch keinen DVT T2 Tuner verbaut und einen externen Receiver hat er auch nicht. In der Werbung war davon keine Rede.



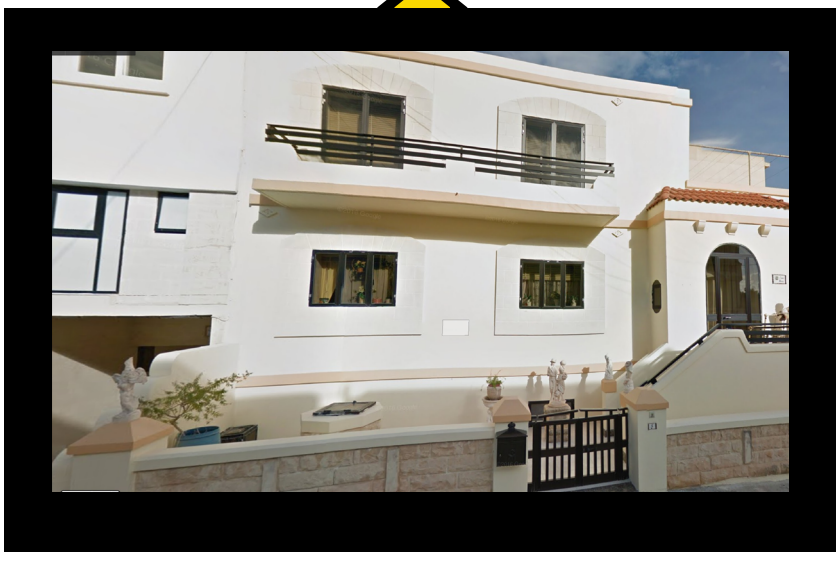
Es hieß nur: Antenne am Fenster befestigen, Kabel anschließen und auf geht's. Resultat zu den 55 Euro für die Antenne kamen nochmals 30 Euro für den billigsten DVB T2-Receiver hinzu.

Einen Tag später war der Receiver da und der automatische Suchlauf wurde gestartet. Ganze vier Sender wurden eigelesen, doch das Signal war so schwach, dass Bild und Ton den Schwellenwert nicht überspringen konnten. Auch die Umplatzierung der Antenne brachte keinen Erfolg. Da blieb nur noch die zugesagte Rückgabe der Wunderantenne übrig. Es wurde eine Adresse für die Rückgabe in Bratislava angegeben. Das Paket dorthin kostete noch einmal 16,50 Euro Porto. Bei PayPal wurde Konfliktlösung beantragt und daraus wurde ein „Case", der bis heute nicht gelöst wurde. Mails wegen der Rückerstattung des Kaufpreises beim Anbieter MDE Commerce Ltd. In Malta blieben unbeantwortet und nach vier Wochen kam das Paket als unzustellbar aus Bratislava zurück.

Und hier begann unsere Recherche. Begonnen wurde mit den Rückgabestationen. Die Adressen wechseln immer wieder in sind zum Teil nicht existent. Es gab während unserer Recherche eine in Kleve, Deutschland, eine in den Niederlanden, eine in Estland und die aktuelle in Bratislava. Hinter keiner dieser Anschriften gab es einen Ableger oder Beauftragten der MDE Commerce Ltd.

Die MDE Commerce Ltd. Ist in Malta unter der Registernummer C86613 beim dortigen Handelsgericht eingetragen. Die Firma gibt selbst den Firmensitz mit 72, TRIQ TAL-QROQQ, MSIDA, Malta an. Das Haus ist ein kleineres Gebäude im Zentrum und beherbergt Briefkastenfirmen.

Eingetragen ist die Firma jedoch in der 1, Triq L Gherien und diese Villa wird durch den Geschäftsführer Ricardo Pereira bewohnt.



Offensichtlich lebt es sich ganz gut mit dem Handel von Wunderantennen. Bei näherer Untersuchung stellt sich heraus, dass die offizielle Telefonnummer +37256076645 in Estland beheimatet ist. Ruft man dort an, kommt eine Ansage, dass der gewünschte Teilnehmer z.Zt. nicht erreichbar sei. Ob Ricardo Pereira nur ein Strohmann ist, oder der Kopf hinter dem Unternehmen, bleibt erst einmal offen. Fest steht nach unseren Recherchen, dass MDE Commerce Ltd. mit dem Verkauf der DigiTennaMax wohl nur das Porto verdient. MDE Commerce Ltd. „verkauft" über einen Shop im Internet alles Mögliche. Vom Robotstaubsauger bis zum Luftreiniger. Nur die bestellten Waren kommen nicht an oder aber in den Paketen befindet sich wertloses Plastikmaterial. Auf der Seite der französischen Organisation „Signal-Arnaques" findet man zahllose Berichte betroffener Menschen. Der Schaden dürfte in die Millionen gehen.

FAZIT

Hände weg von Produkten der Firma MDE Commerce Ltd. und vor allen Dingen der DigiTennaMax oder wie si in Zukunft auch immer heißen mag.

GEFÄHRLICHE APPS IN MEDIAPLAYERN

Gerd. H aus Brandenburg ist wie die meisten Menschen ein Laie oder einfach nur faul, wenn es um die Installation von Apps in einem Mediaplayer geht. Einschalten und alles muss da sein, das ist seine Devise. Und da kam die Werbung für den Mediaplayer „MXQ Pro Android TV Box - Fully Loaded“ gerade recht. Kodi und Mobdro waren an Bord und so stand dem kostenlosen Genuss von Spielfilmen und Pay-TV nichts mehr im Wege.

40 Euro gingen per Paypal an den Anbieter und vier Tage später war er stolzer Besitzer der kleinen Box. Und weil das so günstig war, abonnierte er auch noch gleich Netflix dazu.

Gerd H. war glücklich.

Allerdings gab es nach ein paar Wochen ab und zu Probleme mit Netflix. Der Streamingdienst verweigerte den Zutritt mit dem Hinweis, er sei bereits eingeloggt. Als dann in der Liste der kürzlich angesehenen Filme Titel zu sehen waren, die ihm völlig unbekannt waren, hätte er wach werden müssen.

Das wurde er erst, als von seinem Paypal Konto (Benutzername und Passwort waren identisch den Daten für Netflix) das gesamte Plus von 835,- Euro an einen Empfänger in Asien abwanderte.

Ein Einzelfall? Mitnichten! Der Umsatzzahlen bei den Mediaplayern steigen in Europa rasant an, doch liegt die Nutzung noch weit hinter der der Amerikaner. 75% der Amerikaner be-richten, dass sie mindestens mehrmals im Monat Unterhaltung streamen.

Das meiste davon geschieht über seriöse und bekannte Dienste wie Netflix, Amazon Prime Video und Hulu. In weniger als einem Jahrzehnt haben rund 250 Millionen Kunden weltweit diese Dienste in Anspruch genommen. Und diese Zahl wird sprunghaft ansteigen, wenn andere große Medienunternehmen in den kommenden Monaten ihre eigenen Streaming dienste einführen. Während kein Service absolut narrensicher ist, haben die Verbraucher bei bekannten Marken berechtigte Erwartungen an die Sicherheit.

Einige Verbraucher unternehmen jedoch riskante Schritte, um außerhalb der Mainstream-App-Marktplätze shoppen zu gehen, um ihre Wunsch-inhalte zu finden. Wenn Sie sich die Studentenwohnheime, die Männer-höhle eines Freundes oder das Schlafzimmer eines Teenagers ansehen, können Sie diesen Unterbau des Streamings finden: Pirateriegeräte wie Jailbreak Amazon Fire TV-Stick oder eine sogenannte Kodi-Box, die alle mit illegalen Apps betrieben werden.

In einigen Fällen handelt es sich bei diesen Endgeräten um Set-Top-Boxen - oft aus China importiert - mit wenig vorinstallierter Software, die die Geräteverkäufer mit "Kodi" und Apps aufladen, die auf das Piraterie-Ecosystem zugreifen. In anderen Fällen werden legitime Geräte mit einer Software geladen, die den Zugriff auf illegale Apps ebenso einfach macht, wie auf legitime Apps wie Netflix oder Hulu. Nach dem Laden der Geräte mit den illegalen Apps (einige davon sind kostenlos und andere erfordern eine Abonnementgebühr) werden die Geräte gegen einen erheblichen Aufschlag an die Verbraucher verkauft - oft unter dem Motto: "Zahle niemals mehr für PayTV".

Die Geräte werden hauptsächlich für einen Zweck verwendet: den illegalen Zugriff auf raubkopierte Filme, Fernsehsendungen, Spiele und Musik. In einigen Fällen werden sie verwendet, um Zugang zu Filmen zu erhalten, die sich noch im Kino befinden.

Pirateriegeräte stellen nicht nur eine Bedrohung für das legitime Content-Ecosystem dar, sondern auch für die Cybersicherheit insgesamt. Da Millionen von Geräten - von Telefonen, Tablets und Unterhaltungsgeräten bis hin zu Smart TVs, Thermostaten und Türklingeln - in das Haus gelangen, ist die Fähigkeit von Hackern, ein Haus über diese Boxen zu infiltrieren, unproblematisch.

Der Grund dafür, dass Kodi-Boxen besonders anfällig für Hacking sind, ist zweifach. Zuerst umgehen die Boxen die Sicherheitsmaßnahmen, die im Router enthalten sind. Zweitens sind bei der Konfiguration dieser Boxen normale Sicherheitsvorkehrungen in der Regel nicht installiert oder deaktiviert, um Anwendungen für das Streaming von illegalen Inhalten zu unterstützen. Für Android-Nutzer öffnet die Deaktivierung von Sicherheitsfunktionen beispielsweise einen bestimmten Port, auf dem Botnets routinemäßig scannen.

Einmal erkannt, greift der Hacker gezielt auf dieses Gerät, um es zu infizieren. Darüber hinaus müssen Benutzer, um die Apps nutzen zu können, der App oft vollen Administratorzugriff gewähren, der die Berechtigung zum Zugriff auf den gesamten Speicher des Geräts, sowie dessen Standort und andere Sicherheitsvorkehrungen beinhaltet. Nachdem die XMBC Foundation, die Kodi entwickelte, zunächst Beschwerden darüber ignoriert hatte, wie sehr Kodi anfällig für Piraterie ist, verurteilte sie Piraten-Addons, weil sie Kodi einen schlechten Ruf einbringen. Das war es dann aber auch

schon. Der Löwe hat mal kurz gebrüllt.

Angesichts der zunehmenden Bedenken haben Digital Citizens (*1) und Dark Wolfe (*2) eine Untersuchung eingeleitet. Um das Ecosystem der Streaming-Piraterie zu erforschen, haben die Forscher von Dark Wolfe sechs Streaming-Geräte erworben, die die Kodi-Plattform nutzen. Die Quellen der Einkäufe waren unterschiedlich:

Online-Käufe von Websites, die bei der Suche über Google, Bing und Dogpile gefunden wurden und der Direktkauf bei einem lokalen Händler. Diese Geräte werden typischerweise als "vorinstalliert" mit Apps vermarktet, die es dem Benutzer ermöglichen, kostenlos oder gegen eine geringe monatliche Abo-Gebühr auf On-Demand-Filme (auch solche, die sich noch im Kinostart befinden) und Fernsehprogramme, sowie Live-Echtzeitübertragungen und Kabelunterhaltung, Sport- und Nachrichtenkanäle aus aller Welt zuzugreifen. Die illegalen Apps wiederum werden oft in App-Repositories gesammelt, die als "Repos" bezeichnet werden, in denen der Benutzer dann die gewünschten Apps herunterladen kann.

Mediaplayer mit illegalen Apps werden aus Sicherheitsgründen oft auf Dark Web Marktplätzen beworben. Verkäufer bieten Geräte wie den "MXQ Pro fully loaded" an, die mit einem kompletten Satz von Kodi-Builds versehen sind und in den meisten Ländern als illegal gelten.

„Dream Market“ und "rstforums", etablierte Untergrundmärkte, bieten haufenweise illegale Mediaplayer an. „Dream Market“ ist ein Dark Net Marktplatz im Internet, auf dem eine Vielzahl illegaler Produkte zum Verkauf stehen - darunter Medikamente, Falschgeld, Waffen und gefälschte Kreditkarten.

Ein weiterer Bestandteil der Piraterie gestützten Ecosysteme ist die Werbung. Wie „Digital Citizens“ bei Piraterie-Websites festgestellt hat, integrieren illegale Akteure Mainstream-Werbung (z.B. Mini Cooper) in ihre Angebote. Damit schaffen sie eine potenzielle neue Einnahmequelle und erwecken den Eindruck von Seriosität.

Die Forscher von Dark Wolfe stellten fest, dass einige Piraterieverfechter zwar die "Vorteile" kostenloser Inhalte propagieren - UFC-Kämpfe, Live-Sportveranstaltungen, mehr Filme -, aber die Nutzer nicht vor der potenziellen Bedrohung durch Malware warnen. Das ist beunruhigend, da diese Software bei den Hackern beliebt ist, weil sie es ihnen ermöglicht, Malware recht unkompliziert über den Inhalt zu verbreiten.

FILME, GELD UND MALWARE: WIE DIE PIRATEN UNTERNEHMEN UND VERBRAUCHER ANGREIFEN

Die Enthüllung, dass Kriminelle die Mediaplayer ins Visier nehmen, um Malware zu installieren, ist ein neuer Schlag gegen die Bemühungen Verbraucher zu schütze. Die Untersuchung von „Digital Citizens“ ergab, dass Apps, die auf Streaming-Geräte heruntergeladen wurden, die Benutzer einem viel höheren Risiko eines Malwarebefalls im Heimnetzwerk aussetzen.

Die Akteure stehlen alle Daten aus den Geräten im Heimnetzwerk. Einschließlich die der Dienste wie Netflix- und Amazon-Konten.

Die Malware sucht nach dem Weg zu jedem angeschlossenen Gerät und gefährdet so ein ganzes Heimnetzwerk. Die Erweiterung der Infektionsvektoren (die Wege vom Computer eines Angreifers zu verbundenen Geräten im Netzwerk eines Benutzers - wie z.B. ein Kindertablet, ein neuerer Kühlschrank oder ein Computer) erhöht die Wahrscheinlichkeit eines Datendiebstahls.

Die durch Dark Wolfe identifizierte Malware stammt von Apps, die entweder bereits bei der Entwicklung infiziert, über Updates infiziert , oder über den Stream infiziert wurden. Sobald sie im Netzwerk ist, fügt Malware alle lokal gespeicherten Medien hinzu, die sie im Netzwerk der miteinander verbundenen Geräte eines Benutzers findet und macht sie zu einem Teil seines Medienkatalogs, einschließlich der Filme, Bilder und Anwendungen des Benutzers. Selbst wenn das illegale Gerät später aus dem Heimsystem entfernt wird, bleibt Malware, die bereits benachbarte Systeme infiziert hat, im Netzwerk des Benutzers.

Die Ermittler haben zwei Möglichkeiten identifiziert, wie Kriminelle die gestohlenen Daten monetarisieren um die eigenen Taschen füllen. Der erste ist der Verkauf der Anmeldeinformationen eines legitimen Benutzers. Gefälschte Netflix-Anwendungen, wie "FreeNetflix", erleichtern den illegalen Zu-

griff auf ein legitimes Abonnement und ermöglichen es einer Person, die nach nicht lizenzierten Inhalten sucht, auf das Raubkopien-Abonnement eines legitimen Benutzers zuzugreifen.

Die Betreiber von FreeNetflix bieten den Service für eine einmalige Zahlung von 10 US-Dollar an. Inklusive aller Updates. Rotierende Log in-Informationen helfen Betreibern von „FreeNetflix“mehrere mögliche Probleme zu vermeiden, einschließlich der möglichen Überbelegung des Abonnements eines einzelnen legitimen Benutzers durch mehrere illegale Benutzer auf einmal. Dadurch wird vermieden, dass der Dienst legitimer Benutzer wiederholt unterbrochen wird, wodurch erzwungene Ausfälle, Passwortänderungen und Kontosperren reduziert werden.

Gefälschte Netflix-Anwendungen ergänzen auch die legitimen Netflix-Streams und bieten zusätzliche Inhalte, die nicht in der eigenen Anwendung von Netflix zu finden sind, einschließlich raubkopierter Streams von Sportereignissen, Musik, Spielen und sogar einigen selbst erstellten Inhalten, was sie sehr begehrenswert macht.

Andere Forscher haben herausgefunden, dass Addons von Drittanbietern für Kodi verwendet wurden, um Linux- und Windows-Krypto-Währungs-Mining-Malware zu verteilen. "***Die Malware hat eine mehrstufige Architektur und setzt Maßnahmen ein, um sicherzustellen, dass ihre endgültige Nutzlast - der Kryptominer - nicht leicht auf das bösartige Addon zurückzuführen ist***", berichtete das Sicherheitsunternehmen ESET in einem Bericht vom September 2018.

Während die Quellen der Malware veraltet waren, oder keine Malware mehr verbreiteten, warnte ESET davor, dass "unwissentliche Opfer", die die Kryptominer-Malware heimlich auf ihren Geräten installiert hatten, wahrscheinlich immer noch betroffen sind.Piraterie-Mediaplayer oder Set-Top-Boxen sind besonders anfällig für Malware, da typische Sicherheitsvorkehrungen selten installiert oder einfach deaktiviert werden, um Piraterie-Streaming-Anwendungen zu ermöglichen.

Die Geräte verfügen über deutlich mehr "Angriffsvektoren" als andere angeschlossene Geräte, wie z.B. Smart TVs oder Kühlschränke, was das Risiko erhöht, dass Hacker auf Benutzernamen oder Passwörter für alles zugreifen können, womit das Gerät verbunden ist, wie z.B. Netflix-Konten, Amazon-Konten oder alles andere, was dem System hinzugefügt wurde.

SO FUNKTIONIERT ES TYPISCHERWEISE

In dem Moment, in dem ein Benutzer einen „voll geladenen“ Mediaplayer einschaltet und eine illegale App - wie Mobdro, FreeNetflix, Exodus oder Krypton - verwendet, befindet sich die Anwendung nun hinter der Firewall im vertrauenswürdigen Netzwerk und umgeht die Netzwerksicherheit effektiv.

Nach dem Start wird die App sofort und automatisch aktualisiert. Diese Updates sind erzwungen - der Benutzer hat keine Möglichkeit die Änderungen zu blockieren. Alles scheint wie geplant zu funktionieren, aber der Bedrohungsakteur bekommt auch das, was er will - den Zugriff auf das Gerät und die potenziellen Geräte und Netzwerke darüber hinaus. Während der Benutzer denkt alles sei sicher, wird das Gerät des Benutzers tatsächlich mit gefährlichen Waffen ausgestattet. Cybersicherheitspraktiker bezeichnen dies als "erweiterte Funktionalität".

Zum Beispiel, kurz nachdem ein Dark Wolfe-Forscher Mobdro herunter-geladen hatte, leitete er den Wi-Fi-Netzwerknamen und das Passwort des Forschers an einen Server wei-

ter, der in Indonesien zu sein schien. Forscher weisen darauf hin, dass das Endziel trüb ist, weil die Bedrohungsakteure ein virtuelles privates Netzwerk nutzen, das ihren tatsächlichen Standort verschleiert. Sobald die App gestartet wurde, berichtete der Forscher, dass die App ein Update erzwungen hat. Dann begann Mobdro, den Zugang zu Medieninhalten und anderen legitimen Apps im Netzwerk des Forschers zu suchen.

Ein Befund von Dark Wolfe ist besonders beunruhigend Nach dem ersten Update akzeptierte das Gerät Befehle von einem Hacker. Diese Befehle können von der App selbst oder von den Filmstreams kommen. Mit jeder Auswahl von Inhalten öffnet der Benutzer die Tür zu einem neuen Befehlssatz und bösartigen Nutzlasten von einem Hacker zu einem verwendeten Gerät. Dies kann alles umfassen, von Befehlen zum Ausführen eines Updates, um mehr Malware herunterzuladen, an einem DDoS-Angriff teilzunehmen oder auf dem Gerät ge-speicherte Elemente - wie Bilder, Filme, Dokumente - oder ähnliche Inhalte, die auf Geräten verfügbar sind, die mit einem Netzwerk verbunden sind.

Mit diesen Tools hat der Hacker nicht nur vollen Zugriff auf die ungesicherten Daten, sondern kann sich buchstäblich so in das Gerät eines Benutzers einloggen, als ob er oder sie davorsitzen würde. Der Hacker kann von diesem Gerät aus im Internet navigieren und sich als Benutzer ausgeben.

Nach der Installation sucht die App nach Updates. Dann agiert die Malware aus den Apps. Forscher beobachteten, dass die App, die die WLAN Daten des Benutzers an einen externen Server in Indonesien schickte, dann anfing, das Netzwerk zu untersuchen um mit allen File-Sharing-Diensten im Local Area Network zu kommunizieren. Es wurde auch "port knocked", - ein Prozess zur Suche nach anderer aktiver Malware - entdeckt.

Die App nahm auch die Streamdaten auf. Streams können Befehle enthalten, die es Hackern ermöglichen, die Anwendung aus der Ferne zu steuern. Wenn die App auf einem Jailbreak-Gerät läuft, könnte die App heimlich Audio und Video von einem Smart TV beziehen. Die Befehle könnten der App auch sagen, dass sie von einer anderen Quelle aktualisieren soll, wodurch mehr Malware-Funktionalität zur Verfügung steht. Dies ist eine einfache Möglichkeit für Hacker, in Netzwerke einzudringen und die Sicherheit zu umgehen.

Die Forscher von „Digital Citizens“ beobachteten Fälle, in denen nicht lizenzierte Filme und Fernsehsendungen als Köder benutzt wurden, wodurch die Benutzer dazu gebracht wurden, Anwendungen herunterzuladen, die ihre Geräte infizieren. Die Forschung ergab, dass der Inhalt nicht nur ein Köder ist, sondern auch zur Steuerung und Manipulation von Geräten verwendet wird, die mit dem Netzwerk eines Benutzers verbunden sind.

AUF DER SUCHE NACH EINEM PIRATEN-DREHBUCH

Was die Forscher entdeckten, spiegelt einen gemeinsamen Modus Operandi wider, der von Hackern verwendet wird.
In früheren Berichten über adsupported Piraten-Websites berichteten DCA und das Cybersicherheitsforschungsunternehmen RiskIQ über Partnerschaften, bei denen Piratenbetreiber mit Bedrohungsakteuren über den Preis von Malware-Installationen im Dark Web verhandeln.

Was Hacker im Dark Web diskutieren, ist oft ein Frühindikator für die Bedrohungen, denen Verbraucher in Zukunft ausgesetzt sein werden. Um zu verstehen, was als nächstes kommen könnte, stöberten Analysten des Cybersicherheitsunternehmens GroupSense im Dark Web herum, um zu begreifen, welche Bedrohungen in Zukunft anstehen.

Ein Teil der Diskussion im Dark Web konzentrierte sich auf die Nutzung der Malware zur Nutzung der Rechenleistung des Geräts (z.B. zum Angriff auf andere Computer) oder auf den Zugriff auf Informationen, die auf dem Gerät selbst gespeichert sein können (einschließlich Fotos, Passwörter und Kreditkarten). Die Ermittler entdeckten, dass Bedrohungsakteure eine Möglichkeit sehen, Piraterie Anwendungen zu modifizieren, um die Benutzernamen und Passwörter offenzulegen, die Benutzer für den Zugriff auf ihre Geräte und den Inhalt auf diesen Geräten gewählt haben.

