

TurlaSat: The Fault in our Stars

Turla's Exquisite Satlink Appropriation



Kurt Baumgartner @k_sec
Principal Security Researcher

Stefan Tenase @stefant
Sr Security Researcher
Kaspersky Lab

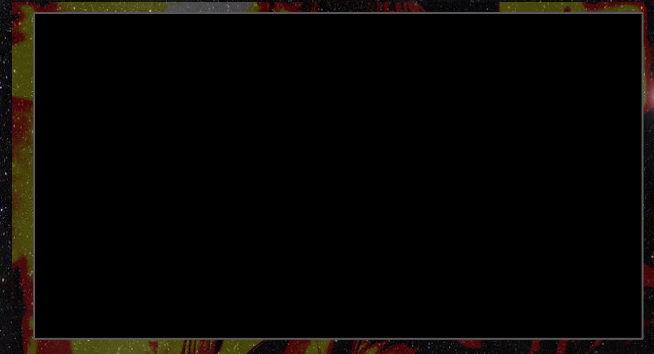
The Ultra3/Turla APT

- Venomous Bear, Turla
- APT Command and Control in the Sky
- Epic Turla(++) Campaigns
- Penguin Turla
- Agent.btz, Chinch, and variants
- Turla/Cobra/Snake/Uroboros/Carbon
- Inspiration from vlad, gilg, urik



Agent.btz Mystery Downloaded Component(s)

- Absence from Threatexpert, F-secure, GData pubs
- worldnews.ath.cx/update/img0008/[rand_num].jpg -> iexplore.\$1F.dll
- simple xor 0x55, c2: euronews.ath.cx
- Ch version 2.14.1 - late 2010
- 83.235.19.125 = Greek satlink comms!
- tapi32d.exe, typecli.exe (Agent.dne?)
 - DE, RU, CN, TO, satcoms



TurlaSat Selectivity, Agent.btz, and Greece

- \$1f.dll finds are very rare
- Caucasus region, Kazakhstan, Far Eastern RU, etc
- But, 10s of thousands agent.btz detections
- Early domains resolved to Greek satlink ip's
 - biznews.ath.cx, intellicast.ath.cx, worldnews.ath.cx, euronews.ath.cx, biznews.podzone.org

