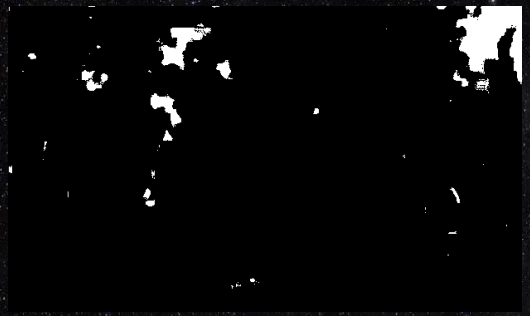
TurlaSat: The Fault in our Stars

Turla's Exquisite Satlink Appropriation

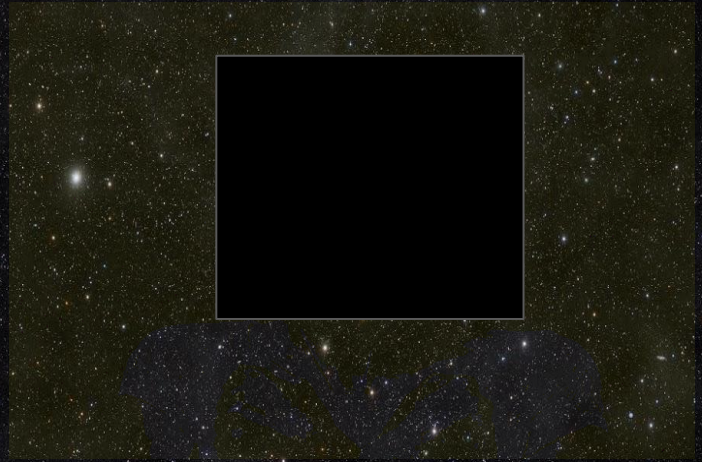


Kurt Baumgartner @k_sec
Principal Security Researcher

Stefan Tenase @stefant
Sr Security Researcher
Kaspersky Lab

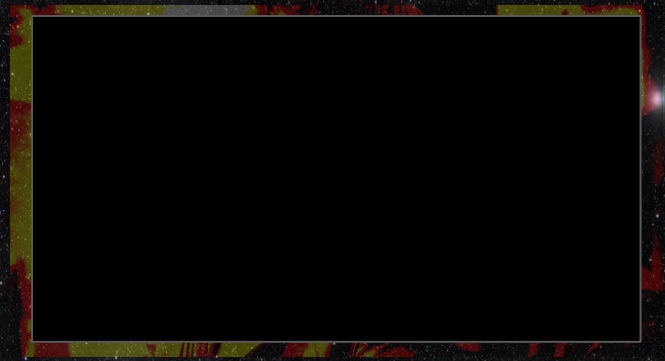
The Ultra3/Turla APT

- Venomous Bear, Turla ….
- APT Command and Control in the Sky
- Epic Turla(++) Campaigns
- Penquin 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



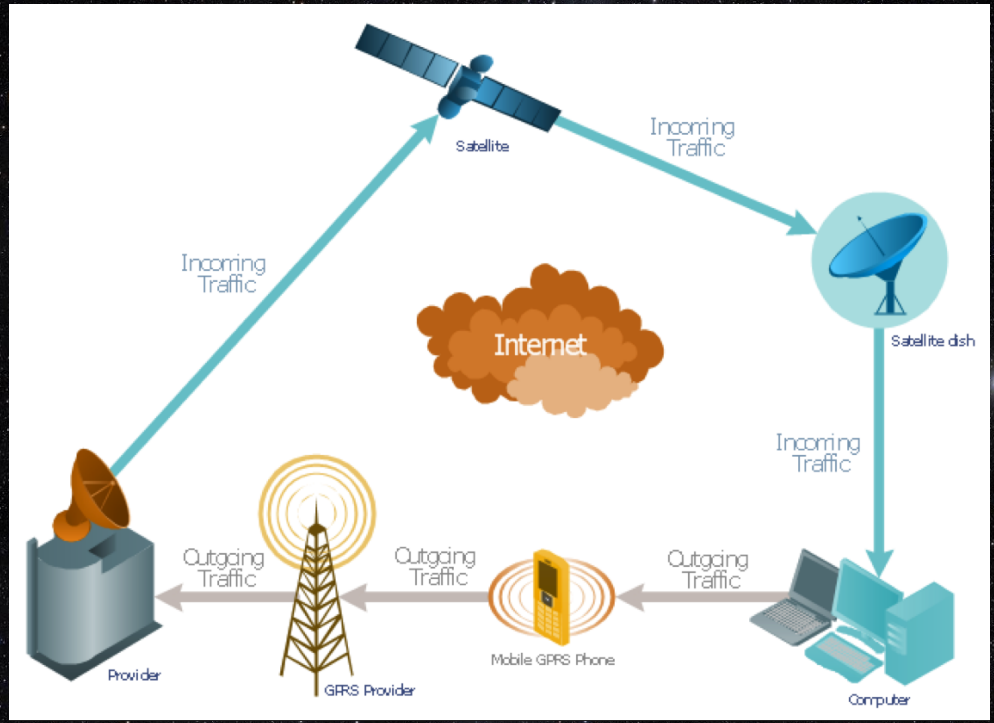
TurlaSat Selectivity, Agent.btz, and Greece