Dies ist beunruhigend, da viele Internetnutzer auf einen einzigen Benutzernamen und ein einziges Passwort für mehrere Geräte, Plattformen und Websites angewiesen sind. Angenommen, "sallyjennings" verwendet das gleiche

"ilovedogs123!" Passwort für ihr Pirateriegerät sowie für ihren Computer und ihr Heim-Wi-Fi-Netzwerk.

Im Dark Web fand GroupSense konkrete Beispiele für potenzielle Hacker, die nach Malware-Tools für Kodi suchen.

Diese Exploits beinhalteten:

- Ein Exploit-Tool namens "17.0 Local File Inclusion", das es Hackern ermöglicht, auf die Inhalte eines Benutzers über eine Kodi-Box zuzugreifen, die auch persönliche Fotos und Videos sowie andere Medien-dateien enthalten kann.
- Ein Exploit-Tool namens "Kodi 15 Arbitrary File Access", das es Hackern ermöglicht, eine Sicherheitsschwachstelle auszunutzen, um auf sensible Informationen auf dem Gerät eines Benutzers zuzugreifen.
- Ein Distributed Denial of Service (DDoS)-Virus namens "Kodi Web Server 16.1", der es einem Hacker ermöglicht, einen Angriff auf Kodi-Boxen über das Netzwerk und die Bandbreite eines Benutzers durchzuführen.

Bei der Untersuchung der Risiken der mit diesen Geräten verbundenen Malware fand GroupSense die folgenden Bedrohungen für Verbraucher im Zusammenhang mit Bedrohungsakteuren, die auf Pirateriean-wendungen abzielen:

- Angriffe, die es einem Hacker ermöglichen, den Datenverkehr abzufangen und zu überwachen. Als "Man-in-the-Middle-Angriff" bezeichnet, glaubt ein Benutzer, dass er sich beispielsweise mit einem legitimen Dienst verbindet, um per Kreditkarte zu bezahlen, aber tatsächlich beobachtet ein Hacker die Verbin-dung. Auf diese Weise können Passwörter, Kreditkarten und andere Informationen gestohlen werden.
- Kodi Addons setzen Benutzern auch Malware aus, die Bedrohungs-akteuren Zugriff auf alle Arten von Inhalten gibt, entweder auf Kodi oder über Kodi. Da Kodi von vielen Verbrauchern als "Medienorganizer" verwendet wird, können sie oft über ihre Kodipowered-Geräte auf persönliche Bilder und Videos zu-greifen. Und da diese Geräte immer ausgereifter sind, werden sie wahr-scheinlich als Portal für den Zugriff auf andere persönliche Inhalte genutzt.

Die in den Rogue-Apps entdeckte Malware suchte die Erlaubnis, Zugang zu anderen Android-Apps zu gewähren, die der Forscher - der Reverse Engineering für Android-Apps erstellt und unterrichtet - noch nie zuvor gesehen hatte. Die Forscher fanden auch Rogue-Apps, die von Videos stammen, die entweder von Torrents oder von Websites außerhalb der Vereinigten Staaten heruntergeladen wurden und die hochinvasive Malware lieferten, die "Port Knocked" und nach anderer Malware suchten.

Das heißt, sie suchten nach anderen Filmquellen und Dateien im Netzwerk der Forscher und "sprachen" mit den Fernsehern im Netzwerk.

FAZIT

Das Ecosystem der Streaming-Piraterie basiert auf Geld verdienen durch Diebstahl. Der Benutzer wird nicht über die Risiken informiert. Benutzer dieser Software werden dazu verleitet, etwas auszuprobieren, von dem sie denken, dass es kostenlos oder billig ist, das aber mit extrem hohen Kosten verbunden ist: Malware die auf Datenklau aus ist.

Darüber hinaus sind die zahlreichen Online-Chats darüber, wie man Kodi-Addons infiziert, und die Diskussionen über Geschäftsmodelle wie man profitiert, rote Flaggen, die signalisieren, dass das Problem wächst. Auch in Deutschland!

Mediaplayer an sich sind eine feine Sache. Auch wenn es noch so reizvoll ist, der Benutzer sollte sich hüten Apps wie MOBDRO oder FreeNetflix herunterzuladen. Allein schon der Download öffnet den Hackern ein paar Türen. Mehr Türen öffnen sich ihnen, wenn die Apps aktiviert werden.

Und wenn Sie Glück haben wurde Ihre Kreditkarte noch nicht leergefegt, doch Sie bekommen dann die Mail unten:

(*1) Über die Digital Citizens Alliance

Die Digital Citizens Alliance ist eine gemeinnützige Organisation, die eine verbraucherorientierte Koalition ist, die sich darauf konzentriert, die Öffentlichkeit und die politischen Entscheidungsträger über die Gefahren aufzuklären, denen die Verbraucher im Internet ausgesetzt sind. Digital Citizens möchte einen Dialog über die Bedeutung führen, die das Internet für die Interessengruppen - Einzelpersonen, Behörden und Industrie - hat, um das Internet sicherer zu machen.

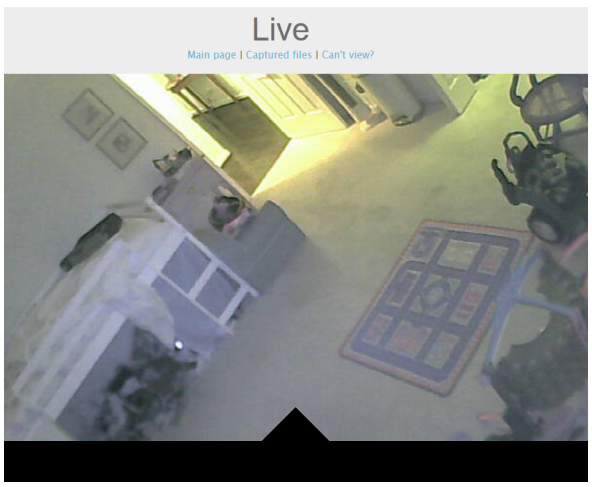
(*2)Über Dark Wolfe Consulting

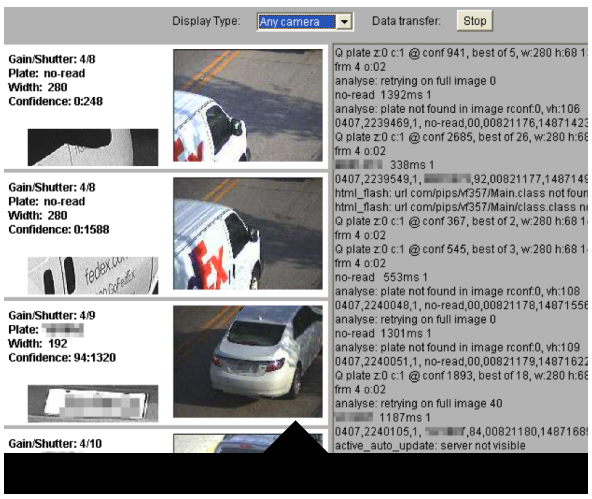
Dark Wolfe Consulting ist ein Cybersicherheitsunternehmen, das spezialisierte und kommerzialisierte Netzwerksicherheitsbewertungen, Schwachstellenbewertungen, Netzwerkdurchdringungstests, Anwendungsbewertungen und Anwendungsdurchdringungstests anbietet

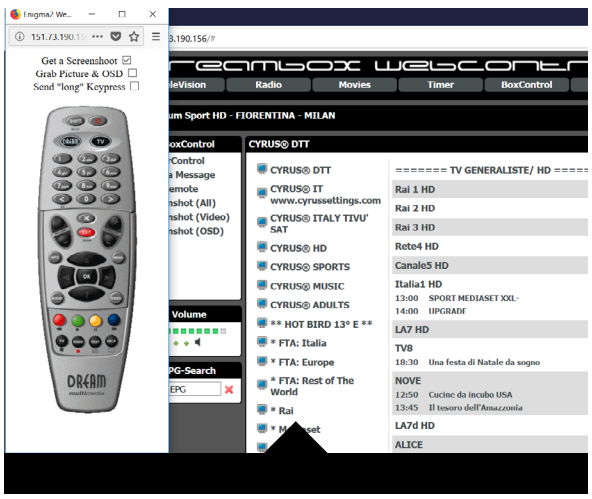
UNSICHERES INTERNET DER DINGE

Schuldhaftes Verhalten der Verbraucher?

Jedes ins Netzwerk eingebundene Gerät wird mit der Möglichkeit Passwörter zu setzen ausgeliefert.





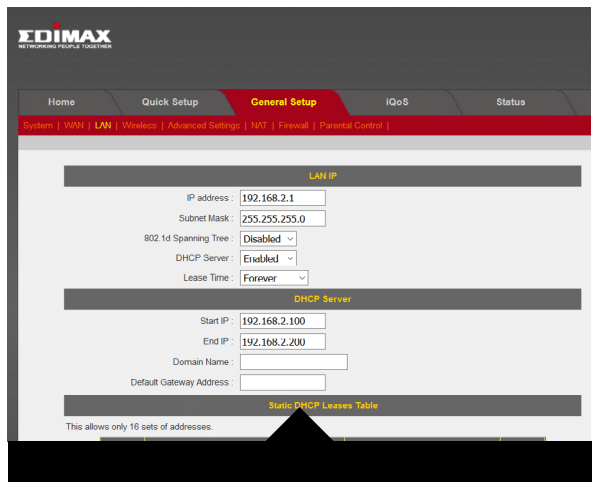


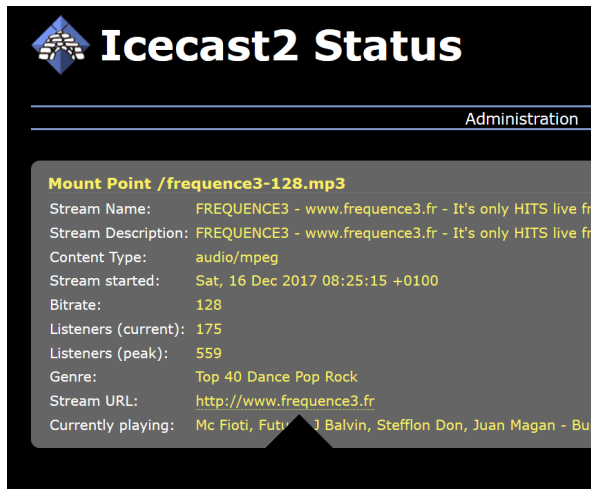
Es ist leicht die Schuld bei Löchern in Netzwerken grundsätzlich bei den Anbietern zu suchen. Sicher, wenn mehr als 1000 Android Apps den Nutzer ausspionieren, dann ist der Besitzer eines Smartphones mit einer oder vielen dieser Apps das Opfer.

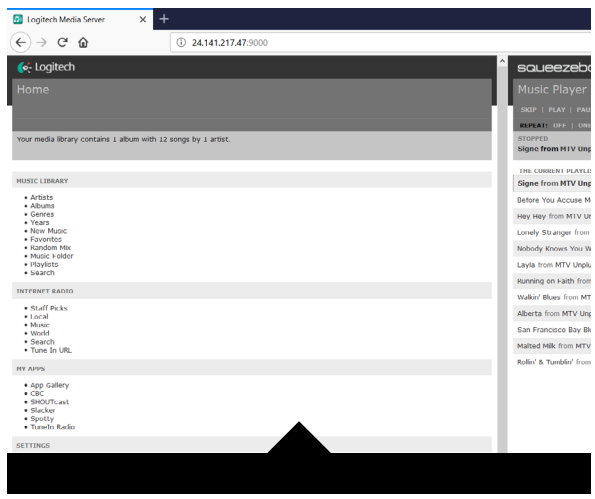
Allerdings wird bei der Installation zumeist darauf hingewiesen, dass diese App den Zugriff auf das Mikrophon und die Kamera hat. Spätestens dann schrillen die Alarmsirenen und man sollte auf die App verzichten.

Doch so etwas ist nur die Spitze des Eisbergs. Was die Suchmaschine Shodan monatlich aus 500 Millionen mit dem Netz verbundenen Geräten und Diensten zutage fördert, veranlasste CNN Shodan als „die erschreckendste Suchmaschine des Internets“ zu bezeichnen.

Als nicht zahlender – jedoch registrierte User – entdeckt man in wenigen Sunden hunderte unsichere Kandidaten. Ziemlich an der Spitze stehen IP-Kameras und Smart Home







Installationen. Die Kameras gewähren Einblick in die Privatsphäre von Familien oder zeigen Sicherheitsbereiche von Unternehmen und Organisationen.

In den USA gibt es die Registrierung von Fahrzeugkennzeichen via Kameras. Einen Schutz gegen Eindringlinge in das System gibt es jedoch oft nicht.

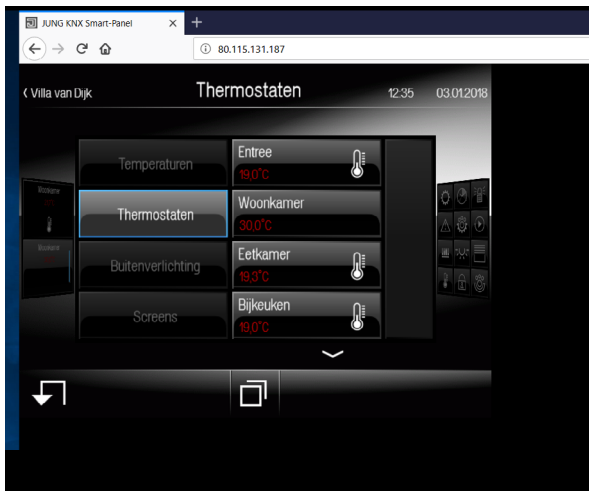
Router im privaten sowie im geschäftlichen Bereich sollten eigentlich geschützt sein, doch sie sind es nur teilweise. Der Hacker hat Zugriff auf das gesamte Heim- oder Firmennetzwerk.

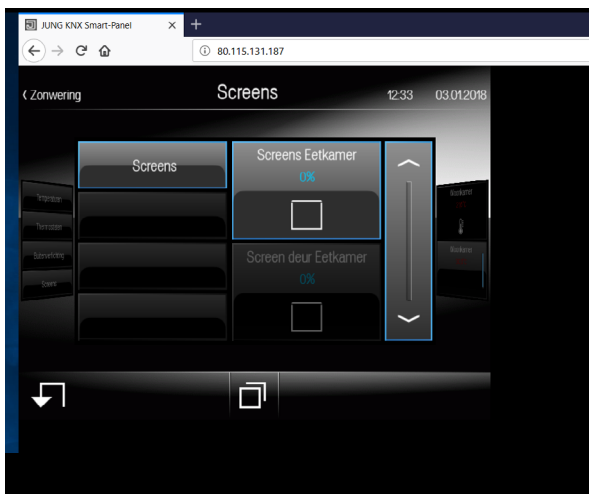
Ein französischer Radiosender erlaubt dem Besucher den Zugriff auf die Playlists. So kann der Hacker das Programm steuern und zum Beispiel eigene Playlists erstellen, die dann auch gesendet werden.

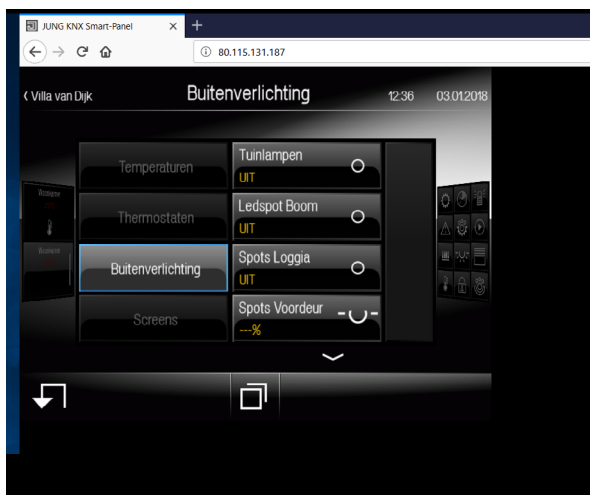
Hier aus Sicherheitsgründen nicht gezeigt, ist eine Wasseraufbereitungsanlage, bei der gefährliche Eingriffe jederzeit möglich sind.

Neben Schwimmbädern, die im Winter als Eislauffläche diesen und deren Temperatur der Eindringling beliebig rauf und runter regeln kann, gibt es Geldtransporter mit Summenangaben zu einzelnen Transporten und deren Wege oder Firmenserver mit sensitiven Daten. Ziemlich makaber war die externe Steuerung eines Krematoriums.

Im privaten Bereich sieht es noch schlimmer aus. Neben den IP-Kameras gibt es Smart-Home Anlagen, auf die







jeder Zugriff hat. So lassen sich die Rollläden steuern, die Temperaturen in verschieden Räumen verändern, die Alarmanlage ausschalten oder das Licht im Haus steuern. Hier sind vor allen Dingen die Smart Panels der Firma Jung betroffen.

Etwas mehr Wert auf Sicherheit legen die Besitzer von Linux Set top Boxen. Aber auch hier gibt es nachlässige Kandidaten. Die Steuerung einer Dreambox oder eines VU+ von außen ist ein Kinderspiel. Programme können gewechselt werden, die Lautstärke lässt sich verändern, Festplatten lasen sich leerfegen oder Box beikommt einen Werks-Reset.

Heute befinden sich in vielen Haushalten Media-Server. Auch hier erfolgt der externe Zugriff ohne Nutzername oder Passwort. So lassen sich Inhalte wie Musik oder Videos manipulieren. Besonders die Server von Logitech fielen hier auf.

Wer trägt nun die Schuld an dieser Misere?

Es sind eindeutig die Nutzer! Jedes ins Netzwerk eingebundene Gerät wird mit der Möglichkeit Passwörter zu setzen ausgeliefert. Im Urzustand kommen sie in der Regel mit admin/1234, admin/admin oder admin/0000 für Nutzer/Passwort. Oder aber die Einträge sind leer.

Die erste Aufgabe des Käufers sollte die Festlegung eines sicheren Passwortes sein, doch leider werden die Geräte oft sofort in Betrieb genommen und das wichtige Passwort zu setzen einfach vergessen.

DECKT ARABSAT PIRATEN?

Der Fall beoutQ

EIN WENIG HINTERGRUNDWISSEN

Die Gründung der Arab Satellite Communications Organization (Arabsat) geht auf die späten 1960er Jahre zurück. Im Jahr 1967 entwickelten die Informationsminister der arabischen Staaten eine Reihe von Prinzipien in Bezug auf ein Satellitennetzwerk, um eine Integration von sozialen und kulturellen Aktivitäten zwischen den Ländern der Arabischen Liga zu schaffen. Andererseits wurde 1969 die Arab States Broadcasting Union (ASBU) gegründet.

Saudi-Arabien trat dieser von Ägypten geführten und in Kairo ansässigen Vereinigung erst 1974 bei, höchstwahrscheinlich aufgrund der damals angespannten Beziehungen zwischen Saudi-Arabien und Ägypten.

Am 14. April 1976 wurde Arabsat unter der Gerichtsbarkeit der Arabischen Liga mit dem Ziel gegründet, den Informations-, Kultur- und Bildungsbedürfnissen seiner Mitgliedsstaaten zu dienen. Saudi-Arabien war von Anfang an der größte Anteileigener der neuen Organisation aufgrund seiner erweiterten finanziellen Ressourcen und aufgrund seiner florierenden Öl exportierenden Industrie. Riyadh beherbergt das Hauptquartier von Arabsat.

Mit 21 Mitgliedsländern spielt die Organisation eine wichtige Rolle bei der Verbesserung der Kommunikation in der arabischen Welt. Saudi-Arabien hält 36,7% an ARABSAT. Der kleine Nachbar Katar gerade mal 9,8%. Und dieser Unterschied macht sich seit dem 5. Juni 2017 zum Nachteil von Qatar bemerkbar.

DIE DIPLOMATISCHE KRISE IN KATAR

Am 5. Juni 2017 hatte Saudi-Arabien offiziell die Beziehungen zu Katar abgebrochen. Saudi-Arabien sagte, es habe die Entscheidung getroffen, die diplomatischen Beziehungen aufgrund der "Umarmung verschiedener terroristischer und sektiererischer Gruppen, die darauf abzielten, die Region zu destabilisieren", einschließlich der Muslimbruderschaft, der Al-Qaida, des islamischen Staates Irak und der Levante, und der vom Iran unterstützten Gruppen in der östlichen Provinzstadt Qatif Islam Hassan, zu beenden.

Seit dem Jahr 2000 und darüber hinaus verfolgt Katar eine unabhängige Außenpolitik, die zeitweise mit den strategischen Interessen Saudi-Arabiens in der Region kollidierte. Die Tatsache, dass Katar nicht die saudische Außenpolitik verfolgt und mit Staaten und nichtstaatlichen Akteuren umgeht, denen die Saudis nicht zustimmen, haben diese Spannungen in den letzten Jahren, vor allem nach den arabischen Aufständen, zugenommen.

Diese Spannungen wurden durch eine Hacking-Story der Qatar News Agency und die Aussage, die Scheich Tamim bin Hamad zugeschrieben wurde, wiederbelebt, die Katar angeblich später verfälschte. Dies geschah zu einer Zeit, in der sich Mohamed bin Salman als Konkurrent von Mohamed bin Nayef im Kampf um den saudischen Thron stark machte. Mohamed bin Salman versuchte den Segen der USA während des Besuchs von Trump in Saudi-Arabien zu erhalten, um Katar in die Knie zu zwingen und mit einem Sieg nach Hause zu gehen, der ihm mehr Popularität in Saudi-Arabien verschaffen würde und sollte seinen Weg an die Macht erleichtern.

Am 02. August 2018 berichtete der Daily Express, dass “ein Invasionsplan von Saudi-Arabien angeführt und von den Vereinigten Arabischen Emiraten unterstützt in der Schublade lag, bevor die USA eingriffen und die Staaten zum Rückzug aufforderten”.

Der Geheimdienst von Katar meldete die befürchtete Invasion an die USA und der damalige Verteidigungsminister James Mattis forderte Saudi-Arabien und die Vereinigten Arabischen Emirate auf, die in Katar stationierten US-Truppen im Central Command Center nicht zu bedrohen. Übrigens, die Saudis vergaßen bei dem Vorwurf Katar würde terro-ristische Gruppen unterstützen, das ein Großteil der 9/11 Attentäter aus Saudi-Arabien kam.

Der in Katar beheimatete Nachrichtensender „Al Jazeera“ war den Saudis von Anfang an ein Dorn im Auge. Zu kritisch war die Berichterstattung für das autokratisch geführte Regime. Als Mitglied der ARABSAT-Organisation hatte Al Jazeera das Recht über die Badr-Satelliten ihr Programm abzustrahlen.