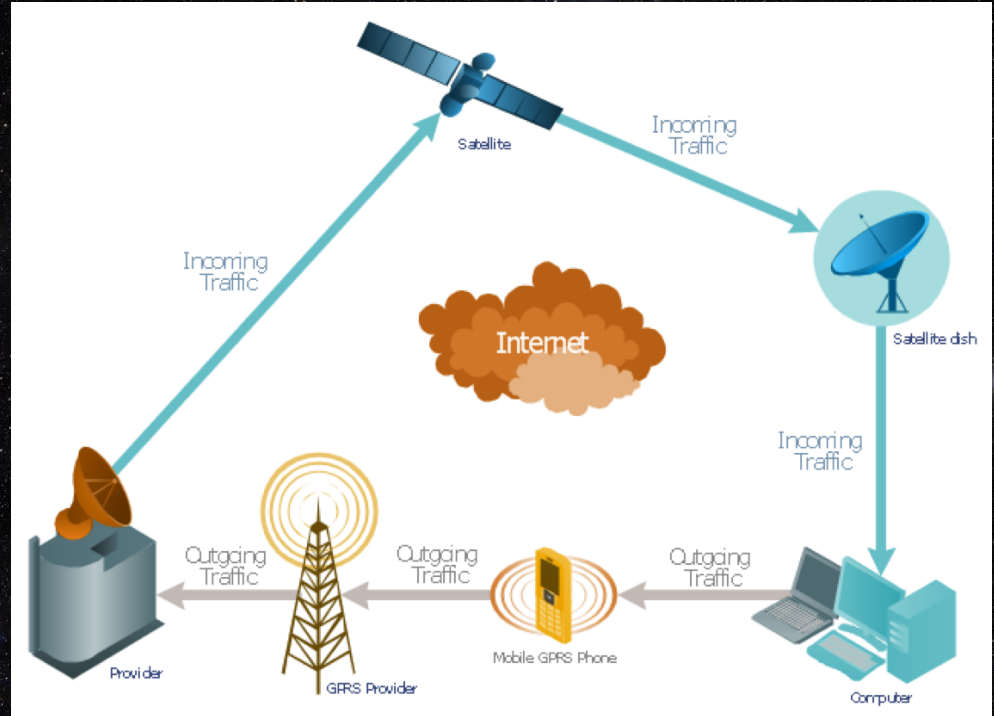


Satlink Hijacks and Listening to the Skies



Ancient One-Way Satellite Internet

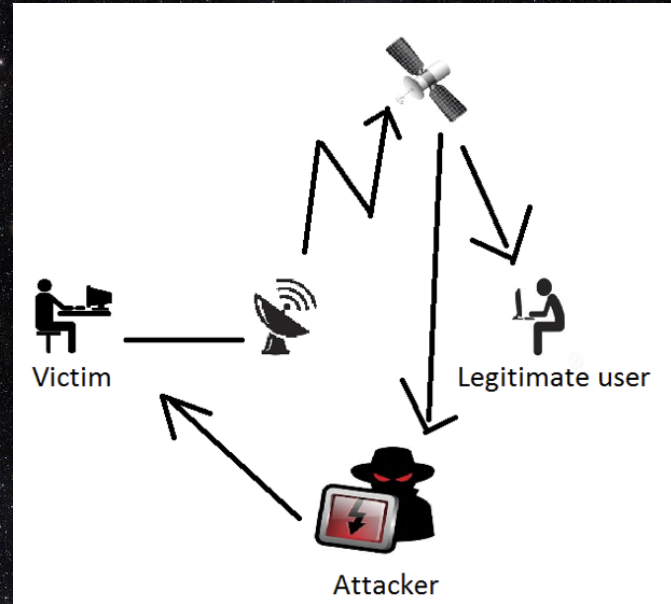
- Used 20 years ago
- Accelerate downloads in areas where fiber/cable is unavailable
- Downstream from satellite (high bandwidth)
- Upstream goes through dial-up or GPRS (low bandwidth)



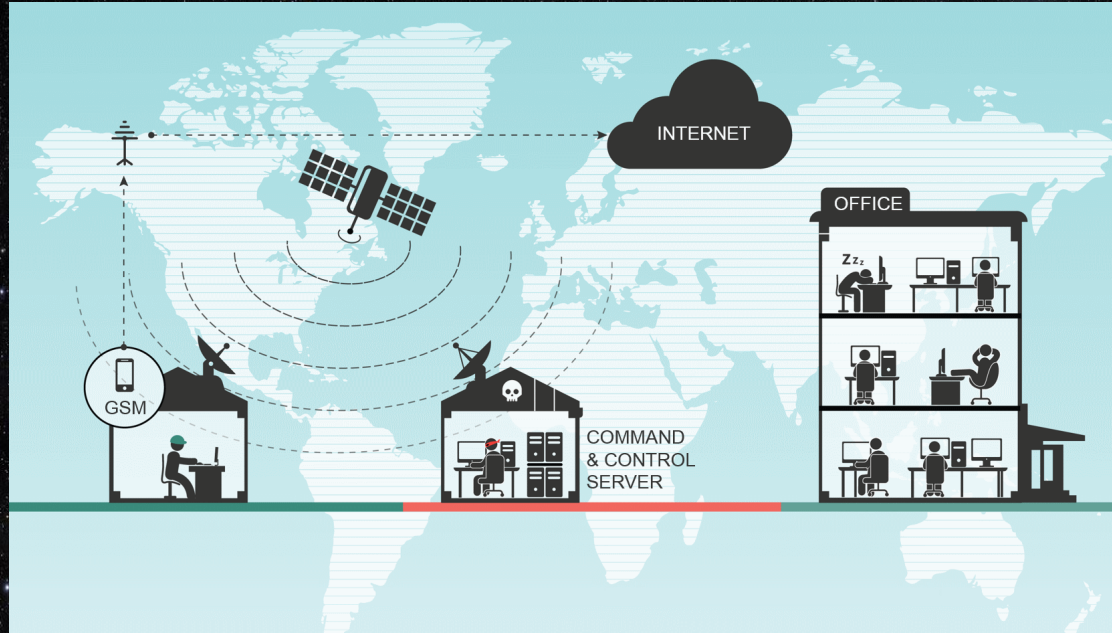
Satellite Internet Hijacking

How does it work?