- $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

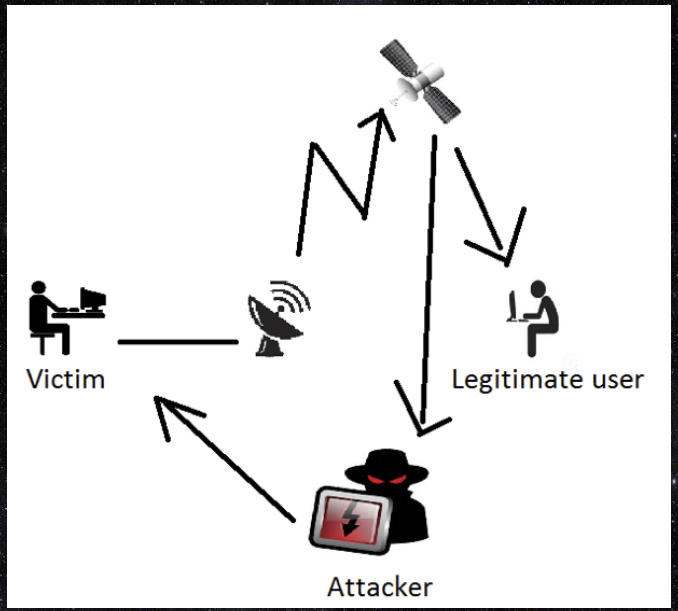
How does it work?