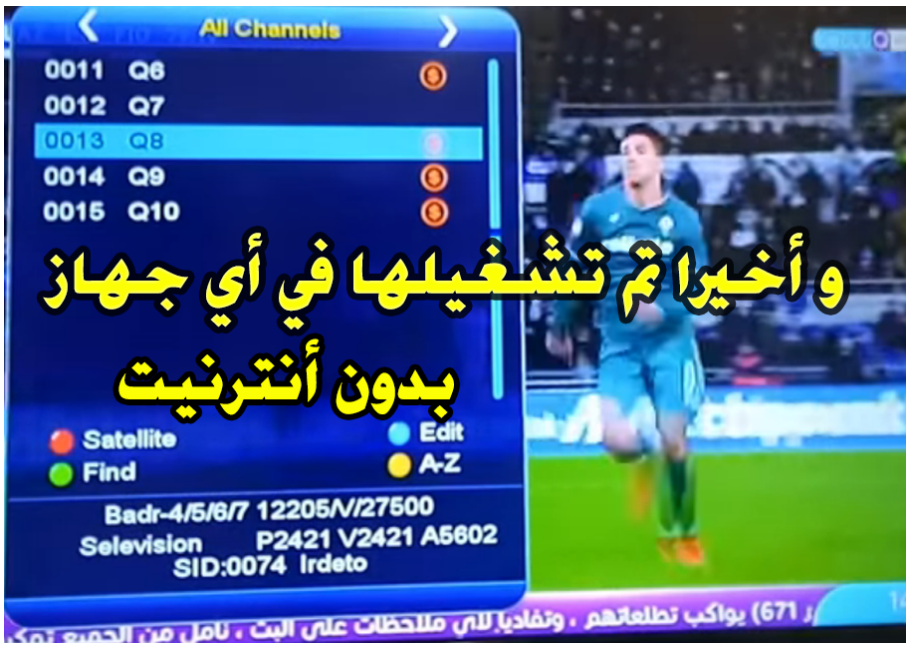
WIE AUS beinQ PLÖTZLICH beoutQ WURDE

beIN Sports ist ein Sportkanal, der im November 2003 ursprünglich als Al Jazeera Sport gegründet wurde. Heute verfügt der Sender über 19 HD-Kanäle und gehört der beIN Media Group - ein Tochterunternehmen von Al Jazeera - an, die ihren Sitz in Doha hat. Seit 2014 wird das PayTV-Paket beINQ über die Badr-Satelliten abgestrahlt und hat einige Millionen Abonnenten.
Die meisten in Saudi Arabien und in den Vereinigten Arabischen Emiraten. beINQ besitzt u.a. die Rechte an der Bundesliga, der Fussball EM und WM und der Formel 1 in der Region.

Nach dem 5. Juni 2017 (dem Tag an dem Saudi Arabien die Beziehungen zu Katar abbrach) tauchten auf den Badr-Satelliten plötzlich 10 Sender unter der Bezeichnung beoutQ auf. Gleichzeit warb beoutQ in der Regio aggressiv für die spezziellen Set Top Boxen (Dream Boxen?) für den Empfang von beoutQ via Satellit und IPTV. Für rund 95 Euro. Die Nachfrage nach den Boxen und Abonnements war immens. Und wer nun Zugang hatte, der empfing mit einer Zeitverzögerung von ca. 10 Minuten die originalen Inhalte vom Rechtehalter beinQ. Das beinQ-Logo verschwand hinter einem Overlay des beoutQ-Logos. In der selben Zeit wurden die Übertragungen von beinQ durch ARABSAT geblockt.

Der Weltfussball-Verband FIFA und der Rechteinhaber beIN Media legten sofort Beschwerde bei der ARABSAT Organisation in Ryad, Saudi-Arabien ein, doch deren Antwort war mehr als verwunderlich:

“Arabsat war sich von Anfang an sicher, dass das Satellitennetz von beoutQ nicht genutzt wurde”, sagte der C.E.O. Khalid Balkheyour in der Arabsat-Erklärung. “Dennoch haben wir eine sehr kostspielige Untersuchung durchgeführt, um alle Zweifel auszuräumen und Beweise zu liefern, die wir mit der FIFA und der Welt teilen können.



Arabsat wurde durch die Angriffe von beIN und der FIFA zutiefst beleidigt und geschädigt", erklärte er. "Nun, da sich die FIFA-Vorwürfe als falsch erwiesen haben, sollte sie sich für solche beleidigenden Äußerungen entschuldigen." ARABSAT sagte, dass man Experten gebeten hat, die Signal von beouQ zu untersuchen und die seien zu der Konklusion gekommen, dass niemals über die ARABSAT-Satelliten gesendete wurde. Es müsse sich hier um einen daneben angesiedelten Satelliten handeln. Sieht man sich die Positionen an, dann wären ASTRA 2E und 2G die Schuldigen. Nur da haben sich die „Experten" nicht die ASTRA Footprints angesehen.

ASTRA 2E und 2G sind in den arabischen Ländern nicht empfangbar. Auch müssen diese „Experten" auf beiden Augen blind gewesen sein, denn die Senderlisten der Set Top Boxen in den arabischen Ländern listen eindeutig 10 beoutQ-Sender auf und es existieren hunderte von Mittschnitten.
Ein Mitarbeiter aus Bangladesch, der diese Woche bei Sharif Electronics in Jeddah telefonisch erreichbar war, sagte, dass sein Geschäft die Boxen seit fünfzehn Monaten verkauft. "Viele Leute kaufen sie", sagte er.

WER STECKT HINTER DEN beoutQ-PIRATEN?

Während des Champions-League-Halbfinales traf sich Tom Keaveny, beINs Geschäftsführer für den Mittleren Osten, der seit drei Jahrzehnten im Fernseh-Business arbeitet, mit einem halben Dutzend beIN-Ingenieuren in einem kleinen Raum namens "the lab" mit einem Mandat: schaltet beoutQ ab!Sie waren bisher nicht erfolgreich.

Keaveny sagte, dass die Operation von beoutQ "industrielles Wissen und Können und eine Finanzierung von mehreren Millionen Dollar erfordert". "Das ist nicht jemand in seinem Schlafzimmer", sagte er.

Die Website von BeoutQ behauptet, die Geldgeber seien ein kolumbianisches und kubanisches Konsortium. Mitarbeiter von beIN sagten, sie hätten mehr als 200.000 Dollar für die Untersuchung des Raubkopierens ausgegeben und das beoutQ-Signal zum in Riad ansässigen Satellitenanbieter Arabsat zurückverfolgt.

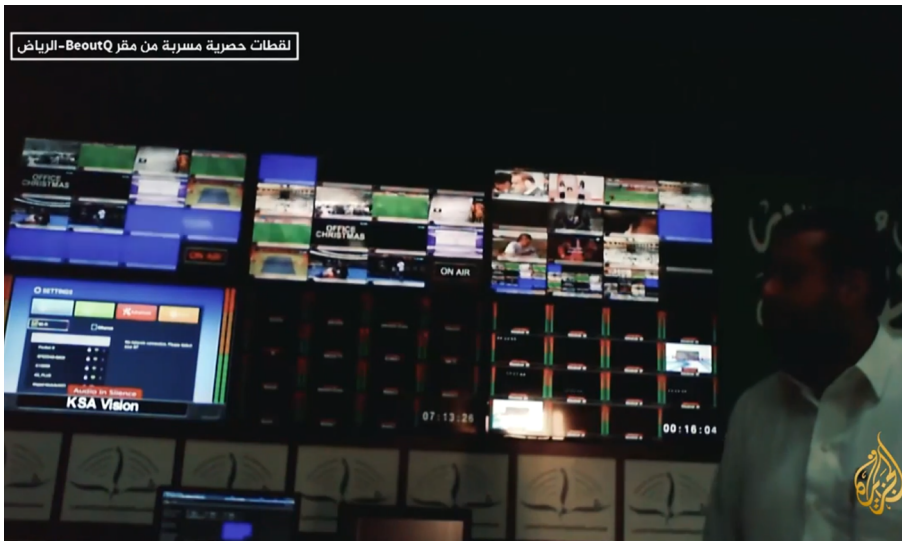
Das beoutQ-Management hat keine Namen. Da arbeitet Saudi-Arabien mit Nebelkanonen. So nahm sich die Tectime Redaktion die Homepage und den Hoster von beoutQ vor. Der sitzt in den USA und sagt nur so viel, dass ein gewisser Dr. Raeed Kusheim die Gebühren mit seiner privaten Kreditkarte bezahlte. Der Redaktion ist Kusheim nur zu gut bekannt. Er ist der C.E.O. der Firma Selevison in Riad und Hersteller von Set Top Boxen und bietet Video on Demand Dienste an. Schon früh war er auf ARABSAT mit eigenen Sendern vertreten. Seine zahlreichen Unternehmen in Saudi-Arabien gelten als ungemein gewinnträchtig! Und seine Beziehungen zum Königshaus kann man getrost als eng bezeichnen. Mal ganz theoretisch und vorsichtig gefragt: haben wir den Finanzier von beoutQ gefunden?

beoutQ
Piraten-Standort ermittelt

beoutQ die Zweite

In der Ausgabe 5 des TecTime-Magazins wurde erstmals über die Machenschaften der saudischen Piratensendergruppe beoutQ berichtet und wir konnten einen Beteiligten – den C.E.O. Dr Raed Khusheim der Firma Selevision – ermitteln. Doch er ist nicht der einzige Beteiligte. Hinter beoutQ steckt die ARABSAT-Organisation und das saudische Könighaus.

Hier ein Blick zurück:



Wie aus beIN Sports plötzlich beoutQ wurde

beIN Sports ist ein Sportkanal, der im November 2003 ursprünglich als Al Jazeera Sport gegründet wurde. Heute verfügt der Sender über 19 HD-Kanäle und gehört der beIN Media Group - ein Tochterunternehmen von Al Jazeera - an, die ihren Sitz in Doha hat. Seit 2014 wird das PayTV-Paket beIN Sports über die Badr Satelliten abgestrahlt und hat einige Millionen Abonnenten. Die meisten in Saudi-Arabien und in den Vereinigten Arabischen Emiraten. beIN Sports besitzt u.a. die Rechte an der Bundesliga, der Fußball EM und WM und der Formel 1 in der Region.

Nach dem 5. Juni 2017 (dem Tag an dem Saudi Arabien die Beziehungen zu Katar abbrach) tauchten auf den Badr-Satelliten plötzlich 10 Sender unter der Bezeichnung beoutQ auf. Gleichzeit warb beoutQ in der Region aggressiv für die speziellen Set Top Boxen für den Empfang von beoutQ via Satellit und IPTV. Für rund 95 Euro. Die Nachfrage nach den Boxen

und Abonnements war immens. Und wer nun Zugang hatte, der empfing mit einer Zeitverzögerung von ca. 10 Minuten die originalen Inhalte vom Rechtehalter beIN Sports. Das beIN-Logo verschwand hinter einem Overlay des beoutQ-Logos. In derselben Zeit wurden die Übertragungen von bein Sports durch ARABSAT geblockt.

Der Weltfußball-Verband FIFA und der Rechteinhaber beIN Media legten sofort Beschwerde bei der ARABSAT Organisation in Ryad, Saudi-Arabien ein, doch deren Antwort war mehr als verwunderlich:

“Arabsat war sich von Anfang an sicher, dass das Satellitennetz von beoutQ nicht genutzt wurde”, sagte der C.E.O. Khalid Balkheyour in der Arabsat-Erklärung. “Dennoch haben wir eine sehr kostspielige Untersuchung durchgeführt, um alle Zweifel auszuräumen und Beweise zu liefern, die wir mit der FIFA und der Welt teilen können. Arabsat wurde durch die Angriffe von beIN und der FIFA zutiefst beleidigt und geschädigt”, erklärte er. “Nun, da sich die FIFA-Vorwürfe als falsch erwiesen haben, sollte sie sich für solche beleidigenden Äußerungen entschuldigen.”

Seitdem haben zwar immer wieder internationale Sportorganisationen und Rechteinhaber gegen beoutQ geklagt und auch gewonnen, doch eine zustellbare Adresse des Senders gab es nicht. Saudi-Arabien verweigerte jegliche Unterstützung und lies Gerüchte verstreuen, die Sendergruppe habe ihren Sitz in Nordafrika.

Al Jazeera liefert Beweise

Dann kam der 22. September 2019. Am Abend dieses Tages strahlte das investigative Programm „What lies below“ von Al Jazeera eine Dokumentation zum Thema beoutQ aus

, die zeigte, wie zwei saudische Dienstleister, Selevision und Shammas, an den von beoutQ durchgeführten Operationen beteiligt waren. Selevision ist im Besitz der Khusheim Holding und der C.E.O. ist Dr.Raed Khusheim. In den USA registrierte er die Domain „beouQ“ und bezahlte mit seiner persönlichen Kreditkarte, wie das Tectime Magazin ermittelte. Dr. Khusheim (Vorgespräch mit dem Autor zu einem Interview in Dubai 2007) steht nach eigenen Angaben dem saudischen Königshaus sehr nahe.

In der Dokumentation bewies „What lies below“ erstmalig, dass beoutQ seinen Sitz am Hauptsitz von Selevision im al-Qirawan-Distrikt der saudischen Hauptstadt Riad hat. Das Video zeigt die Uplink-Anlage und Büros und als Beweis das Foto eines Selevision-Dienstwagens vor der Anlage. Das Filmmaterial enthielt auch Bilder des Hauptkontrollraums und der Server, die die gestohlenen Inhalte von bein Sports übernehmen, das Logo ersetzen und als beoutQ abstrahlen. Das Programm Al Jazeera konnte Dokumente vorweisen, die belegen, dass finanzielle Transaktionen zwischen dem saudischen Unternehmen und dem Management von Arabsat stattgefunden haben.

Die Dokumente enthüllten auch, dass ein alternativer Standort für die Piraterieoperationen in einem unbenannten nordafrikanischen Land diskutiert wurde, nachdem Saudi-Arabien unter zunehmendem Druck stand, die Ausstrahlung des raubkopierten beIN-Signals einzustellen.

Saudi-Arabien hat zuvor Behauptungen zurückgewiesen, dass beoutQ seinen Sitz im Königreich hat.

Die Staatsanwaltschaft Katars hat drei Mitarbeiter der beIN Media Group beschuldigt, mit Saudi-Arabien und Ägypten zu kommunizieren, um den Interessen des Sportnetzwerks zu schaden.

In einem Interview mit Al Jazeera sagte die katarische Staatsanwaltschaft, dass einer der drei Angeklagten nach der Durchsetzung der Blockade nach Saudi-Arabien gereist sei.

Der Angeklagte, der ohne Visastempel in seinem Reisepass in das Königreich einreiste, traf den saudischen Geheimdienstmitarbeiter Maher Mutreb und gab geheime und sensible Informationen an den ägyptischen Geheimdienst weiter.

Mutreb ist ein saudischer Geheimdienstler, der für einen

Dr. Raed Khusheim

Senior Adviser des saudischen Kronprinzen Mohammed bin Salman (MBS) arbeitete. Laut einem Bericht des Sonderberichterstatters der Vereinten Nationen über außergerichtliche Hinrichtungen war Mutreb eng an der Ermordung des saudischen Journalisten Jamal Khashoggi am 2. Oktober im Konsulat des Landes in Istanbul beteiligt.

Die investigative Arbeit von Al Jazeera ergab, dass die Piraterie-Operation nicht das Ergebnis gewöhnlicher Hacker war, wie Saudi-Arabien seit langem behauptet, sondern Teil eines integrierten Systems mit offizieller saudischer Abdeckung und finanzieller Unterstützung war.

NACHTRAG:

Auch in Europa bewegt sich was. Ein erstes Urteil gegen einen illegalen Vertrieb von beoutQ-Boxen und Inhalten wurde gefällt. Auch in Deutschlang gibt es beoutQ Angebote für eine Kundschaft in Berlin und in NRW. Passiert ist bisher nichts.

Ein Einzelhändler in London wurde in London wegen der Verletzung des Urheberrechts, Betrugs und dem Vertrieb von illegalen Streaming-Geräten verurteilt. Der Händler vertrieb beoutQ-Streaming-Boxen im großen Stil. Die Klage war das Ergebnis investigativer Zusammenarbeit zwischen der Premier League, der Federation Against Copyright Theft (FACT) und der Polizei.

TEST

VU+ ULTIMO 4K

IM WOHNZIMMER TUT DER ULTIMO 4K SEINEN DIENST ALS KOMFORTABLER UND HOCHWERTIGER FAMILIEN-RECEIVER

Seit Vu+ den Ultimo4K auf der Anga Cable 2016 vorstellte ist einige Zeit vergangen. Im Laufe der Jahre wurde einige Bugs getilgt und der Ultimo 4K erfreut sich allgemeiner Beliebtheit.

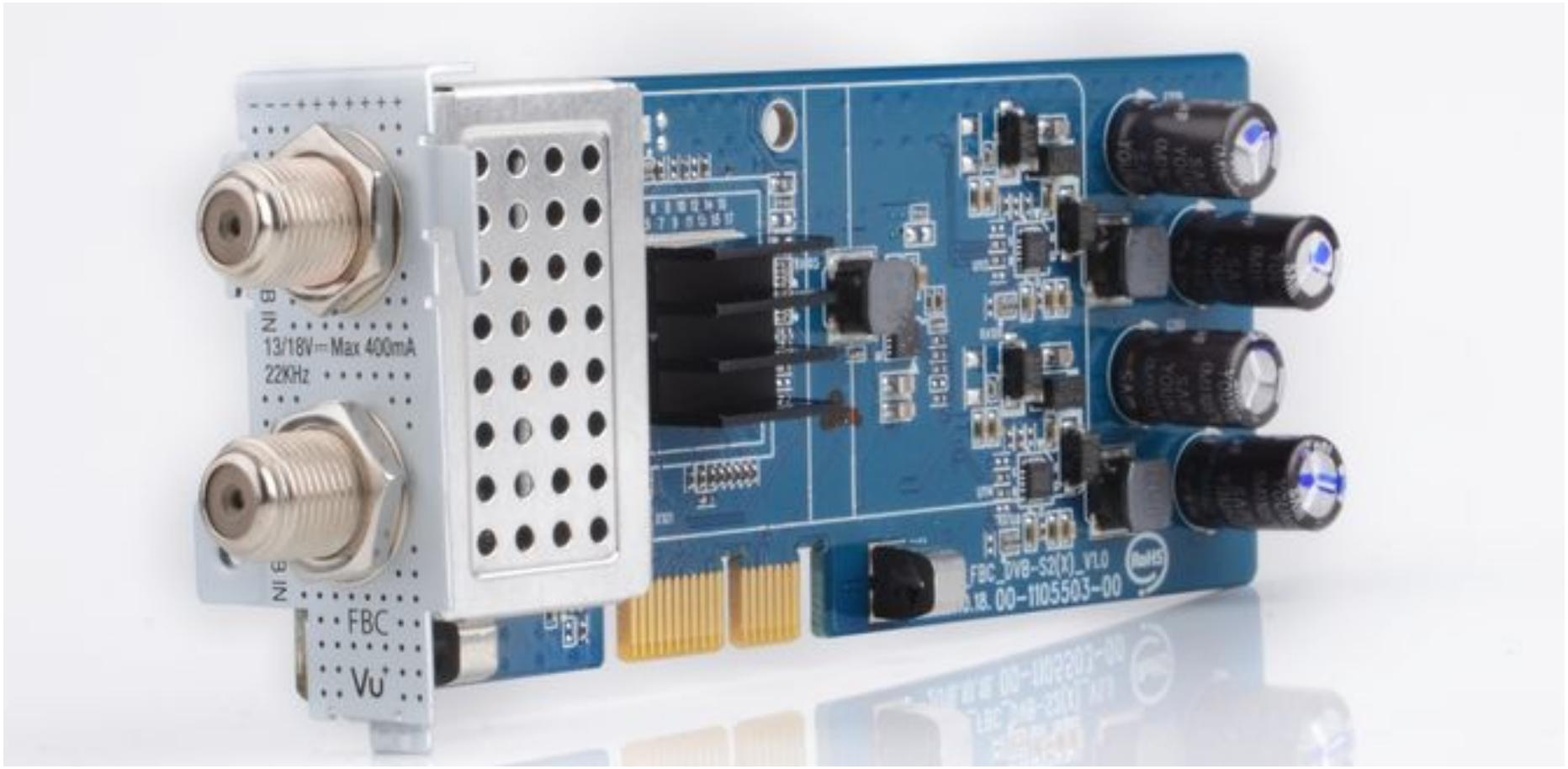
Sehen wir uns das aktuelle Modell etwas genauer an: Der Ultimo4K hat ein schönes großes 4,0" TFT-Display auf der Vorderseite, dies ist eine schöne Größe, da es viel Platz hat, um Kanalnamen, Programmnamen, Start-/Endzeiten, Fortschrittsbalken und auch die aktuelle Zeit anzuzeigen. Es kann auch konfiguriert werden, um ein Kanal-Picon anzuzeigen, und aufgrund seiner Größe ist dies wiederum

sinnvoll.

Alternativ können Sie das 4,0"-Display als MiniTv verwenden und es zeigt das aktuelle Programm auf dem Display an, dies ist nützlich, wenn Sie den Fernseher nicht einschalten möchten. Sie können den Fernsehkanal weiterhin mit einem Paar Bluetooth-Kopfhörer oder einer Soundbar hören.

DAS INNENLEBEN

Im Inneren des Ultimo4K befinden sich hinten rechts die steckbaren FBC-Tuner. Der Ultimo4K wird mit austauschbaren Tunern geliefert, FBC steht für Full Band Capture. Hier wäre z.B. eine gute Kombination 1x DVB-S2X FBC Twin / 1x DVB-C FBC / 1x DVB-S2 Dual Tuner PVR ready. Der DVB-S2 FBC Twin Tuner besitzt 8 Demodulatoren. Bei zwei herkömmlichen (z.B. Twin-LNB) Sat-Zuleitungen ist



der Tuner mit 2 herkömmlichen und 6 zusätzlichen Tunern, die im Durchschleifbetrieb arbeiten, vergleichbar. Man kann somit Sender aus 8 verschiedenen Transpondern aus 2 unterschiedlichen Sat-Ebenen gleichzeitig ansehen, streamen oder aufnehmen. Im SCR-Betrieb (Unicable) mit 8 Frequenzen entspricht dies 8 herkömmlichen Tunern. Der DVB-C FBC Tuner besitzt 8 Demodulatoren. Dies entspricht einem Receiver mit 8 herkömmlichen DVB-C Tunern.

Somit kann man 8 Sender zur gleichen Zeit ansehen, streamen oder aufnehmen.

Der große schwarze Kühlkörper, der in der Mitte sichtbar ist, deckt den Broadcom BCM 7444s 1,5 GHz Quad Core 20.000 DMIPS ARM v7 CPU ab. Vorne rechts gibt es die Kartenleser und CI-Slots. Die Halterung für die interne Festplatte befindet sich vorne links, und man kann entweder eine 2,5" oder 3,5" Festplatte im Ultimo4K montieren. Ein Netzteil sucht man im Inneren vergebens, denn die Stromversorgung erfolgt extern und das hält die Temperatur im Inneren niedrig.

Bluetooth 4.0

Der Ultimo4K verfügt über Bluetooth 4.0, dies kann verwendet werden, um eine Verbindung zu einer Soundbar oder zu einem Paar Bluetooth-Kopfhörer herzustellen, was nützlich ist, wenn man das Frontdisplay als MiniTv verwendet. Das Bluetooth wird jedoch nicht mit einem iPhone oder einem ähnlichen Gerät verbunden.

Wi-Fi

Der Ultimo4K hat ein Wireless Lan eingebaut und unterstützt sowohl 2,4 GHz als auch 5 GHz Bänder.

HDMI-Eingang

Eine schöne Funktion, die Vu+ hier hinzugefügt hat. Dies gibt dem Nutzer die Möglichkeit, ein anderes Media-Gerät an den Ultimo 4K anzuschließen, und es bedeutet, dass man nur die eine HDMI-Verbindung zum Fernseher benötigt. Dies funktioniert möglicherweise nicht mit allen Geräten, da der Kopierschutz HDCP 2.2 nicht gewährleistet ist.