1. Sniff active IPs
2. Spoof legit ip with c2
3. Non-standard port http comms with c2
4. Hijacked link!!



Satlink Hijack and Listening to the Skies



The Hardware

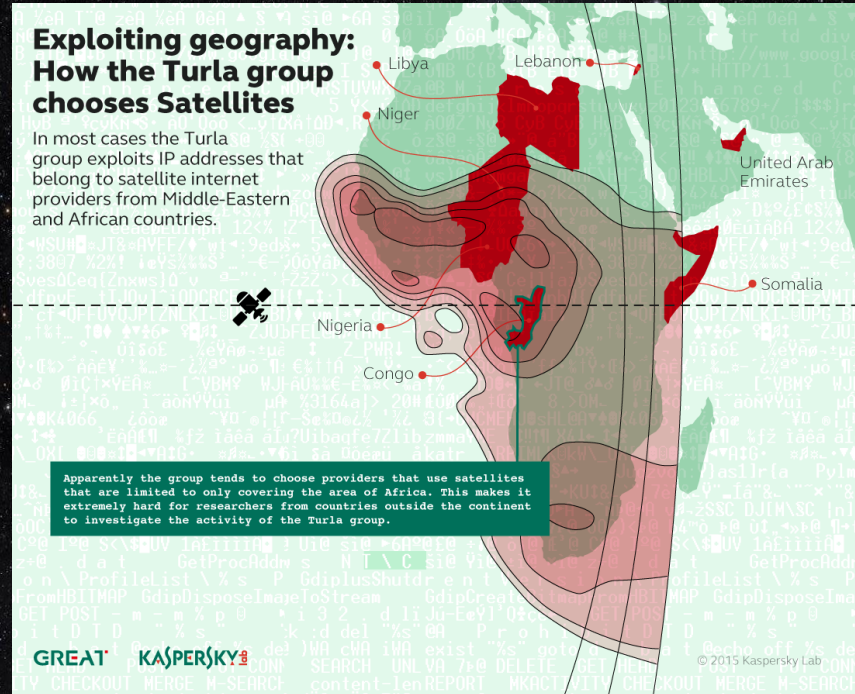
- A satellite dish - size depends on geographical position and satellite
- A low-noise block converter (LNB)
- A dedicated DVB-S PCIe card
- Linux, dvbsnoop, dreambox



Bottom line? ~\$1,000

Why? De-localized. Ultimate Anonymity

- C2 located anywhere here
- Can exceed 1000s kilometers

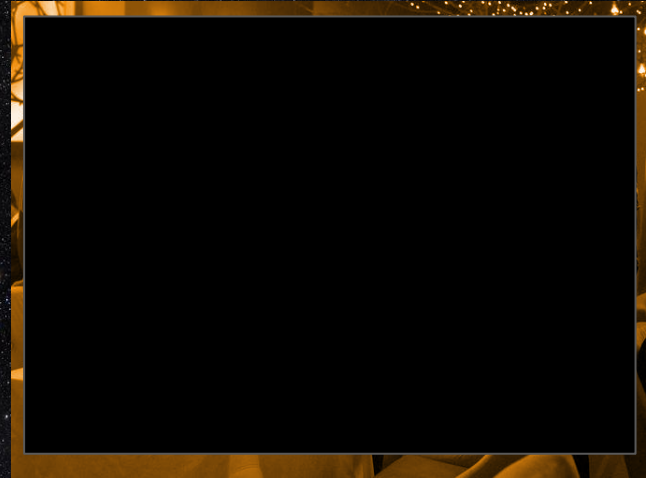


Africa and the Middle East

- Global abuse across satellite IP ranges
- Prefers Middle East and Africa
 - Congo, Togo, Libya, Lebanon, Niger, Nigeria, UAE, Somalia
- Reasons: avoid most security researchers(?) and vulnerable hardware

Turla Components and Satlink Comms

- Agent.btz
- Agent.dne
- Carbon
- Domains, ip's ... 30 - 40
satlink ip resolution, 20 - 30
direct ip comms



Turla-Abused Satellites

- Africa, Middle East, Europe
- Almost one dozen known ISP
- At least 2007 - today
 - Emperion
 - Intrasky Offshore S.A.L.
 - Skylinks Satellite Communications Limited
 - LunaSat ISP
 - SkyVision Global Networks Ltd
 - Teleskies
 - Sky Power International Ltd
 - TTK
 - IABG
 - KBI Hellas, Ote SA...more...

Bonus: Greece, Turla, and Old Cossack Movies

- euronews.ath.cx = 83.235.19.125
 - (July, August 2010 and earlier)
- Ote SA (Hellenic Telecommunications Organisation)
 - owns the greek satellite ip range
- Agent.btz version 2.14.1, compiled in early 2010
 - definitively a Turla C2

Bonus: Greece, Turla, and Old Cossack Movies

The screenshot shows the kinoX.ru website interface. At the top, there's a navigation bar with 'Главная', 'DVD-магазин', 'Форум', 'Чат', 'Реклама', and 'Помощь'. Below this is a search section with filters for 'По жанрам', 'По годам', and 'По компаниям'. A central banner features the title 'Кубанские казаки' and a list of actors. Below the banner is a table of movie details.