1. Sniff active IPs

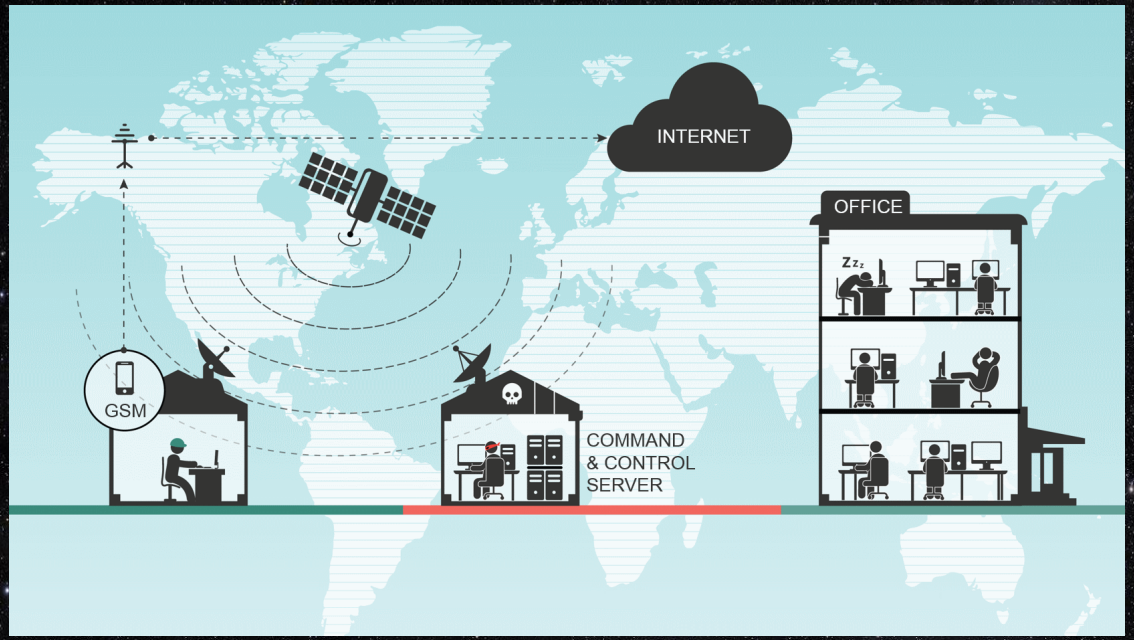
2. Spoof legit ip with c2

3. Non-standard port http comms with c2

4. Hijacked link!!



Satlink Hijack and Listening to the Skies



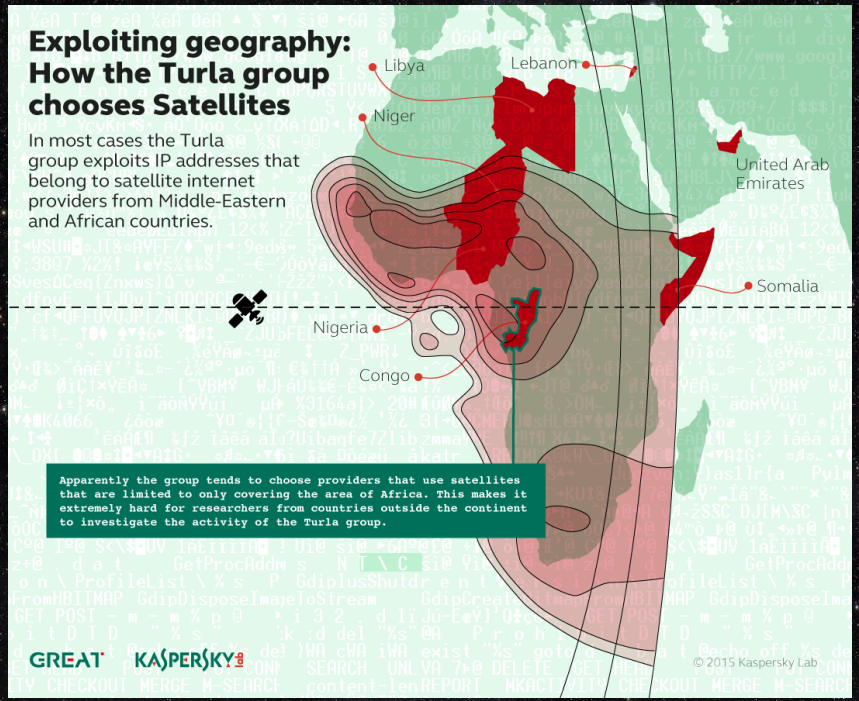
The Hardware

- 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

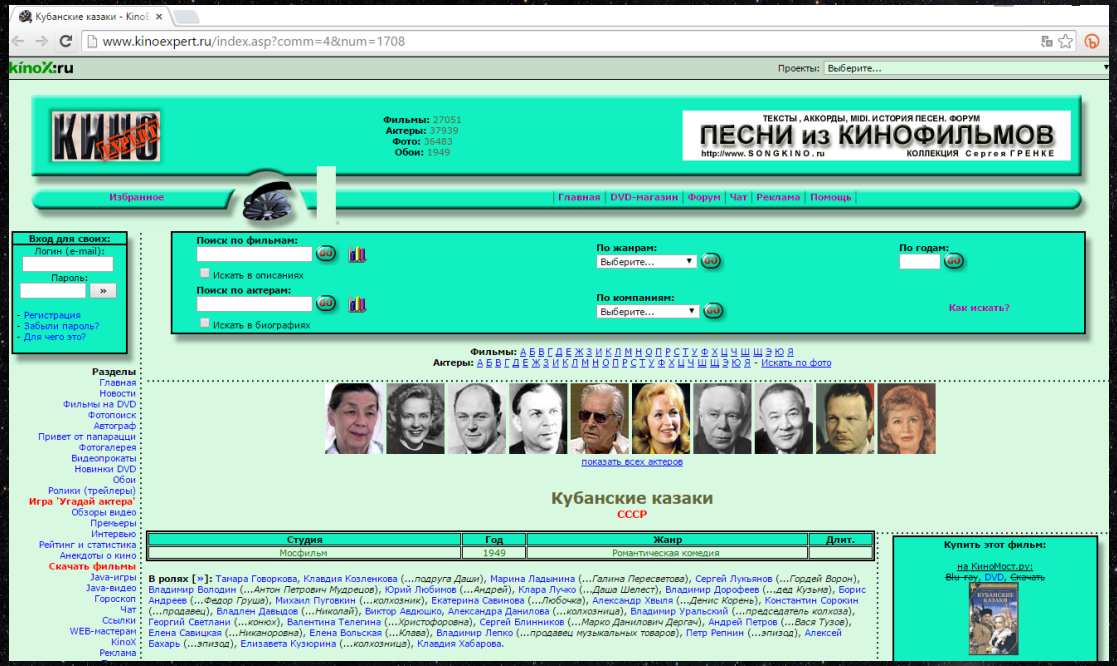
Turla-Abused Satellites

- 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

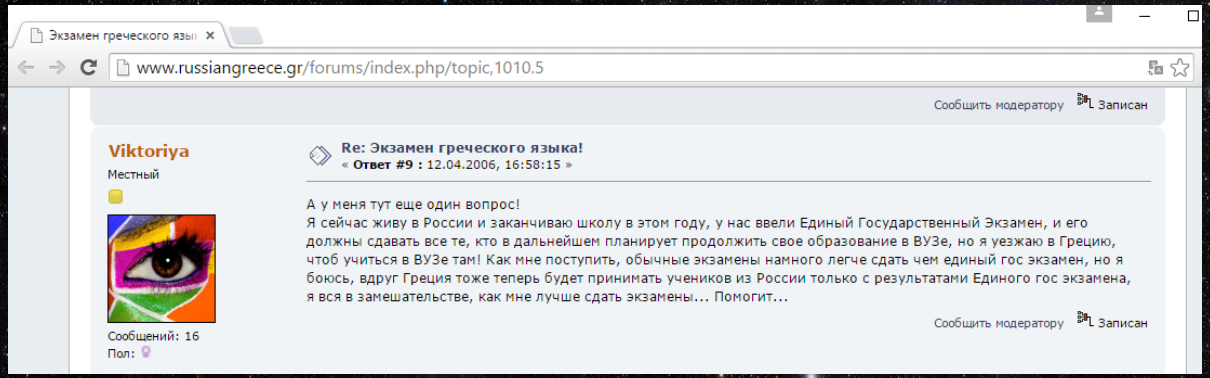
Bonus: Greece, Turla, and Old Cossack Movies

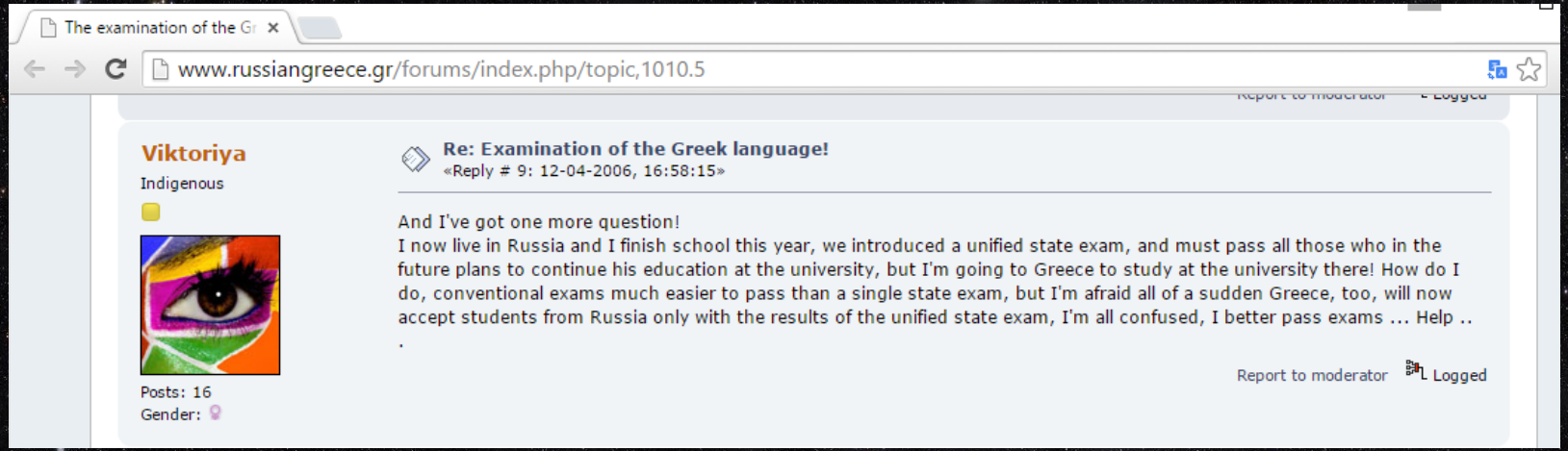


От представителей современной молодежи, (мне 17) могу сказать, что от фильма ия ПРОСТО В ВОСТОРГЕ, всетаки как раньше могли снимать кино, но жизнь и вправду не похожа на реальную послецоенную ситуацию России

Автор: Viktoriya
[02.05.2007, IP 83.235.19.125]

Bonus: Greece, Turla, and Old Cossack Movies





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-penquin-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/uroburos.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-uroburos-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