HbbTV

Der Ultimo4K unterstützt auch HbbTV. Einfach einen Sender einstellen, der den Service bietet und dann den roten Knopf der Fernbedienung drücken. Der Ultimo 4K wird dann die Internetverbindung nutzen, um sich mit den On-Demand-Diensten des Senders zu verbinden.

IPTV

Der Ultimo 4K bietet die Möglichkeit IPTV entweder über Plugins oder direkt aus der Kanalliste (Bouquets) zu nutzen, wenn man IPTV aus den Bouquets wählt.

Blindscan

Ein weiteres tolles Feature des Ultimo 4K ist die Blindscan-Funktion, dies ist eher für Enthusiasten und fortgeschrittene Benutzer gedacht, die den Clark Belt nach allen Kanälen durchsuchen möchten, die sie finden können. Das Blindscan-Plugin fordert auf, den Satelliten auszuwählen, den man absuchen möchte und dann erledigt der Empfänger den Rest. Es ist eine großartige Funktion, besonders bei der Suche nach Feeds.

IN DER PRAXIS

Im Kurztest wurde der Ultimo 4K an eine drehbare Antenne angeschlossen. Die Internet-Anbindung lässt Ethernet als auch WLan zu. Wie bereits erwähnt, gibt es im Ultimo 4K Platz für eine interne Festplatte (2,5" oder 3,5"), aber man kann auch eine Netzwerk-HDD verwenden, wenn ein NAS-Setupvorhanden ist.

Der Ultimo 4K schafft den Kaltstart in etwa 33 Sekunden. Diese Zeit variiert je nachdem wie viele Plugins, Skins usw. installiert sind. Übrigens, der Neustart aus dem Standby-Modus dauert nur 13 Sekunden Der erste Suchlauf auf HOTBIRD war in ca. 8 Minuten erledigt. Alternativ dazu lassen sich auch Kanallisten von Anbietern im Internet oder vom Addons Server verwenden.

Ultra HD

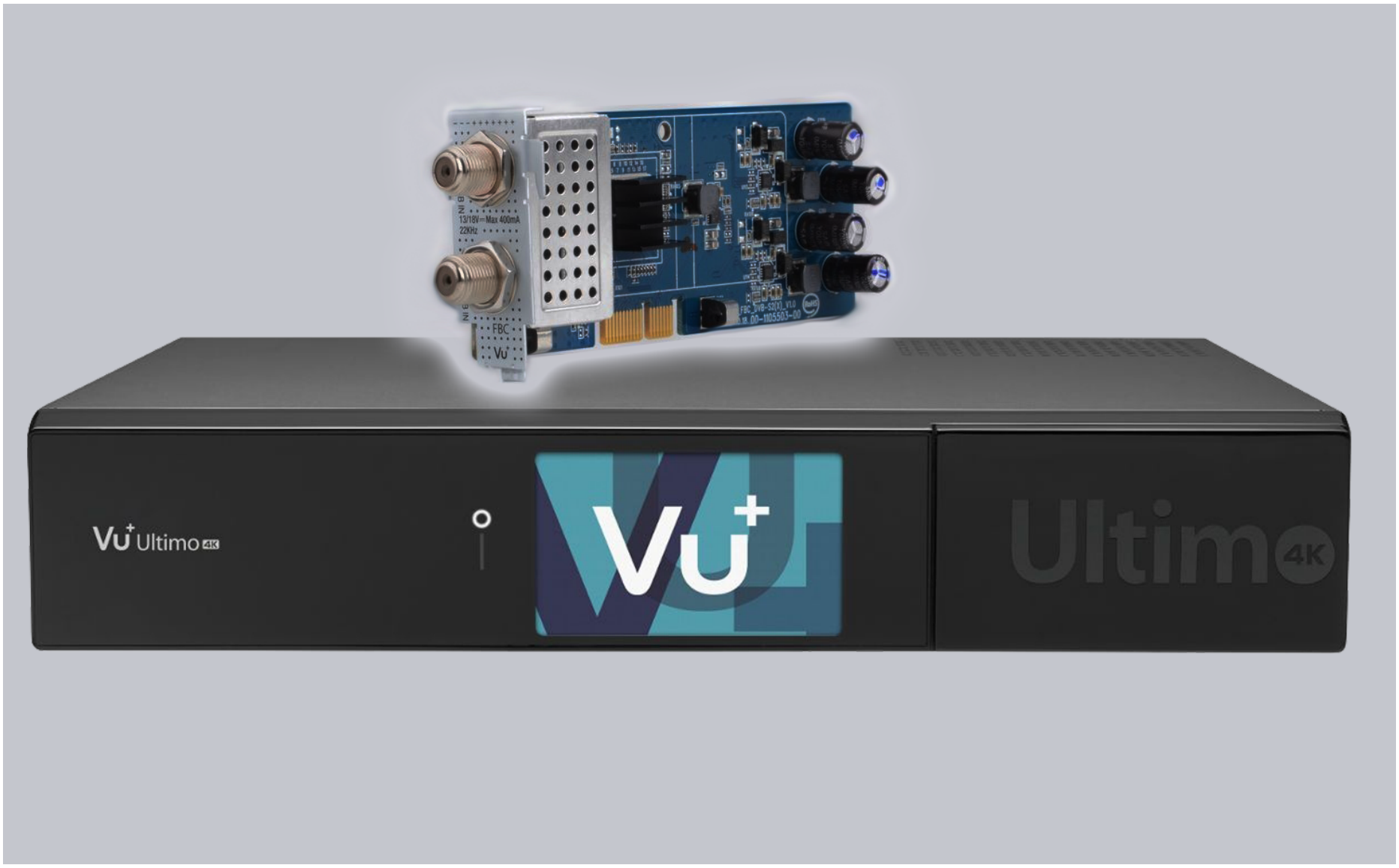
Der Ultimo 4K gibt Fernsehbilder in vielen verschiedenen Auflösungen aus, so dass man keinen Ultra HD Fernseher

benötigt, um diesen Receiver zu verwenden, denn das Betrachten von 4K UHD-Inhalten auf einem 1080p Fernseher wirft die Frage auf, ob man überhaupt einen 4K Fernseher benötigt, da das Bild hell und klar ist. Wie wichtig ein 4K Fernseher ist, sieht am erst wenn echte UHD-Inhalte gesendet werden. Die Brillanz und die Tiefen sind unübertroffen. Leider hält sich die Anzahl der UHD-Sender in Grenzen.

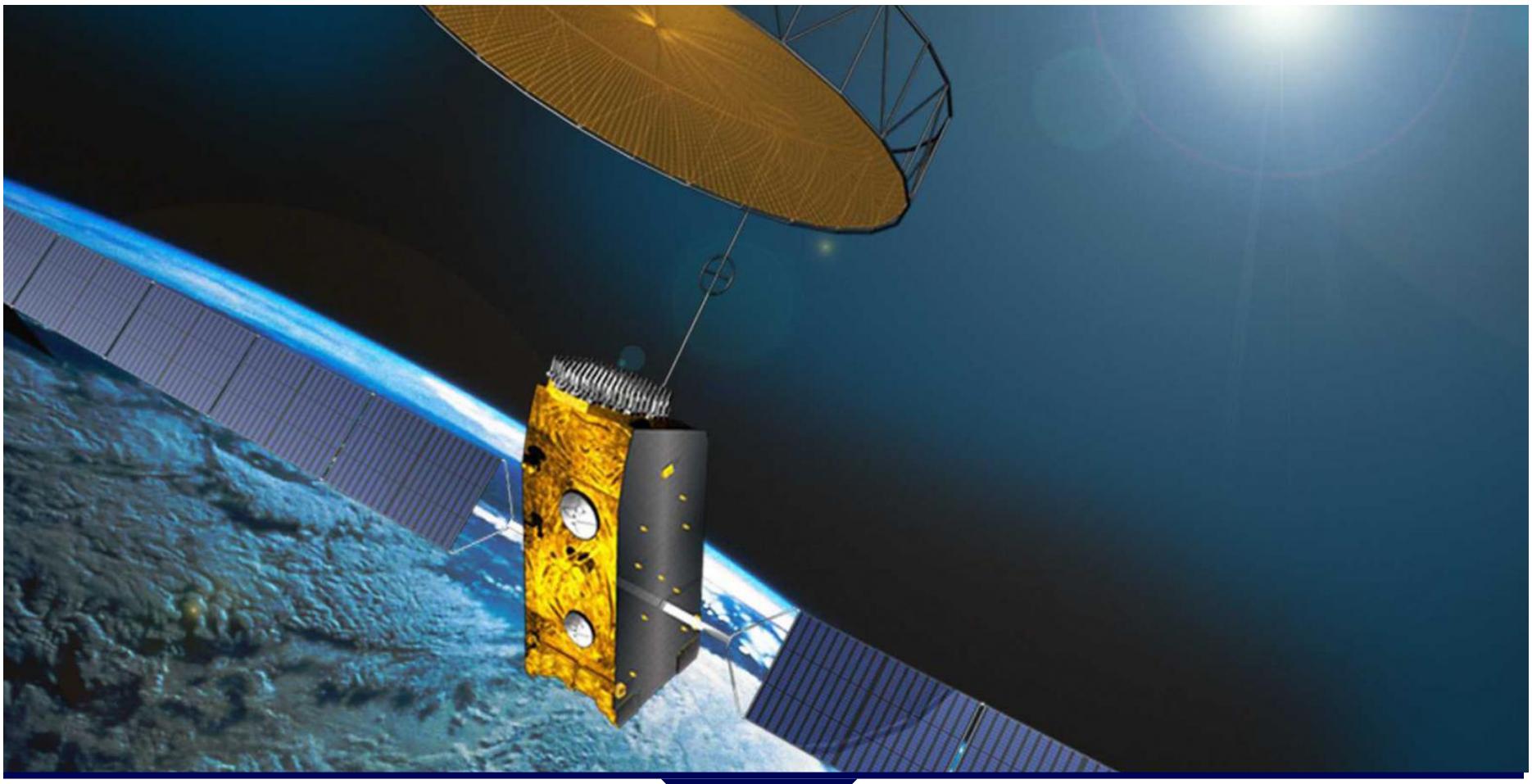
FAZIT

Der Ultimo 4K hat dank seines Quad Core Prozessors (mehr als seine kleine Schwester Solo4K oder der kleine Bruder Uno4K, die beide Dual Core sind) viel Rechenleistung, das bedeutet schnelle Boot-Up- und Restartzeiten, schnelles Kanal-Zappen und vor allem Stabilität. Der Ultimo 4K ist kein billiger Empfänger und wird mit Sicherheit die Satelliten-Freaks ansprechen, da er über Funktionen verfügt die der Enthusiast benötigt.

Sollten Sie man den Ultimo4K kaufen? Vom Autor gibt es hier nur ein klares JA als Antwort. Allein schon die Flexibilität bei der Tuner-Auswahl sind schon das Geld der Anschaffung wert. Aber auch im „normalen" Wohnzimmer tut der Ultimo 4K seinen Dienst als komfortabler und hochwertiger Familien-Receiver.



DAS INMARSAT SYSTEM



Inmarsat wurde 1979 durch Übereinkommen von Vertragsstaaten der Internationalen Seeschifffahrts-Organisation gegründet. Das Ziel war die Verbesserung der Nachrichtenverbindungen für die Schifffahrt via Satellit. Davon profitierten Schiffe in Regionen, die nicht durch den Kurz- oder Mittelwellen-Funk abgedeckt wurden.

Die ersten beiden Satelliten wurden noch angemietet,
doch seit 1983 werden eigene Satelliten genutzt.
Außer dem Standardangebot wie die satellitengestützten Telefonie- und
Internetanbindungen, Fax, Telexdienste bietet Inmarsat
auch Seenotkommunikationsdienste (GMDSS),
Flugsicherung (Future Air Navigation System)
und Transponder zur Verbesserung der
satellitengestützte Positionsbestimmung (GPS oder Galileo) an.

In der folgenden Tabelle sind die aktiven Satelliten
mit ihren Positionen und Abdeckungsbereichen aufgelistet.

5. GENERATION INMARSAT-SATELLITEN

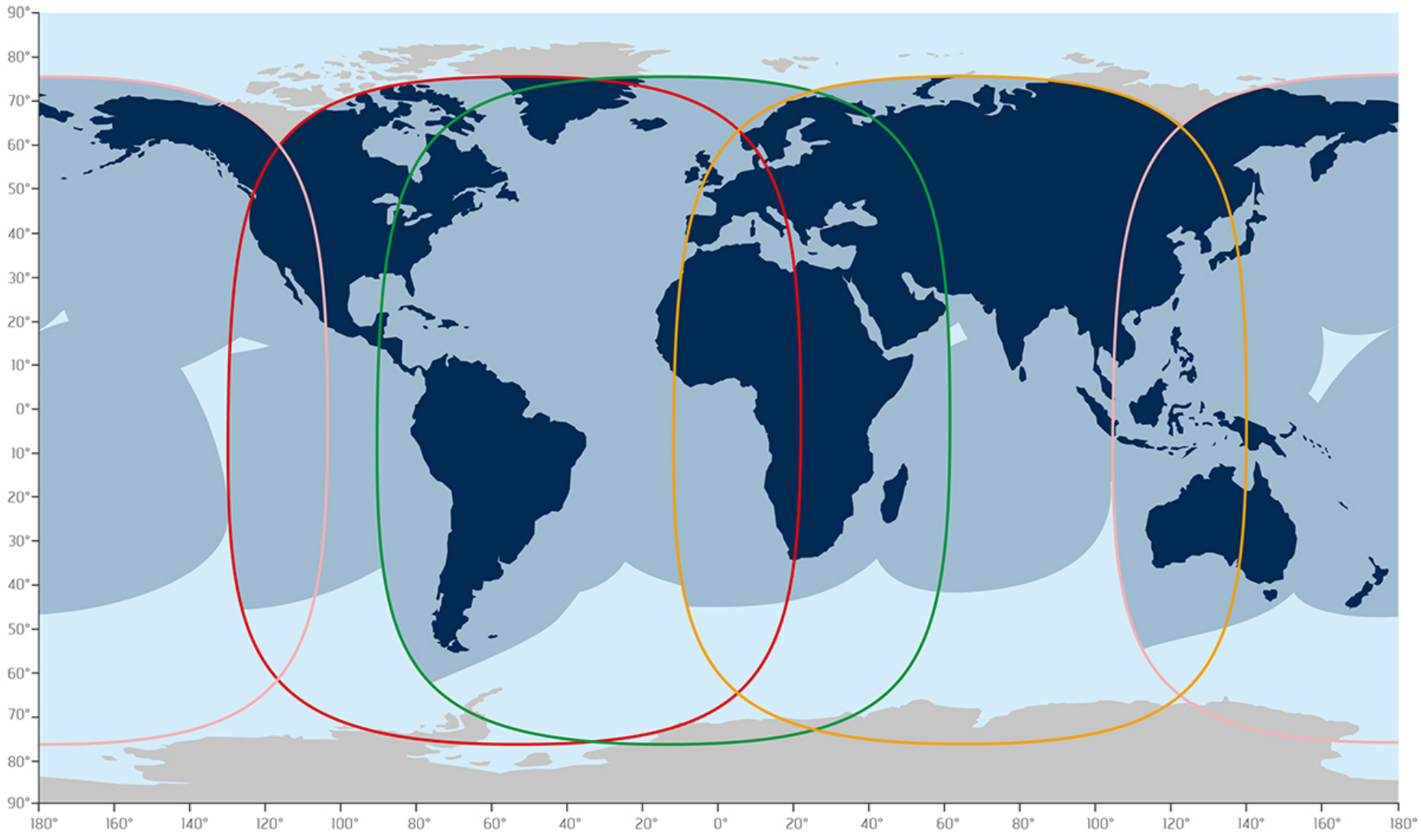
Inmarsat-5 F1	Asien-Pazifik	63° Ost
Inmarsat-5 F2	Amerika, Atlantik	55° West
Inmarsat-5 F3	Pazifik	179,6° Ost
Inmarsat-5 F4	Reserve	

4. Generation Inmarsat-Satelliten

Inmarsat-4 F1	Asien-Pazifik	143.5° Ost
Inmarsat-4 F2	Europa, Mittleren Osten, Afrika (EMEA)	25° Ost
Inmarsat-4 F3	Amerika	98° West
Inmarsat-4A F4	Europa, Mittleren Osten, Afrika (EMEA)	25° Ost

3. Generation Inmarsat-Satelliten

Inmarsat-3 F1	Indischer Ozean	64.5° Ost
Inmarsat-3 F2	Östlicher Atlantik	15.5° West
Inmarsat-3 F3	Pazifik 178° Ost	
Inmarsat-3 F4	Westlicher Atlantik	54° West
Inmarsat-3 F5	Europa, Mittleren Osten, Afrika (EMEA)	25° Ost



Inmarsat sendet im L-Band bei ca. 1,5 GHz. Mit einem RTL-SDR-Dongle, einer günstigen 10 Euro modifizierten GPS-Antenne oder einer Patch-, Dish-oder Helix-Antenne kann man diese Inmarsat-Signale empfangen und einem geeigneten Dekoder zuführen. Er sorgt dann für den Klartext. Zum Beispiel einen „Std-C NCS" Kanal. Dieser Kanal wird hauptsächlich von Schiffen auf See verwendet und enthält Enhanced Group Call (EGC) Nachrichten, die Informationen wie Such-und Rettungsdienste (SAR) und Küstenwache sowie Nachrichten, Wetter und Vorfallberichte enthalten. Weitere Informationen zum L-Band Empfang finden man auf der Seite **http://www.uhf-satcom.com/lband/**
Einige Beispiele für die EGC-Meldungen, die auf dem Std-C NCS-Kanal empfangen können, sind hier dargestellt:

```
PAN PAN
TROPICAL CYCLONE WARNING / ISSUED FOR THE NORTH OF EQUATOR OF METAREA
XI(POR).
WARNING 050900.
WARNING VALID 060900.
TYPHOON WARNING.
TYPHOON 1513 SOUDELOR (1513) 930 HPA
AT 19.9N 133.2E WEST OF PARECE VERA MOVING WEST 12 KNOTS.
POSITION GOOD.
MAX WINDS 95 KNOTS NEAR CENTER.
RADIUS OF OVER 50 KNOT WINDS 80 MILES.
RADIUS OF OVER 30 KNOT WINDS 240 MILES NORTH SEMICIRCLE AND 210 MILES
ELSEWHERE.
FORECAST POSITION FOR 052100UTC AT 20.1N 130.6E WITH 50 MILES RADIUS
OF 70 PERCENT PROBABILITY CIRCLE.
935 HPA, MAX WINDS 90 KNOTS NEAR CENTER.
FORECAST POSITION FOR 060900UTC AT 20.8N 128.1E WITH 75 MILES RADIUS
OF 70 PERCENT PROBABILITY CIRCLE.
935 HPA, MAX WINDS 90 KNOTS NEAR CENTER.
```

```
STRATOS CSAT 4-AUG-2015 03:21:25 436322
SECURITE
FM: RCC NEW ZEALAND 040300 UTC AUG 15

COASTAL NAVIGATION WARNING 151/15

AREA COLVILLE, PLENTY
CUVIER ISLAND (REPUNGA ISLAND), BAY OF PLENTY
1. LIVE FIRING 060300 UTC TO 060500 UTC AUG 15 IN DANGER AREA NZM204.
ANNUAL NEW ZEALAND NOTICES TO MARINERS NUMBER 5 REFERS.
2. CANCEL THIS MESSAGE 060600 UTC AUG 15
NNNN
```

```
NAVAREA XI WARNING
NAVAREA XI 0571/15
SINGAPORE STRAIT.
ARMED ROBBERY INFORMATION. 301845Z JUL.
01-04.5N 103-41.8E.
FIVE ROBBERS ARMED WITH LONG KNIVES IN A SMALL UNLIT HIGH SPEED BOAT APPROACHED A
BULK CARRIER UNDERWAY.  ONE OF THE ROBBERS ATTEMPTED TO BOARD THE SHIP USING A HOOK
ATTACHED TO A ROPE. ALERT CREW NOTICED THE ROBBER AND RAISED THE ALARM AND CREW RUSHED
TO THE LOCATION. HEARING THE ALARM AND SEEING THE CREW ALERTNESS, THE ROBBERS ABORTED
THE ATTEMPTED ATTACK AND MOVED AWAY. INCIDENT REPORTED TO VTIS SINGAPORE. ON ARRIVAL
AT SINGAPORE WATERS, THE COAST GUARD BOARDED THE SHIP FOR INVESTIGATION.

VESSELS REQUESTED TO BE CAUTION ADVISED.
```

Es ist eh ungemütlich draußen und so kommt ein gar nicht so aufwendiges Bastelprojekt für den Inmarsat-Empfang gerade recht.

DIE EIGENBAUANTENNE ODER EINE DVB-T ANTENNE

Manuel a.k.a. Tysonpower beschreibt in seinem neuesten YouTube Video-Tutorial den einfachen Bau einer 1550 MHz L-Band LHCP spiralförmigen Antenne für den Empfang von Satelliten-Signalen wie Inmarsat, Aero und HRPT (Wettersatelliten).

In dem Video verwendet er den spiralförmigen Feed an einer 80cm Satellitenschüssel und einer Standard-40mm LNB-Halterung auf dem Dish Arm. An der Zuführung sind zwei LNAs in Serie angebracht, die dazu beitragen, die Rauschzahl zu senken und Verluste im Koaxialkabel zu reduzieren.

Die 3D-Druck STL-Dateien und die Liste der benötigten Teile sind auf Thingiverse, und das Begleitvideo kann über **https://youtu.be/kNuf8zcLdHk** abgerufen werden.
Noch einfacher – jedoch mit weniger Verstärkung – geht es mit einer einfachen DVB-T Antenne. Um zu beweisen, dass man damit auch L-Band Inmarsat Aero Satellitensignale empfangen kann, hat das YouTube User Skywatcher in einem Video gezeigt.

DER EMPFÄNGER

Gute Empfänger für den Bereich um 1.500 MHz kosteten vor gar nicht langer Zeit ein kleines Vermögen. Heute reicht ein DVB-T USB Stick für unter 22 Euro. Hier kann man das Modell TV28T v2 von NooElec (Aamazon.de) empfehlen.
Was nun noch fehlt, ist ein Stück Software zu richtigen Darstellung der Signale. Das kostenlose Programm SDR# erfüllt genau diesen Zweck. Zusätzlich sorgt das kleine Programm ZADIG für die Einbindung des passenden Treibers. Downloads für SDR# und Zadig gibt es bei **https://www.ocinside.de/modding/sdr_anleitung_d/3/**

AUF GEHT´S

Nun geht es an die ersten Empfangsversuche und die Ausrichtung der Antenne. Für unsere Breitengrade ist der Inmarsat-3 F2 auf 15.5° West genau der Richtige. Doch zuvor brauchen wir eine aktive Frequenz.

Wir schalten auf den Modus USB (upper side band) und tunen genau 2 kHz unter der mittleren Frequenz. Zum Beispiel. wenn die mittlere Frequenz genau 1.541.450.000 kHz ist, dann tunen wir auf 1.541.448.000 kHz.

Bei der Bandbreite wird ca. 4 kHz (4000) eingestellt. Wichtig ist, dass SDR# zuvor auf einer bekannten Frequenz abgeglichen wird. Man kann hier einen bekannten Amateurfunk-Repeater nehmen und einen eventuellen Frequenz-Offset an die echte Frequenz anpassen.

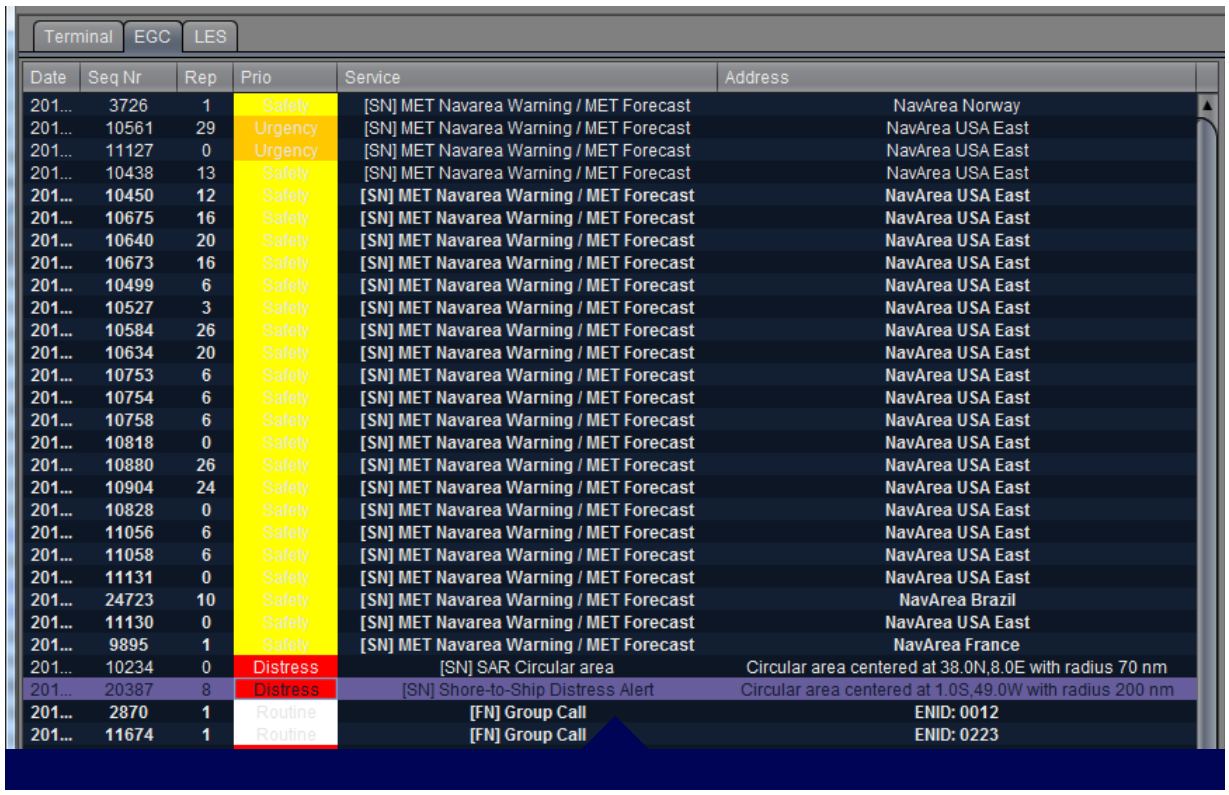
Die Antennen-Elevation ist nicht also kritisch. Bei rund 20° sollte der 3F4 bereits empfangbar sein. Ist das Signal hörbar und im Spektrum des SDR# sichtbar, dann folgt die Feineinstellung der Antenne.

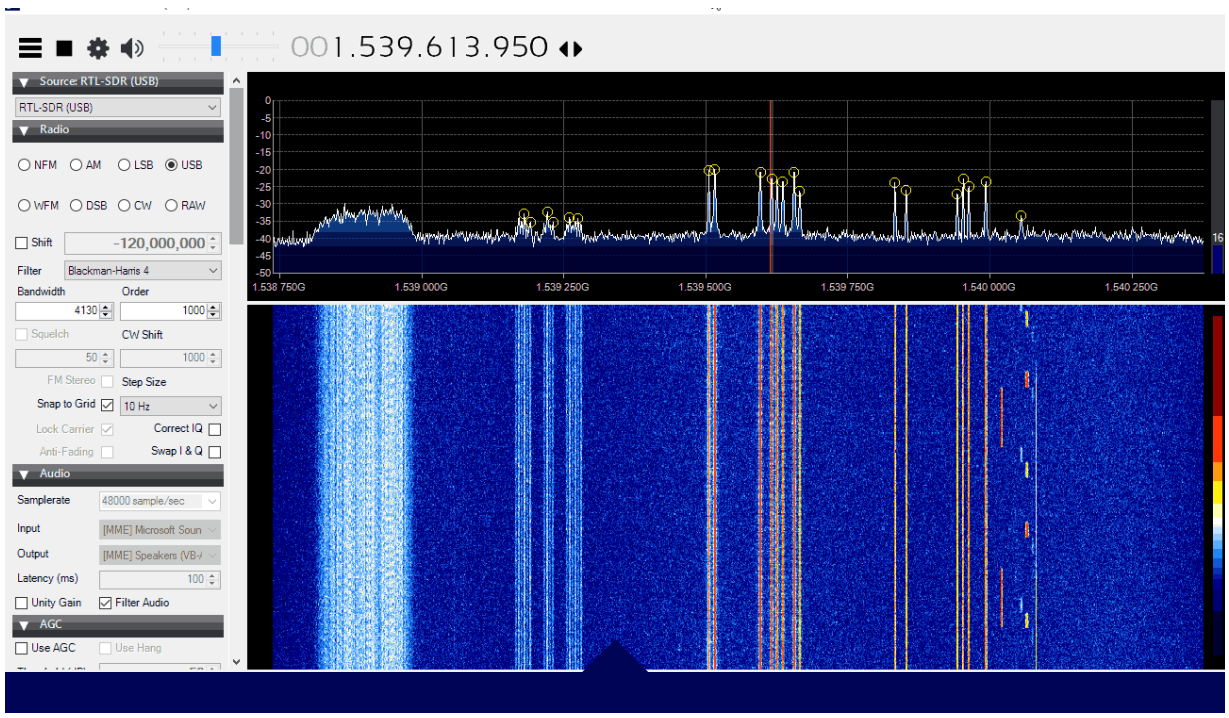
DER DEKODER

Nun fehlt nur noch der Dekoder. Dieser muss mit einem virtuellen Audiokabel mit SDR# verbunden werden. Eine kostenlose Version des Programms Virtual Audio Cable 4.14 gibt es bei Chip.de. Der TEKMANOID (**http://www.tekmanoid.com/**) wurde bei ersten Tests erfolgreich genutzt. Es gibt Tekmanoid in ein einer Pro-Version für 50 Euro, die wesentlich mehr kann. Als Beispiel seien die LES-Kanäle angeführt. Da hier auch private Kommunikation zu hören ist, sollte der Nutzer sehr diskret sein. Hier eine Liste der LES-Kanäle:

Über weitere Satelliten im L-Band gibt es weiterführende Infos auf **http://www.uhf-satcom.com/lband/**

Achtung: der Empfang und/oder die Dekodierung ist nicht in jedem Land erlaubt. Dieser Bericht dienst rein edukativen Zwecken.





FEEDSIGNALE

DVB S und S2 Empfang für 20 Euro

... wer auf der Suche nach Feedsignalen bis zu einer Symbolrate von 8.000 ksym/s ist, wird seinen Spaß haben.

Vor 35 Jahren baute ich meinen ersten Satelliten-Receiver für den russischen Satelliten GORIZONT im C-Band auf 14 Grad West. Billig war die Sache trotz Eigenbaus nicht. Aus den USA wurde ein Tuner (960 – 1.450 MHz) bezogen. Der Rest kam aus der Bastelkiste. Die Frequenzeinstellung erfolgte über ein simplen VFO und ein Display gab es nicht. Alles zusammen schlug mit etwa 400,- DM (200,-Euro) zu Buche. 600,- DM wurden in einen LNA und einen LNC (damals kamen sie noch separat) investiert. Der Feed war Marke Eigenbau. Als Antenne eine 160 cm Parabolantenne vom Surplus-Handel aus militärischen Beständen.

Heute gibt es zwar nagelneue Set Top Boxen ab ca. 30 Euro, doch der Reiz liegt im do it yourself. Die Frage nach einem passenden Tuner stellt sich nicht mehr, da man dafür ca. 20 Euro einen DVB-T Stick nutzen kann. Da fehlt eigentlich nur noch die passende Software. Es gab für SDR-Projekte zwar die Software „TVSharp", doch die stellt nur analoges TV dar und diese Signale sind Geschichte.

Eigentlich wollte ich nur erste Empfangsversuche des Es Hail-2 Geosat auf 25,9 Grad Ost wagen. Im Forum von AMSAT DL wurde ich fündig und fand geeignete Software (DVB S2 Demod GUI) von Marcel Kröner. Bei genauerer Betrachtung

der Oberfläche entdeckte ich neben den Modi DVB-S und S2 (nur QPSK) alle gängigen Einstellungen für den Empfang von Kommunikations-Satelliten:

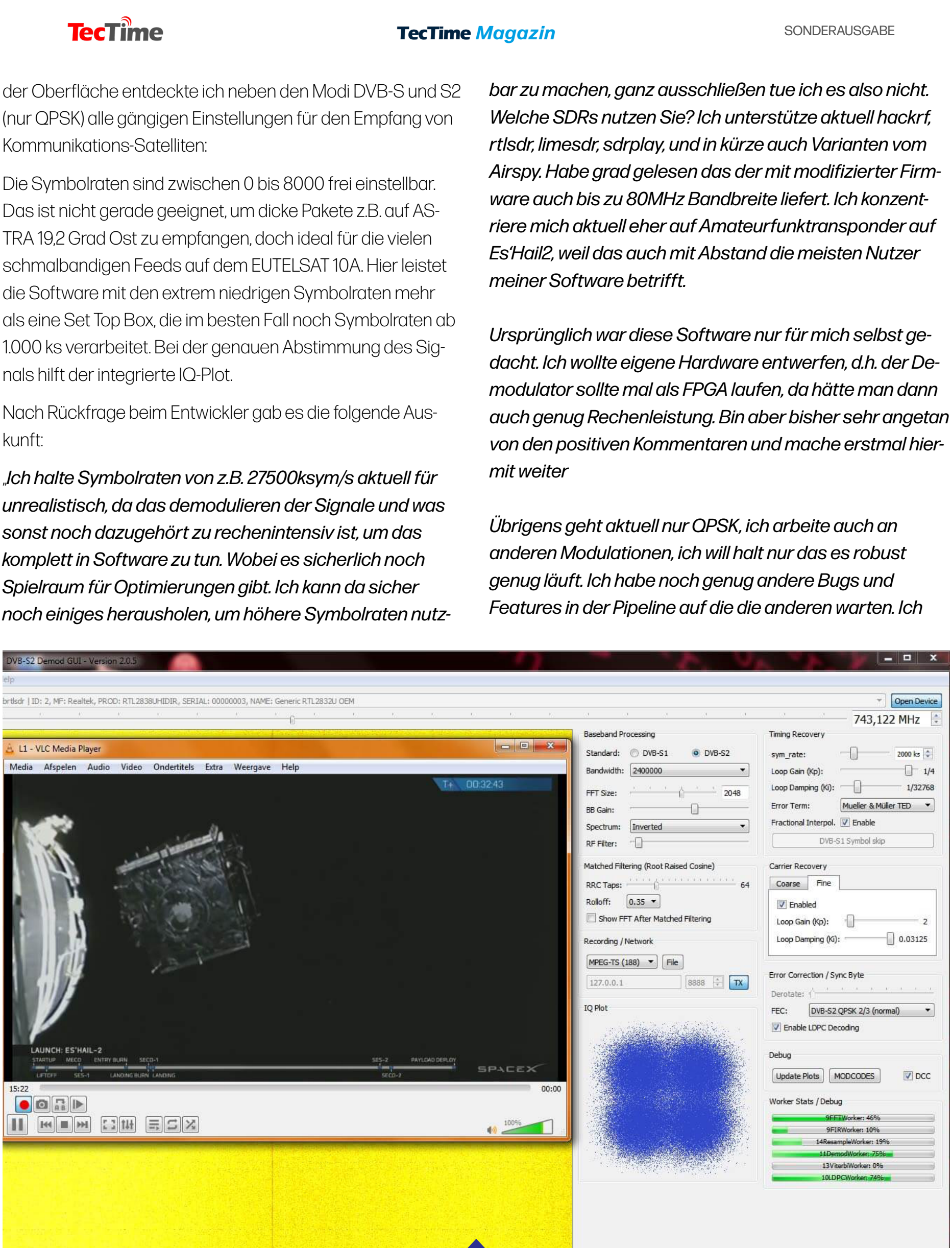
Die Symbolraten sind zwischen 0 bis 8000 frei einstellbar. Das ist nicht gerade geeignet, um dicke Pakete z.B. auf ASTRA 19,2 Grad Ost zu empfangen, doch ideal für die vielen schmalbandigen Feeds auf dem EUTELSAT 10A. Hier leistet die Software mit den extrem niedrigen Symbolraten mehr als eine Set Top Box, die im besten Fall noch Symbolraten ab 1.000 ks verarbeitet. Bei der genauen Abstimmung des Signals hilft der integrierte IQ-Plot.

Nach Rückfrage beim Entwickler gab es die folgende Auskunft:

„Ich halte Symbolraten von z.B. 27500ksym/s aktuell für unrealistisch, da das demodulieren der Signale und was sonst noch dazugehört zu rechenintensiv ist, um das komplett in Software zu tun. Wobei es sicherlich noch Spielraum für Optimierungen gibt. Ich kann da sicher noch einiges herausholen, um höhere Symbolraten nutzbar zu machen, ganz ausschließen tue ich es also nicht. Welche SDRs nutzen Sie? Ich unterstütze aktuell hackrf, rtlsdr, limesdr, sdrplay, und in kürze auch Varianten vom Airspy. Habe grad gelesen das der mit modifizierter Firmware auch bis zu 80MHz Bandbreite liefert. Ich konzentriere mich aktuell eher auf Amateurfunktransponder auf Es'Hail2, weil das auch mit Abstand die meisten Nutzer meiner Software betrifft.

Ursprünglich war diese Software nur für mich selbst gedacht. Ich wollte eigene Hardware entwerfen, d.h. der Demodulator sollte mal als FPGA laufen, da hätte man dann auch genug Rechenleistung. Bin aber bisher sehr angetan von den positiven Kommentaren und mache erstmal hiermit weiter

Übrigens geht aktuell nur QPSK, ich arbeite auch an anderen Modulationen, ich will halt nur das es robust genug läuft. Ich habe noch genug andere Bugs und Features in der Pipeline auf die die anderen warten. Ich

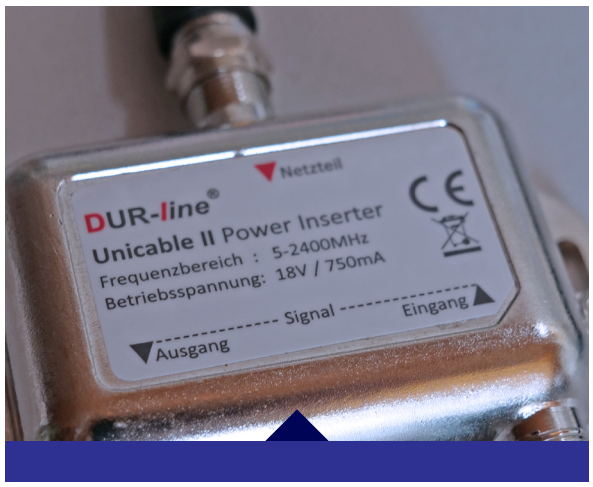


Es'hail 2 at 25.8°E

werde den Symbolraten-Bereich mal via Config Datei änderbar machen, dann ist das ganze flexibler. Wird dann in Version 2.0.11 drin sein.“

Wenn man schon mal dabei ist sollte man einen Empfangsversuch des Es´Hail 2 auf 25,8 Grad Ost wagen. Dummerweise sendet der Promo-Kanal auf 10.942 GHz horizontal (Symbolrate 2.000 und FEC 2/3, QPSK). Um diese Frequenz zu erreichen bedarf es einen Eingriff in den LNB. Und was und wie man das macht, dass gibt es bei AMSAT DL als Anleitung:

https://forum.amsat-dl.org/index.php?thread/78-umbau-octagon-optima-lnb-auf-tcxo/



WAS MAN SONST NOCH BRAUCHT

Nun reichen die Software der SDR Stick und eine Antenne mit LNB für den Empfang noch nicht aus. Es fehlen die 14 Volt (horizontal) und 18 Volt (vertikal) für den LNB. Diese Spannungen müssen extern zugeführt werden. Die betagten DXer werden im Keller bestimmt noch eine Einspeiseweiche aus uralten Satellitentagen finden, oder Ebay & Co. sind hier hilfreich. Aber auch auf Amazon findet man solche Teile. Wenn´s geht gleich mit 22 kHz-Schaltung für das Unter- und Oberband.

Beim Anschluss der externen Stromversorgung sollte man unbedingt darauf achten, dass der spannungsführende Ausgang mit dem LNB verbunden wird und nicht umgekehrt. Das wäre ungesund!

FAZIT

Um zuhause im Sessel zu sitzen, um einen gemütlichen TV-Abend zu genießen, ist DVB S2 Demod GUI nicht geeignet. Jedoch wer auf der Suche nach Feedsignalen bis zu einer Symbolrate von 8.000 ksym/s ist, wird seinen Spaß haben. Und in der Software ist noch Luft nach oben drin.

KRIMINELLE SDR-PROJEKTE

Das SDR wird zum Mittäter

Der RollJam ist in der Lage, jedes Auto oder jede Garage mit nur einem einfachen Knopfdruck zu entriegeln und macht so wird „Auto Hacking“ zum Kinderspiel.

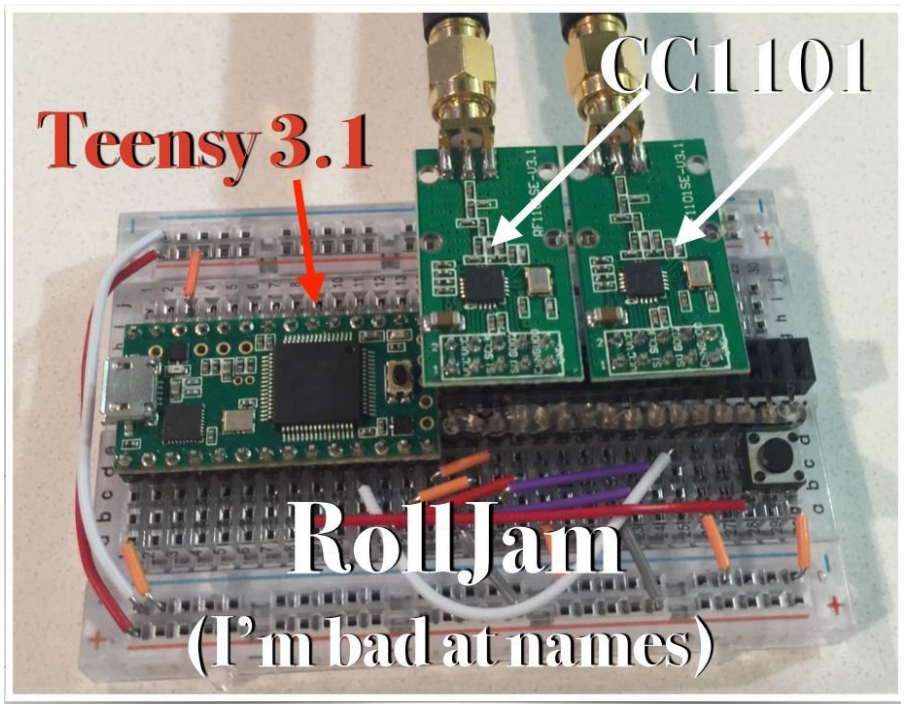
Das Hacker einen Jeep Cherokee während der Fahrt aus der Ferne entführen können, um die volle Kontrolle über die Lenkung, die Bremsen und sogar das Getriebe der Fahrzeuge zu erlangen, wurde bereits beweisen. Auch die Öffnung eines geparkten Wagens oder eines Garagentors ließ sich mit Hilfe eines kleinen SDR Tranceivers mühelos bewerkstelligen. Das vom Schlüssel des Wagenbesitzers gesendete Öffnungssignal wurde einfach empfangen und aufgezeichnet.

Im Schutz der Nacht sendete Dieb das aufgezeichnete Signal an das Auto und schon war die Tür offen und der High-Tech Dieb konnte das Auto ausräumen. Diebesbanden aus Osteuropa mussten nun nicht mehr die Türschlösser aufbrechen, sondern erledigten ihren Job in Sekundenschnelle und vor allen Dingen geräuschlos.

Die Versicherungen sahen ihren Profit schwinden und machten druck auf die Autoindustrie die Fahrzeuge besser abzusichern. Das Ergebnis war die Erfindung des „Rolling Codes“. Und der funktioniert so:

Wenn der Autobesitzer auf seinem Funkschlüssel die Taste „Unlock/Lock“ drückt wird ein Code an das Schloss der Autotür gesendet und die Tür lässt sich öffnen. Dieser Code ist einmalig und kann nicht mehr verwendet werden. Für das nächste Mal wird ein neuer Code generiert und so weiter. Das Türschloss verfügt auch über einen synchronisierten Codegenerator, der den zugewiesenen Code nicht nur erkennt, sondern auch zerstört. Dadurch wird verhindert, dass der Code erneut verwendet wird.

Eine ganze Zeitlang durften sich die Autobesitzer sicher fühlen. Wäre da nicht der Hacker Samy Kamkar. Er hatte sich bereits in der Vergangenheit einem Namen mit der Analyse und dem Hack unsicherer digitaler Kandidaten gemacht.



Samy Kamkar´s Rolljam-Projekt

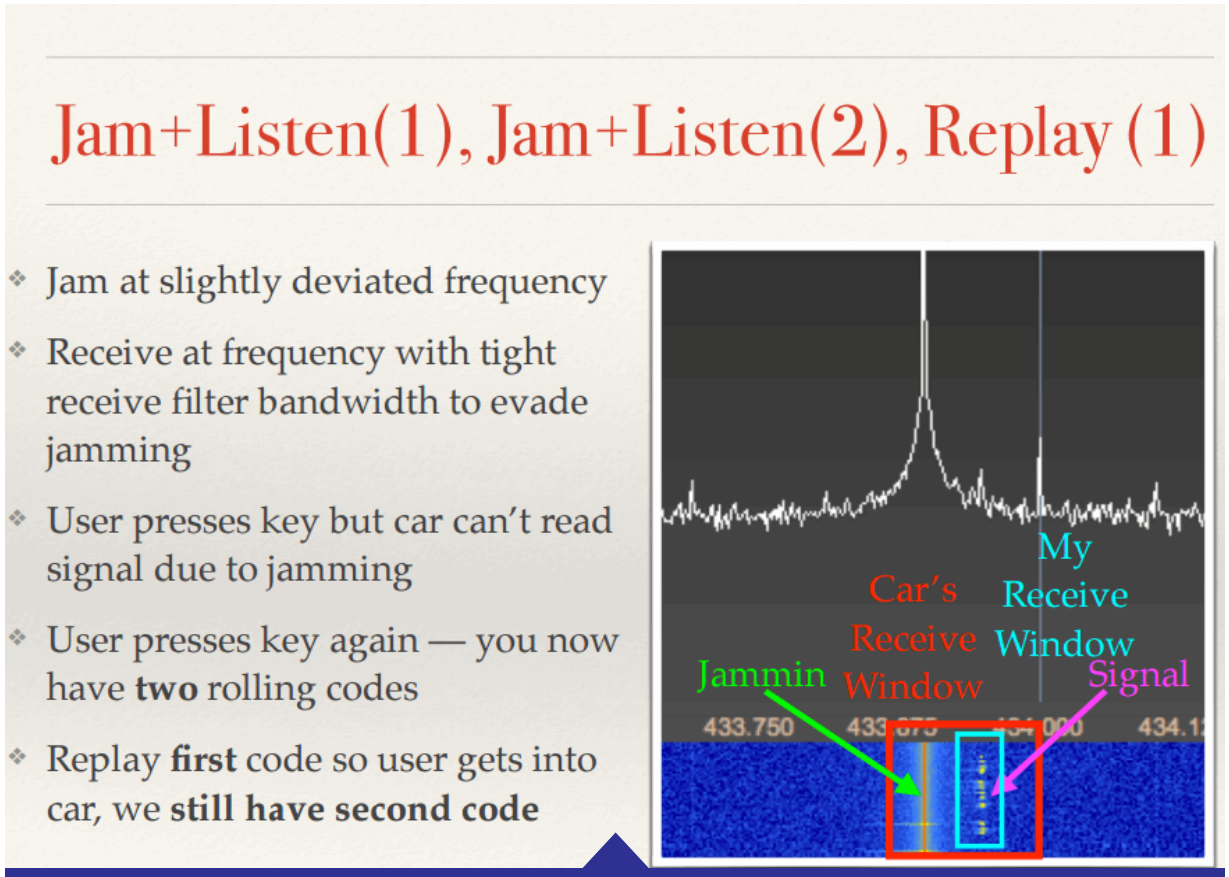
ROLLJAM

Mit nur zwei SDR Transceivern (CC1101 oder Noolelec Yardstick One), einem Mikrocontroller (Teensy 31.) und einer Batterie, die alle über eBay für weniger als 50 Euro (mit Ausnahme des Yardstick) erhältlich sind, hat der unabhängige Forscher Samy Kamkar den Versicherungen und Autoherstellern das Fürchten gelehrt.

Sein sogenannter RollJam nutzt einen Designfehler im Protokoll, der bestimmt, wie Schlüssel mit Autos kommunizieren. Es fängt „Rolling Codes" ab, die einmaligen Authentifizierungscodes, die mit dem Auto und dem Schlüssel ausgetauscht werden und sich bei jedem Sperren und Entsperren ändern. Da es keine Zeitüberschreitung bei den Codes gibt, kann RollJam sie abfangen, um sicherzustellen, dass sie nie das Auto erreichen, und so später verwendet werden können. Selbst wenn das Gerät nur Sperrcodes sammelt, behauptet Kamkar, ein Verfahren entwickelt zu haben, dass diese in Entsperr-Codes umwandeln kann. „Ich kann einige Informationen innerhalb des Signals umdrehen", sagte er.

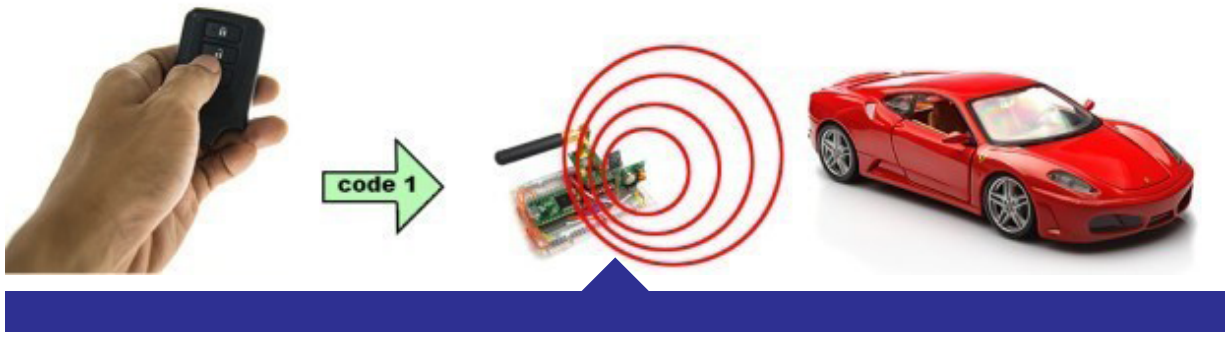
Samy Kamkar, der seine Entwicklung auf der DEF CON-Konferenz in Las Vegas zeigte, sagte, dass seine Kreation im Wesentlichen dazu bestimmt war, auto-gnostisch zu sein und „viele verschiedene Arten von Autos in Marken und Modellen freizuschalten.... es ist wie eine universelle Fernbedienung". „An meinem Auto, wo ich Zeit habe, mir das Signal oder den Chip anzusehen, kann ich den Unterschied zwischen Sperren und Entsperren sehen und mein Gerät kann es live verändern", sagte er zu FORBES.

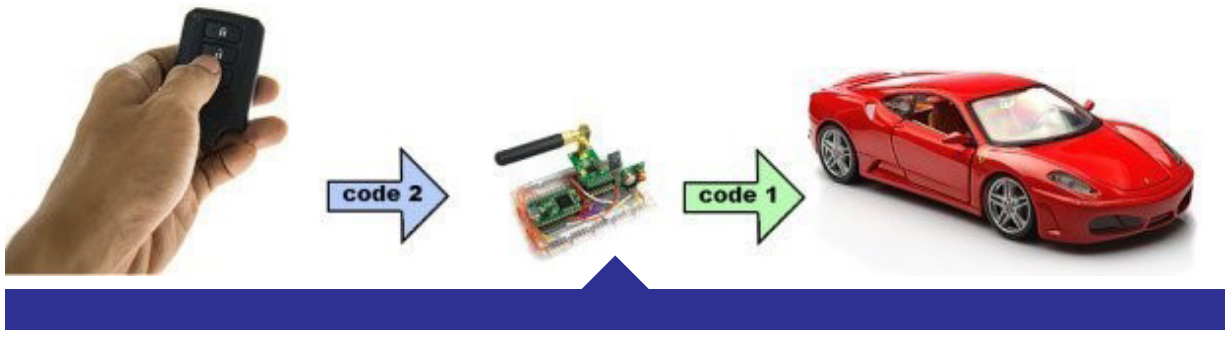
Der RollJam ist in der Lage, jedes Auto oder jede Garage mit nur einem einfachen Knopfdruck zu entriegeln und macht so wird „Auto Hacking" zum Kinderspiel.

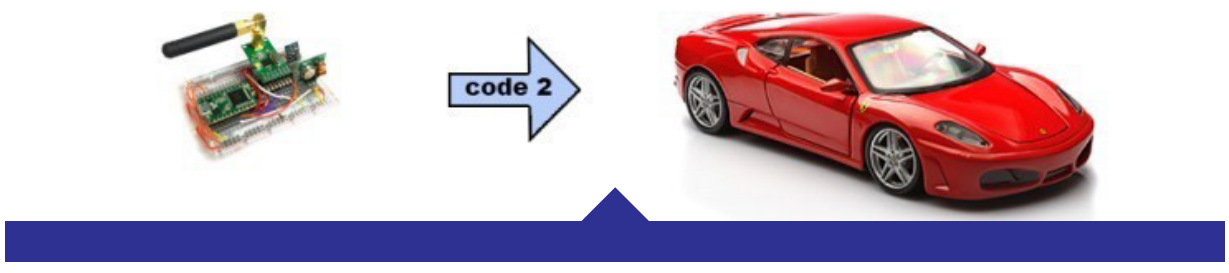


Dicht neben das Schlüsselsignal wird ein Störträger gesetzt und gleichzeit das Originalsignal aufgezeichnet.

WIE FUNKTIONIERT ROLLJAM?







Die Antwort ist leider einfach. Was der RollJam macht, ist, dass er tatsächlich die Funkfrequenz stört und somit blockiert, so dass das Auto den Besitzer zwingt, die Taste noch einmal zu drücken.

Durch die Blockierung des Code 1 errichte dieser nicht das Auto und bleibt somit weiter gültig. Diesen Code speichert der Dieb für die spätere Verwendung. Nachdem beim ersten Druck auf die Taste sich das Auto nicht öffnete, drückt der Besitzer automatisch ein zweites Mal. Und da der Störsender nun ausgeschaltet ist, öffnet sich das Fahrzeug ganz normal. Der Dieb ist nun im Besitz eines gültigen Codes und hat Zugang zum Fahrzeug wann immer er es will.

Der Materialaufwand liegt bei ca. 50 Euro. Professionellen Dieben bietet ein russisches Unternehmen den Rolljam für glatte 900 Dollar an. Und zwar unbehelligt. Auch wenn sich der Rolljam nur eine Funktion hat: Autos aufzubrechen!

Home / Uncategorized / Rfid Rooljam

Rfid Rooljam

$900.00

The Device that can intercept and store keyless entry codes for cars and garage (Ready to use straight out of the box)

1 Add to cart

Category: Uncategorized

Description **Reviews (0)**

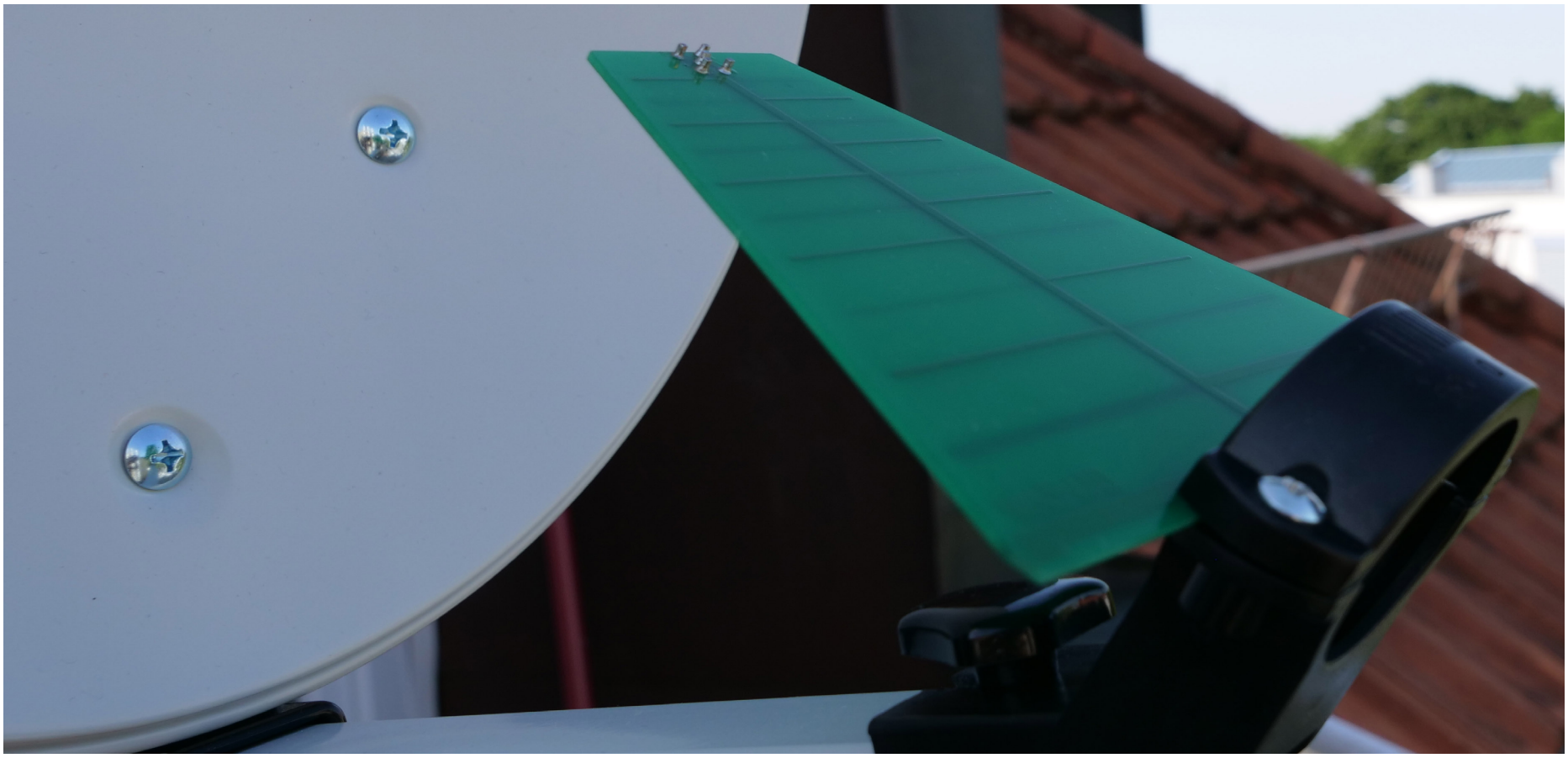
"RollJam" device is said to allow its user unfettered access to your automobile or garage, via stolen electronic codes.

The concept is fairly simple. The device tricks you into giving it a functional code for your car or garage by making it appear as though the first click of the remote simply didn't work. By then clicking again, you're giving it two functional codes. It can then sacrifice one code to unlock your car and keep you from thinking about the fact that you were just hacked.

INMARSAT KOMMUNIKATION MITLESEN

SDR-Projekte

Die Ausbeute dieser Fleißarbeit ist die Kommunikation vom Boden zum Flugzeug. Und das sind Wetterdaten, Flugplatzmeldungen, Sicherheitsmeldungen und ganz normale Schlagzeilen für das On Board Entertainment System.



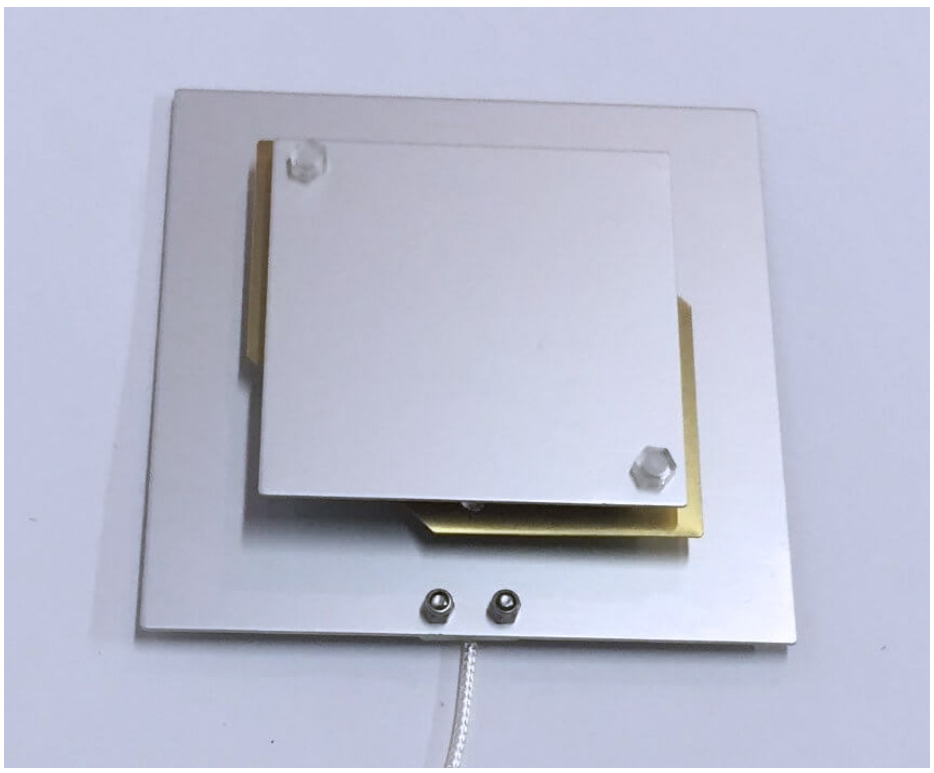
ACARS wurde hier bereits vorgestellt. Die ACARS-Daten auf 1090 MHz sind gut zu empfangen und genauso leicht zu dekodieren. Nachteil: mit der eigenen Antenne sieht man vielleicht im besten Fall 600 km weit. Die weltweite Kommunikation zwischen den Bodenstationen und den Flugzeugen findet im L-Band und im C-Band auf der Inmarsat-Flotte statt. Und da wir uns in der Mitte Europas befinden wäre der Inmarsat 3-F2 auf 15.5° West das ideale Opfer. Inmarsats kommunizieren im L-Band und im C-Band. Wir beschränken uns hier auf das L-Band, wo der Antennenaufwand deutlich geringer ist. Und hier wählen wir dann den NCS-Channel (Network Controll Station) auf 1.541,50 Hz aus. Was ist an Hardware nötig? Da ist erst einmal die Antenne. Ideal ist eine Eigenbau Wendelantenne mit 10 Windungen. Infos dazu gibt es auf **https://www.rtl-sdr.com/?s=Inmarsat+antenna**

Aber auch eine logperiodische Antenne (ca. 9 Euro) an der Feedhalterung einer 35cm-Offset-Antenne (ca. 20 Euro) tut es. Wenn auch nicht besonders gut, da das Inmarsat-Signal zirkular (RHP) ankommt und die logperiodische Antenne linear ausgelegt ist. Aber es funktioniert. Wie auch bei der Wendelantenne wird der Verstärker für 1,5 GHz direkt hinter die Antenne geschaltet. Wer Glück hat, findet im Internet für ein paar Euro eine „Outernet Patchantenne“ (diesen Begriff googeln).‘

Und ganz billig geht es mit einer auf das Fenster zu klebenden Antenne für rund 9 Euro bei Amazon (unter DVB-T Antennen, Modell SL 1000).

Nun zum Empfänger. Die Zeiten eines extrem teuren Gerätes – wie ein AOR – sind vorbei. Für rund 25 Euro gibt es gute SDR-USB-Sticks. Wir z.B. von „Nooelec“ bei Amazon. Inder Regel endet der Frequenzbereich oben bei etwas 1.700 bis 2.000 MHz. Und das passt. Die nötige Empfängersoftware gibt auf **https://airspy.com/download/** Hier sollte man gleich das ganze Paket „Windows SDR Software Package“ runterladen und installieren

So, und nun kommen wir zur Ausrichtung der Antenne. Am Redaktionsstandort in der Nähe von München gelten folgende Daten: Elevation: 28.8° und Azimuth (magn.): 211.3°.

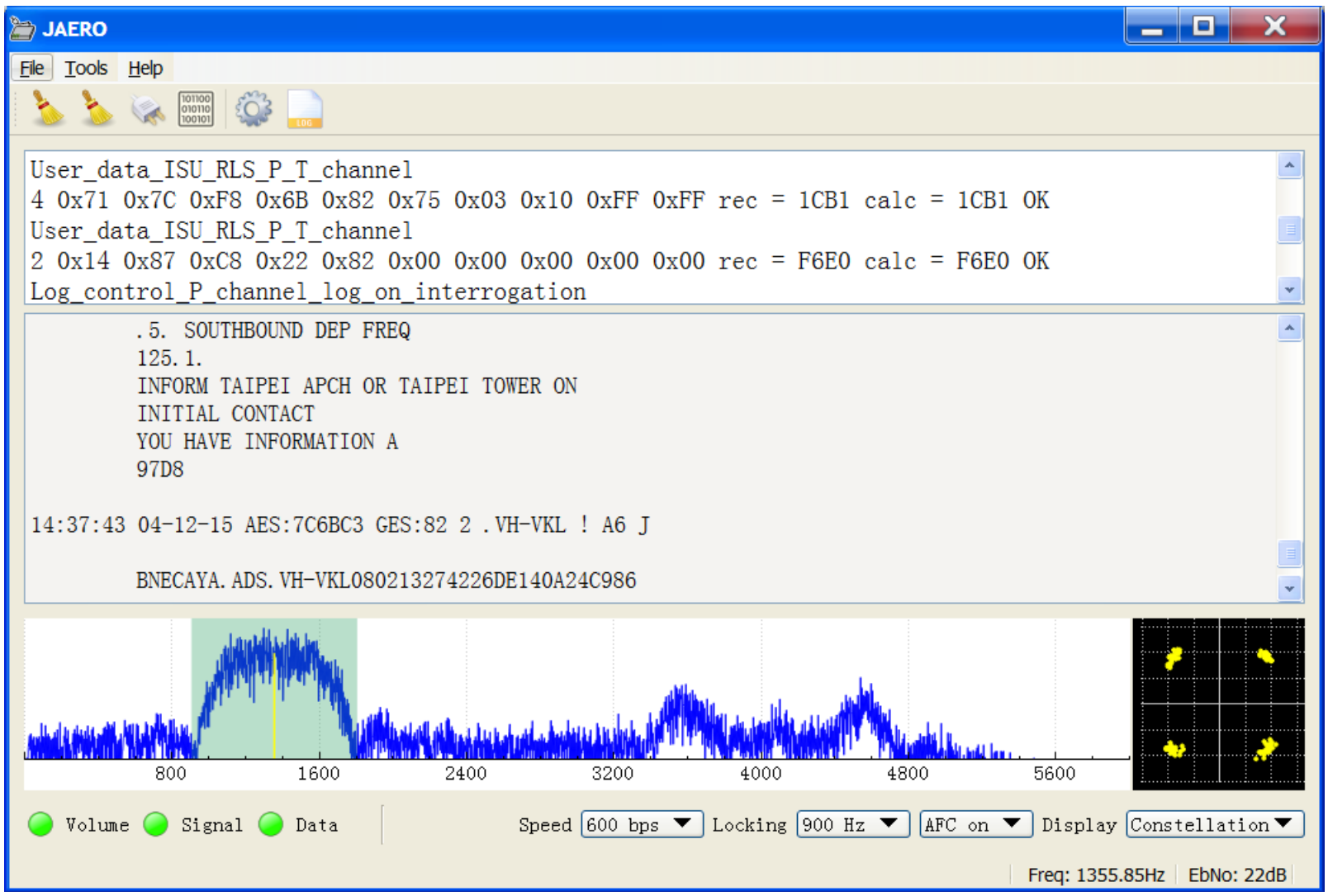


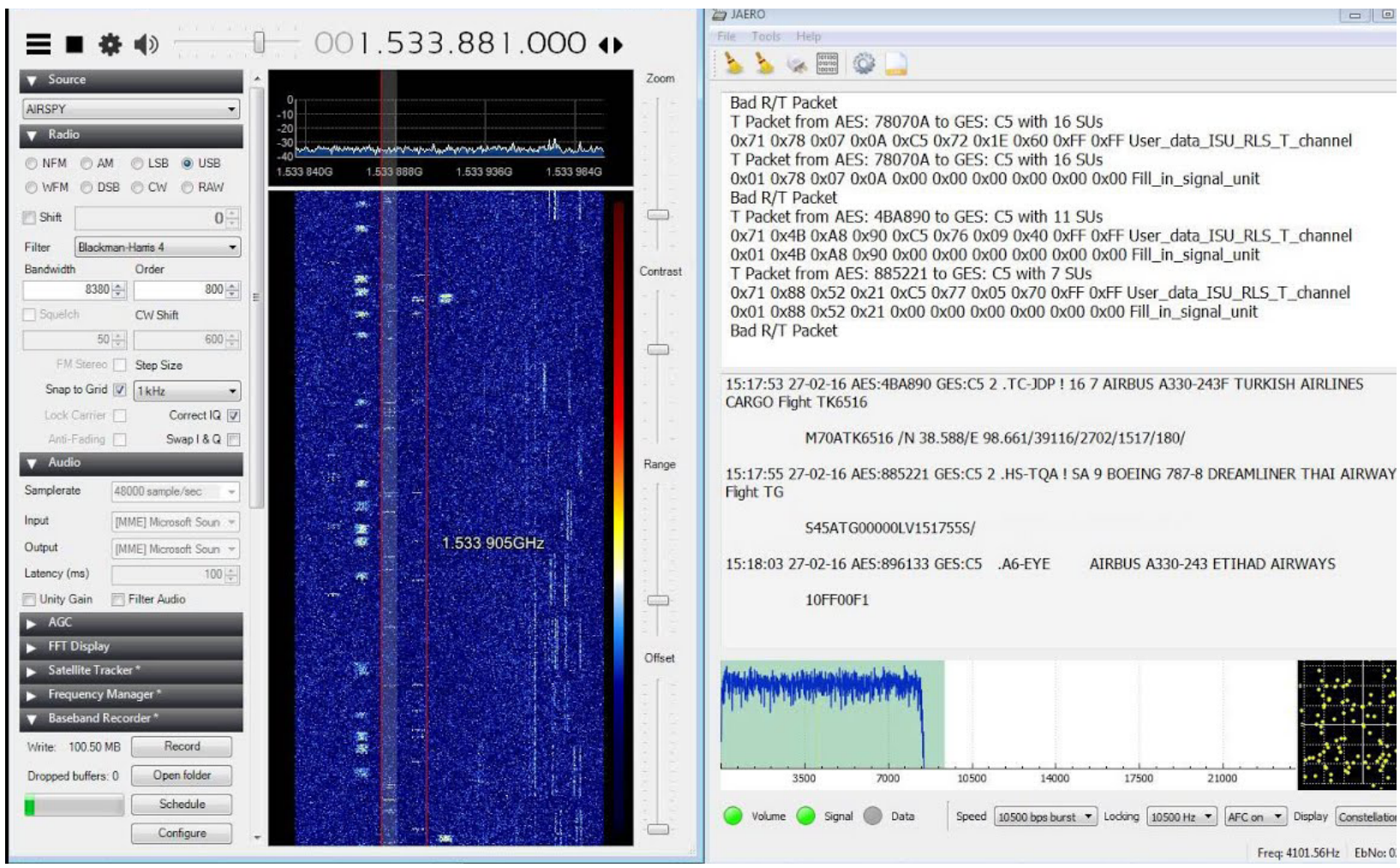
Den eigenen Standort kann auf man auf **http://www.satz-entrale.de/sat/dishpointer.shtml** eingeben und den Satelliten wählen und schon gibt es das passende Ergebnis.

Auf 1.541,450 MHz sollte ein Signal erscheinen. Wichtig ist die SSB-Einstellung der Empfänger-Software. Richtig ist: „USB“. Jetzt haben wir das Signal und es fehlt nur noch die Dekodier-Software. Und die gibt es auf: **http://jontio.zapto.org/hda1/jaero.html**. Eeinfach die Software runterladen und installieren. Bitte nicht vergessen. Zwischen der Empfängersoftware und Jaero muss ein virtuelles Audiokabel installiert werden und das gibt es kostenlos im Internet.

Die Ausbeute dieser Fleißarbeit ist die Kommunikation vom Boden zum Flugzeug. Und das sind Wetterdaten, Flugplatzmeldungen, Sicherheitsmeldungen und ganz normale Schlagzeilen für das On Board Entertainment System.

Und wer hier noch weiterkommen möchte, dem bieten wir in der nächsten Ausgabe des TecTime-Magazins ein Projekt zur Entschlüsselung der Audio-Kommunikation via Inmarsat.





Satellitenempfang: DER ANFANG VOM ENDE?

„DA KOMMT WAS, DA IST WAS, DA WAR WAS!"

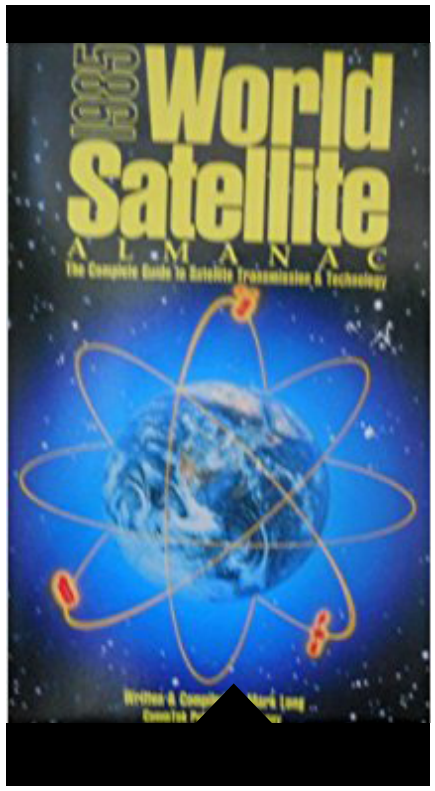
Mit der Zeit gab es Kommunikation zwischen etwa fünf europäischen Freaks, die sich per Telefon die Empfangsdaten zuriefen.

Ted Turner – der Gründer von CNN – propagierte 1984 in den USA den TV-Empfang via Satellit. In vielen Gegenden auf dem flachen Land war der terrestrische Empfang nicht möglich und Tageszeitungen waren bei Ankunft schon zwei Tage alt. So mancher Farmer ließ sich eine 5 Meter Schüssel installieren und lebte plötzlich in der Jetzt-Welt.

In Europa war Satellitenempfang kein Thema, denn die terrestrische Grundversorgung war gegeben. Allerdings gab es ein paar Freaks, denen war das nicht genug und sie suchten nach einer Lösung. Die bot sich 1985 bei der Firma Stodiek aus Düsseldorf an.

Zum Einkaufspreis von rund 7.000,- DM (so hieß die Währung damals) gab es einen 12 Kanal- DX-Antenna Empfänger, eine 1.40 Meter Offset-Antenne und einen ein Riesen-LNB ebenfalls vom japanischen Hersteller DX-Antenna. Nachteil der ganzen Geschichte: bei dem LNB gab es noch keine Umschaltmöglichkeit zwischen horizontal und vertikal. Also musste ein OMT (Orthomode Transducer) und ein zweiter LNB her. Die beiden Teile rissen ein 1.600,- DM Loch in die Portokasse. Wer das Geld nicht ausgeben wollte, der stieg durchs Fenster auf das Vordach und drehte den LNB um 90 Grad.

Die Suche nach aktiven Satelliten erforderte eine Kontrollperson vor dem Fernseher und einen Dreher an der Antenne. Vorsichtig wurde die Antenne nach Osten und Westen bewegt. Bis von innen der



Aufschrei kam: „da kommt was, da ist was, da war was!“ Mit der Zeit gab es Kommunikation zwischen etwa fünf europäischen Freaks, die sich per Telefon die Empfangsdaten zuriefen. Es gab damals keine Fachzeitschriften. Lediglich die Tele-Audiovision brachte erste zögerliche Berichte.

In dieser Situation kam dem Autor die Ausgabe 1985 des „World Satellite Almanac“ von Mark Long auf den Tisch. Was für eine Erleichterung. Weltweit waren hier alle Satelliten mit Sendern gelistet. Hinzu kamen viele Fachartikel, die von der DXer-Gemeinde verschlungen wurden. 13 Grad Ost, 60 Grad Ost und 27.5 Grad West waren die in Europa empfangbaren Positionen. Der Anfang war gemacht.

Satellitenempfang wird hoffähig. Während im benachbarten Ausland der Satellitenempfang mehr und mehr Freunde fand, war Deutschland zwischen 1985 und 1987 noch ein Satelliten-Niemandsland. Das sollte sich ändern, als Peter Lepper 1987 sein Unternehmen TechniSat in Daun / Eifel gründete. Er lud zu einer Presse-Präsentation ein und zeigte stolz die ersten TechniSat „Eigenentwicklungen“.

Der Besucher aus dem benachbarten Ausland entdeckte schnell, dass der vorgestellte Receiver aus dem Hause DRAKE aus den USA kam, die Antennen von SONIM aus den Niederlanden und die LNB´s von NEC in Japan. Schön überklebt mit dem TechniSat-Logo. Wie auch immer, ohne die Initiative von Peter Lepper hätte die Akzeptanz des Satelliten-Empfangs in Deutschland doch wesentlich länger gedauert.

Die TechniSat-Leute fuhren von TV-Fachhändler zu TV-Fachhändler in einem rollenden Empfangsstudio und brachten so den ziemlich unbedarften Fachhändlern die „Satollogie“ bei.

Die Freaks waren weniger interessiert. Ihre Marken für den DX-Empfang waren Chaparral und Echostar. Die Amerikaner kannten den europäischen Markt und die Wünsche der Käufer noch nicht so gut und so arbeitete der Autor bei der Entwicklung des Echostar SR 5500 mit.

1989, 1990 und 1992 gingen die deutschen Satelliten KOPERNIKUS in den Orbit und erleichterten den Empfang europäischer Sender erheblich.

Eine 90cm-Antenne war ausreichend. Allerdings machten technische Probleme und die Aktivierung des ersten ASTRA-Satelliten 1989 den Betreibern das Leben schwer.

Immerhin waren nun nur noch 60cm-Antennen nötig und es zeichneten sich Kampfpreise bei den ASTRA Empfangsanlagen ab. Übrigens, auch Dr.Dish TV nutzte zwischen 1995 und 1998 den KOPERNIKUS-Satelliten.

Nach dem Start des dritten auf 19,2° Ost parallel positionierten Astra-Satelliten, der am 12. Mai 1993 erfolgte, war der Kampf um den deutschsprachigen Satellitenhimmel

entschieden, und fand mit dem Aufschalten von ARD und ZDF am 27. August 1993 auf das Astra-Satellitensystem ihren Abschluss und KOPERNKUS geriet in Vergessenheit.

Mit ASTRA war auch die Zeit der drehbaren Antennen vorbei. Man hatte alles was man brauchte auf einem Satelliten. Und wer noch den HOTBIRD benötigte mit seinen fremdsprachlichen Programmen, der montierte eine schielende Lösung auf die LNB-Schiene.

Bis etwa 2010 stiegen die Umsätze bei den Set Top Boxen regelmäßig an und hielten sich auf diesem Niveau bis etwa 2014. Linux-Boxen waren bis dahin Mauerblümchen, deren Umgang nur von Spezialisten bewältigt werden konnte. Doch nun kamen die Enigma 2 Images wie Open ATV und erleichterten den Umgang mit den Boxen erheblich.

Jetzt war nicht nur der reine lineare Empfang von Satelliten-Sendern möglich, sondern bei Anbindung an das Internet gab es plötzlich ungeahnte Möglichkeiten, wie z.B. das berühmte Medienportal, das den Zugriff auf unzählige Mediatheken und Streaming-Angebote erlaubte.

Der Absatz von herkömmlichen Set Top Boxen ging deutlich zurück und immer mehr Hersteller und so mit auch Händler gaben auf.

WIE GEHT ES WEITER?

Das Sehverhalten der Zuschauer hat sich deutlich verändert. Die junge Generation setzt auf Youtube mit kurzen Inhalten und auf die sozialen Netzwerke. Die Generation der 25- bis 49 Jährigen wendete sich mehr und mehr den Streamingdiensten wie Netflix und Amazon Prime zu. Das Diktat der 20:00 Uhr Nachrichten ist vorbei, da sie zeitversetzt aus der Mediathek abgerufen werden.

Natürlich wird es Leute geben, die das lineare Fernsehen bevorzugen oder bevorzugen müssen, da sie in der Fläche mit keiner oder schlechter Internetanbindung leben. Für andere kommt das Internet überhaupt nicht in Frage, da sie fürchten ausspioniert zu werden. Doch die Vorfahren dieser Leute haben vielleicht auch schon das Telefon als Teufelszeug angesehen.

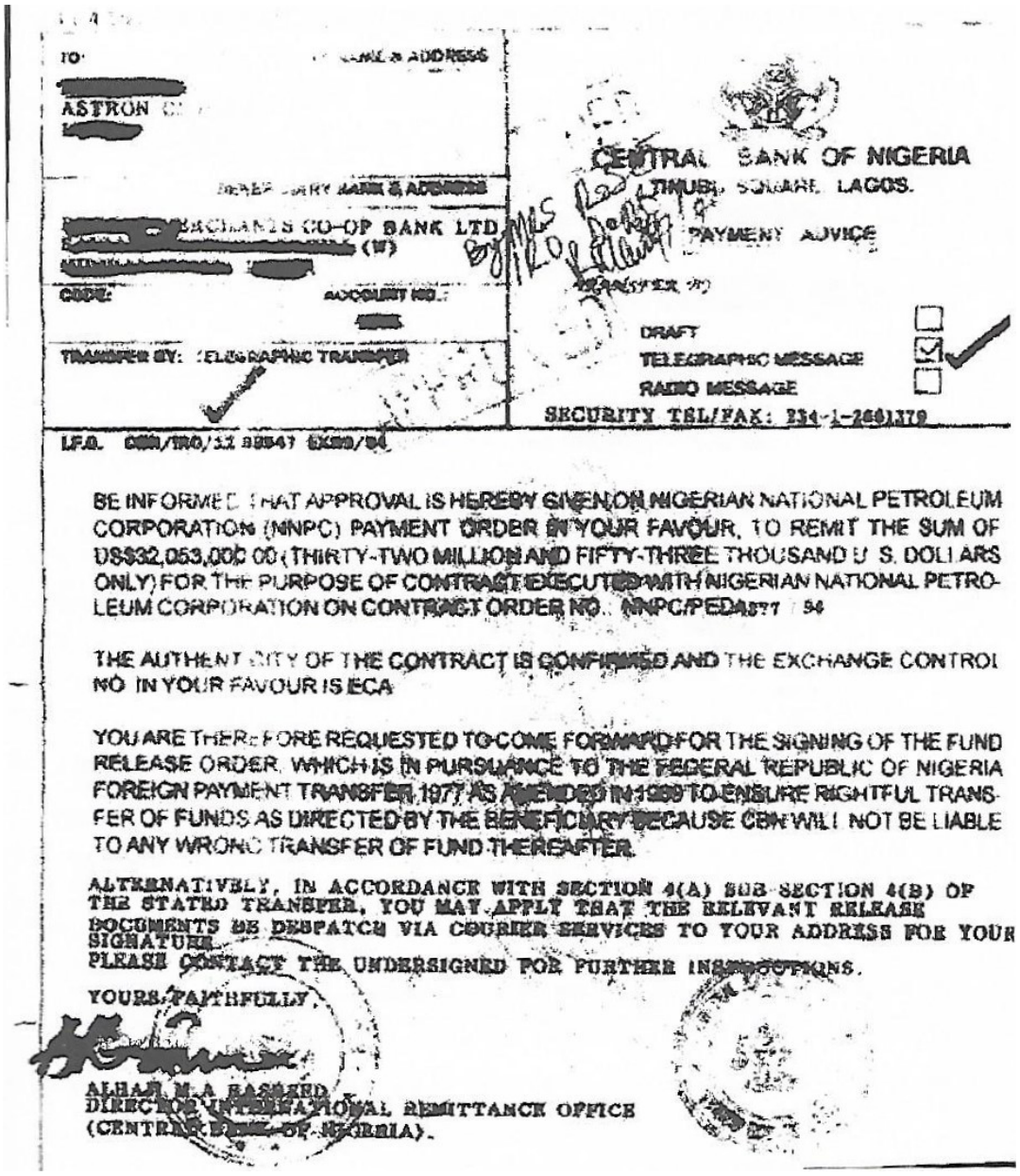
Wir werden uns alle den neuen Herausforderungen stellen müssen. Und zwar vom Hersteller bis zum Endverbraucher hin. Extrem hohe Transponderkosten auf den Satelliten und immer bessere Internetanbindungen werden irgendwann auch die öffentlich rechtlichen TV-Sender nachdenklich machen.

Was bleibt, und da bin ich mir sicher, sind die Freaks. Sie werden auch weiterhin Satellit für Satellit abklappern, um neues zu entdecken. Dass man das nicht freie DVB T2 Freenet auch wirklich frei über Satellit empfangen kann, ist schließlich eine Entdeckung der Satelliten Dxer.

D.D.

NOSTALGIE

VOR 21 JAHREN



TO: [redacted]
ASTRON [redacted]

[redacted] BENIN'S CO-OP BANK LTD [redacted]
CODE: ACCOUNT NO.: [redacted]
TRANSFER BY: TELEGRAPHIC TRANSFER

CENTRAL BANK OF NIGERIA
TINUBU SQUARE LAGOS.
PAYMENT ADVICE
DRAFT
TELEGRAPHIC MESSAGE
RADIO MESSAGE
SECURITY TEL/FAX: 234-1-2661379

L.F.O. CBN/IRO/12 88547 EXCD/94

BE INFORMED THAT APPROVAL IS HEREBY GIVEN ON NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC) PAYMENT ORDER IN YOUR FAVOUR, TO REMIT THE SUM OF US$32,053,000 00 (THIRTY-TWO MILLION AND FIFTY-THREE THOUSAND U S. DOLLARS ONLY) FOR THE PURPOSE OF CONTRACT EXECUTED WITH NIGERIAN NATIONAL PETROLEUM CORPORATION ON CONTRACT ORDER NO. NNPC/PEDA/77 94

THE AUTHENTICITY OF THE CONTRACT IS CONFIRMED AND THE EXCHANGE CONTROL NO IN YOUR FAVOUR IS ECA

YOU ARE THEREFORE REQUESTED TO COME FORWARD FOR THE SIGNING OF THE FUND RELEASE ORDER, WHICH IS IN PURSUANCE TO THE FEDERAL REPUBLIC OF NIGERIA FOREIGN PAYMENT TRANSFER 1977 AS AMENDED IN 1999 TO ENSURE RIGHTFUL TRANSFER OF FUNDS AS DIRECTED BY THE BENEFICIARY BECAUSE CBN WILL NOT BE LIABLE TO ANY WRONG TRANSFER OF FUND THEREAFTER.

ALTERNATIVELY, IN ACCORDANCE WITH SECTION 4(A) SUB SECTION 4(B) OF THE STATED TRANSFER, YOU MAY APPLY THAT THE RELEVANT RELEASE DOCUMENTS BE DESPATCH VIA COURIER SERVICES TO YOUR ADDRESS FOR YOUR SIGNATURE.
PLEASE CONTACT THE UNDERSIGNED FOR FURTHER INSTRUCTIONS.

YOURS FAITHFULLY,

ALHAJI M.A RASHEED
DIRECTOR INTERNATIONAL REMITTANCE OFFICE
(CENTRAL BANK OF NIGERIA).

ANGEBLICHE ÜBERWEISUNG AUS NIGERIA

Ende 1998 erschien diese Story in der Fachzeitschrift „Tele-Satellit“ und sorgte für Nervosität bei den Tätern und brachte dem Autor eine Morddrohung ein.

NIGERIA CONNECTION

Im wohlverdienten Urlaub auf Redaktionskosten im firmeneigenen Iglu an der herrlichen Nordküste Grönlands erreichte mich die Kunde, dass sich nach relativ langer Ruhe die Scam-Mafia aus Nigeria wieder melden würde. Vor einigen Jahren in Teil neun dieser Serie wurde über die Machenschaften berichtet, und eigentlich bestand auch kein Grund mehr, sich darum zu kümmern, denn Staatschef Sani Abacha von Shells Gnaden war verschwunden, und nach fast demokratischen Wahlen war der zivile Machthaber Olusegua Obasanjo am Steuer. Und der hatte gleich versprochen, mit den Scam-Letter Betrügern und korrupten Beamten abzurechnen. Wie das mit „abrechnen" gemeint sein mag, wissen wir nicht. Fest steht jedoch, dass nach einer Schrecksekunde die alten Figuren – teilweise unter anderen Namen – wieder ihr Unwesen treiben.

Vorgesehen hatte ich eigentlich einen ersten Erfahrungsbericht mit dem neuen Ikonos-Satelliten der Space-Imaging Group. TSI berichtete als erste Fachzeitschrift weltweit bereits ausführlich über das Projekt, kommerzielle Fotos mit einer Auflösung von einem Meter anzubieten, und als Dank bekommt die TSI-Redaktion auch die ersten Bilder des Satelliten. Auch die eigene Empfangsanlage ist inzwischen fertiggestellt und wartet eigentlich nur auf die ersten Signale. Leider befand sich der Satellit zum Redaktionsschluss noch in seiner 90-Tage Testphase. Alles hatte sich im Lauf der Jahre verzögert. Einsprüche diverser Geheimdienste (vor allen Dingen aus Israel) und der verunglückte Start von Ikonos-I waren der Grund. Die Auflösung der Fotos könnte heute schon leicht unterhalb der Im-Grenze liegen, doch hier sprach die National Security Agency (NSA) in den USA ein Machtwort. Nicht ganz von sich aus, auch hier drückten die Israelis von hinten. So müssen sich die polizeilichen Organisationen, die sich mit Mord und Tot- schlag beschäftigen, noch etwas gedulden, um endlich Fotos in hoher Auflösung einer bestimmten geographischen Zone und von einem bestimmten Zeitpunkt zu bekommen.

Nur so lässt sich eventuell feststellen, ob zu einem Tatzeitpunkt z.B. ein Auto an einem Waldrand geparkt wurde und wie es denn ungefähr aussehen könnte. Immerhin lässt sich mit dem IKONOS schon mal die Farbe und die Größe bestimmen. Nach meinem Vorschlag und nach einem konkreten Fall lief ein süddeutsches LKA in die geheimdienstliche Sackgasse. Aus Sicherheitsgründen wollte man nicht helfen, obwohl die Keyhole-Satelliten der Amerikaner hier Hilfe leisten könnten, ohne ihr Gesicht zu verlieren.

SCAM-MAFIA

In den letzten 15 Jahren hat sich unter verschiedenen Regierungen – von denen nicht nur geduldet – die Nigeria-Connection etabliert. Unter verschiedenen Absendern versehen mit falschen Briefköpfen irgendwelcher Ministerien – werden an (vermeintlich) wohlbetuchte Amerikaner und Europäer brandeilige Briefe, Faxe und neuerdings auch E-Mails geschickt. Darin („Privat/Confidential") wird dem Empfänger ein kleines Millionen-Geschäft vorgeschlagen. Ein Betrag (z.B. 20 Millionen US-Dollar) muss angeblich außer Landes geschafft werden. Der Grund könnten überschüssige Einnahmen aus dubiosen Ölgeschäften sein, die gewaschen werden müssen, oder in letzter Zeit angesammelte Gelder von Ministern, die sich im Ausland nach der Machtübernahme durch Zivilisten eine neue Existenz aufbauen wollen. Dazu benötigt man dringend ein unverfängliches Auslandskonto, und das sollte partout das des Briefempfängers ein. Man möge doch alle Bankverbindungen bekanntgeben, damit die 20 Millionen US Dollar überwiesen werden können.

Als kleine Anerkennung für die geleisteten Dienste dürfe der Empfänger auch gleich 20% (4 Millionen Dollar) für sich abzweigen. Nur schnell muss alles gehen, und ein Rückruf noch heute wäre äußerst wichtig. Wer dumm und geldgierig genug ist, fällt darauf rein. Eine Kontonummer ist schließlich kein Geheimnis, und die kann man ja mal mitteilen. Sollte diese Kontonummer erkennbar ein verstecktes Konto in Liechtenstein, der Schweiz oder auf den Antillen sein, wird es ernst. Sollte unser Mr. Raffgier die Restfunktionen seiner kleinen Walnuss im Kopf abgeschaltet haben und auch noch das Passwort seines Kontos nennen, kann er die Sache eigentlich gleich vergessen. Der nächste Kontoauszug wird einen Saldo von 0,00 ausweisen.

Der Besitzer eines „anständigen" Kontos erhält ein tolles Transfer-Schreiben der Bank of Nigeria, in dem man ihm mitteilt, dass der erwartete Betrag zur Überweisung ansteht, jedoch noch einige Formalitäten nötig seien. Unter anderem stehen noch die Transfer-Kosten in Höhe von 1% der Summe (200.000 US-Dollar) aus. Der Auftraggeber sei bereit, die Hälfte davon selbst zu übernehmen, die andere Hälfte sollte jedoch schnellstens überwiesen werden. Reagiert der Empfänger zögerlich, so wird er mit tollen Schreiben und einigen kleinen Zusatzforderungen in Atem gehalten, bis ihm derselbe ausgeht. Unsere Scam-Letter Mafia hat ihr Ziel erreicht und ist von nun an nicht mehr erreichbar.

ERSTES ANGEBOT AUS NIGERIA

TIN: [redacted]

Subject: ATTN: [redacted]
Date: Thu, 2 Sep 1999 03:06:57 -0700 (PDT)
From: STEPHEN HOZANE <hozanests@yahoo.com>
To: [redacted]

NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC) FALOMO IKOYI, I.AGOS.

ROM: DESK OF: STEPHEN HOZANB (DR) .
E-MAIL: HOZANESTS@YAEOO.COM

ATTN: [redacted]

DEAR STR,

CONFIDENTIAL BUSINESS PROPOSAL

1 AM DIRECTOR OF NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC) WE ARE MAKING THIS CONTRACT WITH YOU BECAUSE OF THE RELIABLE INFORMATION. WE GATHERED FROM THE NIGERIAN CHAMBERS O? COMMERCE AND INDUSTRY HIGHLIGHTING YOUR COMPANY'S PROFIL. THE INEOPETION IS SO POSITIVE AS TO CONVINCE US THAT YOU WOULD BE CAPABLE OF PROVIDING US WITH SOLUTION TO A MONEY TRANSFER TRANSACTION OF SIXTY—FIVE MILLION, FIVE HUNDRED THOUSAND UNTIED STATES DOLLARS ONLY (US$65.5M) .

WE ARE EMBERS OF THE SPECIAL COMMITTEE FOR BUDGETS AND PLANNING cp THE MINISTRY OF THIS COi011TTEE IS PRINCIPALLY CONCERNED WITH CONTRACT APPRAISALS THE APPROVAL 0? CONTRACTS IN ORDER 0? PRIORITIES AS REGARDS CAPITAL PROCECTS OF THE MILITARY GOVERNI.ENQ O? NIGERIA. WITH OUR POSITIONS, WE EAVE SUCCESSFUL SECURED FOR OURSELVES TEE SUM OF MILLION, ?IVE HUNDRED THOUSAND UNITED STATES DOLLARS ONLY (US$65.5M) THIS AMOUNT WAS ACCUMU%ATED THROUGH UNDECLARED FROM SALES 0? CRUDE DURING THE GULF WAR.

In Folge neun dieser Serie bewiesen wir, dass es selbst mit verhältnismäßig einfachen Mitteln und etwas Sachkenntnis möglich ist, den Telefon/Fax- Verkehr dieser Gangster via Satellit mitzuhören und zu lesen. Den Autor erreichten nach Veröffentlichung einige nette Einladungen nach Nigeria, die er allerdings dankend ablehnte.

LAUSCHANGRIFF II

Nach entsprechenden Hinweisen auf neue Aktivitäten wurde das alte Equipment wieder aktiviert. Inzwischen funktionierte auch das provisorische Fax-Modem etwas besser. Zumindest waren die Texte zu 80% lesbar. Da ein überwiegender Teil internationaler Telekommunikation über die diversen Intelsats läuft, war es erst einmal wichtig, den richtigen Satelliten zu finden. Vor einigen Jahren war es die Position 60° Ost. Hier wird inzwischen ein Hemi-Beam eingesetzt, und der ist leider in den nördlicheren Gefilden nicht empfangbar.
Auf Nachfrage stellte sich auch schnell heraus, dass die 60,0-Position zwar noch von der Bodenstation Lanlate I genutzt wird, doch überwiegend im innerafrikanischen Verkehr.
Die nächsten Tage verzog ich mit allen Antennen-Listings auf den Dachboden und kam erst nach diversen Drohungen seitens der Familie und des Verlegers mit Spinnweben zwischen den Armen wieder runter. Immerhin mit einigem Erfolg. Es mussten die Positionen 27 und 24,5 0 West sein. Die restlichen Infos kamen von lieben Menschen auf der IBC99, die als Belohnung die der Presse zustehenden Verzehrbons bekamen.

Es klappte auf Anhieb. Lanlate-2 (LAN-02a) bedient mit FDM 24,5 0 West im C-Band und Lagos-4 (LAG-04B) versorgt 27,5 0 West mit analogem SCPC. FDM wird für Telefonie, Fax und Data von Telekommunikations-Organisationen genutzt; SCPC sehr oft von Sicherheitsdiensten, Hilfsorganisationen, Ölgesellschaften und wesentlich zweifelhafteren Diensten. Der FDM-Verkehr ist mit recht einfachen Mitteln zu verfolgen. Man nehme einen etwas größeren Spiegel für das C-Band (Minimum: 180cm), einen analogen Low-Threshold-Receiver und einen erstklassigen SSB-Radio-Empfänger, der den Fre-

quenzbereich bis etwa zehn MHz überstreicht (NRD; ICOM, AOR oder militärische Surplus-Geräte). Der Baseband-Videoausgang des Sat-Receivers wird über Koaxialkabel auf dem kürzesten Weg mit dem Antenneneingang des Kurzwellen-Receivers verbunden. Im C-Band wird auf betimmten Satelliten, die FDM transportieren, nach Transpondern gesucht, die sich durch dunkle Störungen auf dem Kontrollmonitor bemerkbar machen. Dieses „Störsignal" ist nichts anderes als FDM. Der Empfang wird der Low-Threshold-Funktion optimiert. Firmen-Bierzelt für

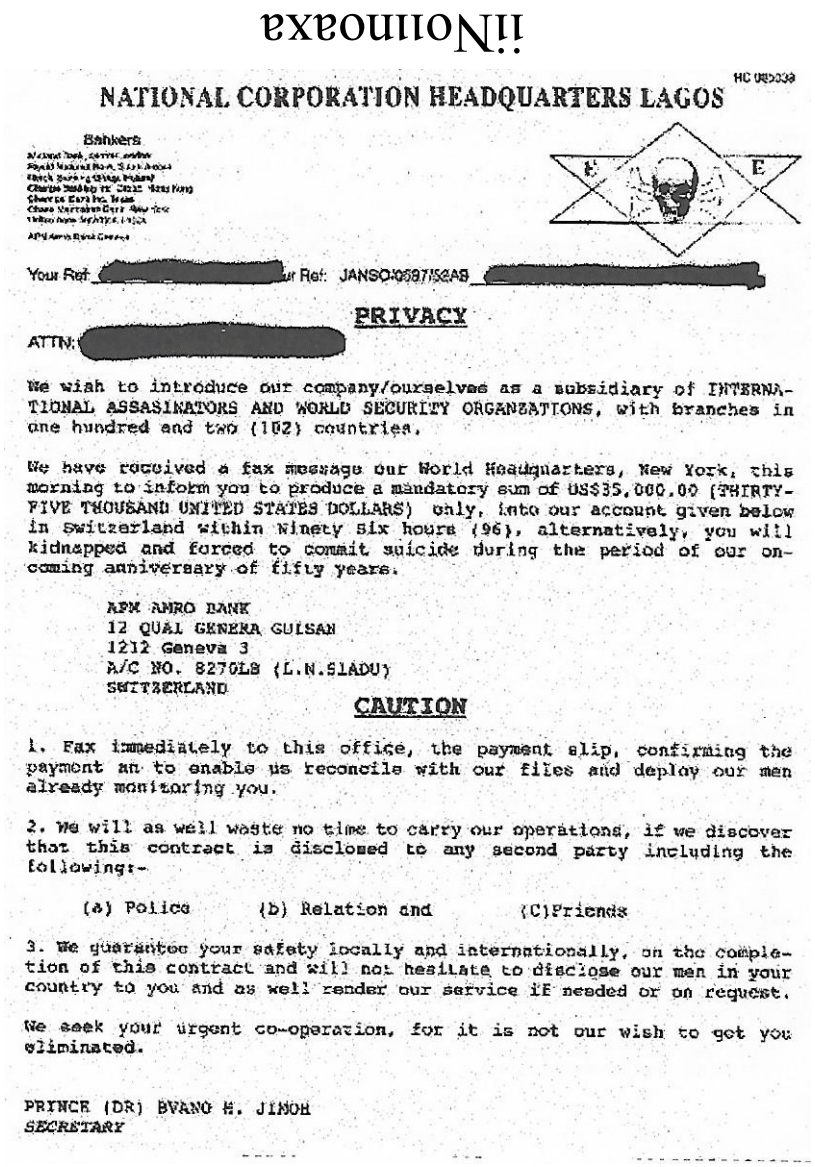
Nun wird der nachgeschaltete KW-Receiver im Bereich von 0 bis ca. 4MHz sehr vorsichtig in USB und LSB (oberes und unteres Seitenband in SSB- Modus) durchsucht. Theoretisch gibt es alle 4kHz einen Kanal. Eine reine Lern- und Nervensache ist es nun, diese Radiosignale einer bestimmten geografischen Gegend zuzuweisen. Ein Receiver mit eingebautem DTMFModul (z.B. AR5000) kann die gewählten Telefonnummern mitlesen und vereinfacht die Suche natürlich. Nigeria hat den Landescode 234, und so filtert man nur diese Telefonate und Faxe
aus.

Bitte nicht nachmachen, denn das ist in den meisten Ländern verboten und geschah auch in unserem Fall rein experimentell. Dies ist wiederum am Standort unserer Monitoranlage erlaubt.

Die nächsten Wochen konzentrierte ich mich auf 24,5° West und vergaß meine Kollegen, die sich auf Einladung des Verlegers mit mitgebrachtem Firmen-Bierzelt für zehn Personen und Bier aus dem lokalen Supermarkt auf dem Münchner Oktoberfest vergnügten. Und das alles auf Verlegerkosten.

Doch es lohnte sich. Da waren sie wieder. Der gesamte Bello-Clan führte weltweite Gespräche (die Nummer 1-49709215 gibt es immer noch), und immer noch scheint Ralph Chukwuma (Tel. 1-234-5891200) der große Pate zu sein. Ziemlich oft konnte das Unwesen eines Dr. Dele Ibrahim (I5451940 und Fax 1-2881474) verfolgt werden. Dummerweise gab er einem „Kunden" in Österreich seine E-Mail Adresse (deleibrahim@yahoo.co.uk) bekannt, und da mir der Ösi leid tat (er war fast weichgekocht), ließ ich zumindest die E-Mail Adresse sperren. Yahoo reagiert da recht schnell. Unglaublich, aber wahr: genau zu dieser Zeit erreichte einen Mitarbeiter der TSI-Redaktion und mich ein gleichlautendes Angebot eines 65-Millionen Dollar-Deals eines gewissen Dr. Stephen Hozane. Einmal stellte er sich vor als Direktor der National Petroleum Corporation (NNPC) in Lagos, und bei mir als „Top Official from the Federal Ministry of Works and Housing" in Abuja.

DER AUTOR IST AUFGEFLOGEN - MORDDROHUNG



NATIONAL CORPORATION HEADQUARTERS LAGOS

Bankers

Your Ref: [redacted] Our Ref: JANSO/0597/S2AS [redacted]

PRIVACY

ATTN: [redacted]

We wish to introduce our company/ourselves as a subsidiary of INTERNATIONAL ASSASINATORS AND WORLD SECURITY ORGANZATIONS, with branches in one hundred and two (102) countries.

We have received a fax message our World Headquarters, New York, this morning to inform you to produce a mandatory sum of US$35,000.00 (THIRTY-FIVE THOUSAND UNITED STATES DOLLARS) only, into our account given below in Switzerland within Ninety Six hours (96), alternatively, you will kidnapped and forced to commit suicide during the period of our oncoming anniversary of fifty years.

APM AMRO BANK
12 QUAL GENERA GUISAN
1212 Geneva 3
A/C NO. 8270LS (L.N.SIADU)
SWITZERLAND

CAUTION

1. Fax immediately to this office, the payment slip, confirming the payment an to enable us reconcile with our files and deploy our men already monitoring you.

2. We will as well waste no time to carry our operations, if we discover that this contract is disclosed to any second party including the following:-

(a) Police (b) Relation and (C)Friends

3. We guarantee your safety locally and internationally, on the completion of this contract and will not hesitate to disclose our men in your country to you and as well render our service if needed or on request.

We seek your urgent co-operation, for it is not our wish to get you eliminated.

PRINCE (DR) BVANO H. JINOH
SECRETARY

Er wurde als mein Opfer ausgewählt. Zum Schein wurde auf den Deal eingegangen. Er bekam den Namen einer Luxemburger Bank und eine Kontonummer genannt; verbunden mit dem zarten Hinweis, das nötige Passwort gebe es erst, wenn er eine Bankgarantie erbringen würde. Hier gab es was für ihn abzuräumen, und er reagierte schneller als die freiwillige Feuerwehr, die manchmal schon

vor dem Brand da ist. Per Fax kam die Bankgarantie und eine Telefonnummer (1-888830) mit dem Hinweis, dort am folgenden Tag gegen 21:00 UTC anzurufen. Um es gleich vorweg zu sagen, die Nummer gehört zu keinem Ministerium, sondern ist wahrscheinlich eine gemietete Nummer einer Briefkastenanschrift. Das gesamte Empfangsequipment wurde vorbereitet, und ein kundiger Helfer hatte nicht anderes zu tun, als während des Gesprächs am folgenden Tag Dr. Hazane innerhalb eines drei MHz-Bereiches zu finden. Das heißt, ich musste das Gespräch künstlich verlängern (wer bezahlt mir das eigentlich?)

„Dr.Hazane" schilderte nochmals die Eiligkeit des Deals und reizte mich mit schnell verdientem Geld. Ich erklärte ihm interessiert, dies alles würde ganz gut passen, denn eine Geschäftsreise würde mich folgende Woche eh nach Abuja führen. Da ich auf Einladung einer Organisation dort sei, könnte ich keine Angaben zum Hotel machen, doch die echten Daten des Fluges Frankfurt/Main-Lagos-Abuja bekam er von mir.

Die Gier nach meinem Geld (und ich habe tatsächlich ein Budget für so etwas. Allerdings in Lire, und davon sind es immerhin 500.000) ließ ihn ein wenig leichtsinnig werden, und so verriet er mir seine Anschrift in Abuja:

Sekou Tour, Crescent/Ecke Ecowas Road (Hausnummern hat man nicht)

Bis hierher wollte ich gehen, denn dies ist in letzter Zeit der kritische Punkt. Wer nämlich abbricht, bekommt eine Mahnung zur Zahlung der angelaufenen Kosten, und die werden dann schon mal mit US$50.000 beziffert. Sollte man nicht zahlen und auch nicht auf den Deal eingehen, gibt es seit etwa in einem Jahr eine Mahnung der besonderen Art, und die kann besonders schädlich für herzkranke oder sensible Menschen sein. Unter dem Absender der „National Assasination and World Security Organization" wird um Begleichung der „Schuld" gebeten, und zwar innerhalb von 96 Stunden. Falls nicht bezahlt wird, sieht man sich zu folgenden Maßnahmen (im Auftrage des Kunden) gezwungen:

, Anderenfalls werden Sie entführt und zum Selbstmord gezwungen. ... Faxen Sie unserem Büro umgehend eine Bestätigung Ihrer Zahlung, oder wir werden den Vorgang abschließen und unsere Männer schicken, die Sie bereits beobachten. Wir werden außerdem nicht zögern, unsere Operation auszuführen, sollten wir herausfinden, dass dieser Vertrag anderen zur Kenntnis gebracht wird; einschließlich Polizei, Verwandte und Freunde."

In der Vergangenheit wurde als Konto die Nummer 8270LB (L.N.SLADU bei der AMRO-Bank in 1212 Genf) angegeben, doch scheint man inzwischen auf eine Offshore-Bank ausgewichen zu sein. Unterschrieben wird der nette Brief durch einen Prince Bvano H. Jimor.

Zumindest hatten wir während des Telefonats das Frequenzsegment für Gespräche Nigeria-Europa ausfindig machen können. In den folgenden Wochen war unser Dr. Stephen Hozane ein recht williges und informatives Opfer. Zwei seiner Klienten konnten frühzeitig gewarnt werden, und auch die „419-Coalition" (eine private Organisation, die seit Jahren die Umtriebe der Scam-Mafia beobachtet und wichtige Details an das FBI und andere Dienste weiterleitet) wurde mit ausreichend Material gefüttert.

So ganz scheint es Nigerias Staatschef Obasanjo nicht ernst zu sein mit seiner Säuberungsaktion im eigenen Haus.

Mehrfach gaben Hozane und andere Mitglieder des Bello-Clans eine Telefonnummer an, unter der sie momentan zu erreichen seien: +234392344107. Sie gehört zum Informationsministerium des Landes.

NACHTRAG

Die in dieser Geschichte beschriebenen Abhörmethoden waren legal, da die Technik in den Niederlanden benutzt wurde und nach geltendem Recht nicht gegen Gesetzt verstoßen wurde.

Diese und andere Stories erscheinen als Serie in der Fachzeitschrift „Tele-Satellit" und zum Teil später in den Büchern des Autors. Leider sind nicht mehr alle Teile der Serie erhalten, da der Verleger aus dem mageren Online-Archiv alle Spionage-Stories des Autors entfernt hat. Die Berichte erregten teilweise Aufsehen und wurden teilweise in der EU in Brüssel („Das Echelon-System) und im US-Congress („Nigeria Connection" und „Fax-Interception via Satellite") diskutiert.

NOSTALGIE

VOR 23 JAHREN

14. Oktober 1997

„Free to Air TV“ statt Pay TV:

Sendung von Satellitenfreaks

Usingen (AP) - Mitten im Wald trifft sich am Freitag abend eine kleine Gruppe verschworener Satelliten-freaks und geht auf Sendung: Von der Erdfunkstelle der Deutschen Telekom nahe der Taunus-Kleinstadt Usingen be

richtet „Dr. Dish TV“ über die neuesten Tips für den Satellitenempfang - und verbreitet ganz nebenbei auch eine medienpolitische Botschaft: Freier Empfang von «Free to Air TV“ statt Pay TV bei der Übertragung von Kultur- oder Sportereignissen.

„Ich bin Programmdirektor, Moderator und Putzfrau in einem“, sagt Christian Mass alias „Dr. Dish“. Mit seinen beiden Mitarbeitern Mike Bauernfeind aus Leipzig und Ay Renneberg aus dem niederländischen Schinveld bedient der 54jährige Fachautor ein Hobby, das immer mehr Menschen in seinen Bann zieht. Allein in Deutschland sind mehr als 400.000 Anlagen installiert, die Signale von mehr als einem Satelliten empfangen können. Wer dabei einmal zufällig auf einen exotischen Sender gestoßen ist, will immer wieder etwas Neues empfangen - und das möglichst als erster, wie Bauerfeind erklärt.

Routiniert bauen die drei im Informationszentrum der Erdfunkstelle ihr Sendestudio auf. Aber dann kommt Nervosität auf. Eine Kabelverbindung scheint nicht zu funktionieren. Und die Sprechprobe verläuft auch nicht ganz zufriedenstellend. Aber der Sendebeginn 20.00 Uhr rückt unerbittlich näher, und Mass konzentriert sich auf sein Publikum. „Guten Abend! Da sind wir wieder bei Dr.-Dish-TV. Ich begrüße auch die Zuschauer im Internet, die zum ersten Mal mit dabei

sein können.“ Zwei Telekom-Techniker schicken die Signale ins All, zum Fernmeldesatelliten DFS2 Kopernikus. Dort hat die Telekom für drei Stunden die Frequenz 11.550 Gigahertz zur Verfügung gestellt. „Die Leute von Dr. Dish gehen die Sache mit so viel Idealismus an, daß man dies einfach nur unterstützen kann“, sagt der Telekom-Sprecher in Usingen, Klaus Flössel. Und schließlich stehe die Satellitentechnik ja auch im Zentrum der 35 Kilometer nördlich von Frankfurt am Main gelegenen Erdfunkstelle.

Regelmäßige Video-Beiträge vom Polarkreis

Mit viel Improvisationstalent steuert Mass die Sendung durch aktuelle Nachrichten, Interviews mit Gästen und einem Gewinnspiel sowie Beiträgen von Zuschauern. „Wir haben oben am Polarkreis den Bo Wall, der schickt uns regelmäßig seine Videos“, erklärt Mass. Etwa 120.000 vom Satelliten-Hobby gepackte Zuschauer zwischen Island und Griechenland empfangen das an jedem zweiten Freitag im Monat ausgestrahlte Programm - je weiter die Entfernung, desto größer muß die Schüssel sein. Vor allem aus Ungarn, Rumänien und Tschechien gebe es zahlreiche Rückmeldungen von Zuschauern, sagt Mass. Im Internet ist das Empfangsgebiet global - aber unter der Adresse http://www.sat-soft.com/drdishtv.html gibt es zunächst nur die alle 15 Sekunden aktualisierten Bilder zu sehen.

Die erste Sendung wurde schon Anfang 1994 ausgestrahlt. Den Anstoß gab die Fachzeitschrift „Tele Satellite“, wo Mass unter anderem Hinweise für den Empfang von Satelliten-Signalen von der russischen Raumstation „Mir“ gibt - nicht ohne eine besondere „Warnung: Die hier veröffentlichten Daten dienen rein experimentellen Zwecken. Die nationalen Bestimmungen zum Empfang solcher Signale variieren von Land zu Land, und man sollte sich kundig machen oder emigrieren.“
Von Peter Zschunke

TecTime Magazin direkt ABONNIEREN:

http://tectime-tv.de/magazin-abonnieren/

oder

magazin@tectime.tv

TecTime
Zeit für Technik

Suche ... SUCHE

VIDEOS FÜR ABONNENTEN | ABONNIEREN | FRAGEN AN DR.DISH | VIDEOS | NEWSLETTER | IMPRESSUM | DATENSCHUTZERKLÄRUNG

TecTime Magazin abonnieren

Ihr Name (Pflichtfeld)

Ihre E-Mail-Adresse (Pflichtfeld)

☐ TecTime Magazin abonnieren

BESTELLUNG JETZT ABSENDEN

Preis: 12 Ausgaben für NUR 36 Euro –