Студия	Год	Жанр	Длит.
Мосфильм	1949	Романтическая комедия	

Кубанские казаки
СССР

В ролях [и]: Тамара Говоркова, Клавдия Колленкова (...*поборуга Даша*), Марина Ладынина (...*Галина Пересветова*), Сергей Лукьянов (...*Гордей Ворон*), Владимир Волыгин (...*Антон Петроич Мудрецов*), Юрий Любимов (...*Андрей*), Клара Лукина (...*Даша Шелест*), Владимир Добровен (...*дядя Кузьма*), Борис Андреев (...*Федор Груше*), Михаил Пуговкин (...*колхозник*), Екатерина Савинова (...*Любочка*), Александр Устинов (...*Денис Корень*), Константин Сорокин (...*продавец*), Владлен Давыдов (...*Николай*), Виктор Авадошко, Александра Данилова (...*колхозница*), Владимир Уральский (...*председатель колхоза*), Георгий Савицкий (...*доктор*), Валентина Телегина (...*Христорождина*), Сергей Ефимов (...*Марко Данилович Драгач*), Андрей Петров (...*Вася Тузов*), Елена Савицкая (...*Николаевна*), Елена Болыкина (...*Клавя*), Владимир Петов (...*продавец музыкальных товаров*), Петр Репнин (...*эпизод*), Алексей Бахарь (...*эпизод*), Елизавета Кузурина (...*колхозница*), Клавдия Хабарова.

От представителей современной молодежи, (мне 17) могу сказать, что от фильма *и ПРОСТО В ВОСТОРГЕ*, всетаки как раньше могли снимать кино, но жизнь и вправду не похожа на реальную послевоенную ситуацию России

Автор: [Viktoriya](#)
[02.05.2007, IP 83.235.19.125]


Bonus: Greece, Turla, and Old Cossack Movies

Экзамен греческого языка x

www.russiangreece.gr/forums/index.php/topic,1010.5

Сообщить модератору Залисан

Viktoriya
Местный



Сообщений: 16
Пол: ♀

Re: Экзамен греческого языка!
« Ответ #9 : 12.04.2006, 16:58:15 »

А у меня тут еще один вопрос!
Я сейчас живу в России и заканчиваю школу в этом году, у нас ввели Единый Государственный Экзамен, и его должны сдавать все те, кто в дальнейшем планирует продолжить свое образование в ВУЗе, но я уезжаю в Грецию, чтоб учиться в ВУЗе там! Как мне поступить, обычные экзамены намного легче сдать чем единый гос экзамен, но я боюсь, вдруг Греция тоже теперь будет принимать учеников из России только с результатами Единого гос экзамена, я вся в замешательстве, как мне лучше сдать экзамены... Помогит...


Сообщить модератору Залисан

The examination of the Gr x

www.russiangreece.gr/forums/index.php/topic,1010.5

report to moderator Logged

Viktoriya
Indigenous



Posts: 16
Gender: ♀

Re: Examination of the Greek language!
«Reply # 9: 12-04-2006, 16:58:15»

And I've got one more question!
I now live in Russia and I finish school this year, we introduced a unified state exam, and must pass all those who in the future plans to continue his education at the university, but I'm going to Greece to study at the university there! How do I do, conventional exams much easier to pass than a single state exam, but I'm afraid all of a sudden Greece, too, will now accept students from Russia only with the results of the unified state exam, I'm all confused, I better pass exams ... Help ..

Report to moderator Logged

Bonus: Greece, Turla, and Old Cossack Movies

Old Cossack movies review (CCCP) →

ip address →

Greek satellite link →

Turla c2

More Turla...

<https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/>

<https://securelist.com/blog/research/67962/the-penguin-turla-2/>

<https://securelist.com/analysis/publications/65545/the-epic-turla-operation/>

<https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/>

<http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html>

<http://artemonsecurity.com/urobuos.pdf>

https://www.f-secure.com/v-descs/worm_w32_agent_btz.shtml

<http://www.baesystems.com/en/cybersecurity/feature/the-snake-campaign>

<https://blog.gdatasoftware.com/blog/article/the-urobuos-case-new-sophisticated-rat-identified.html>

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf