Satellite Turla: APT Command and Control in the Sky

How the Turla operators hijack satellite Internet links

By Stefan Tanase on September 9, 2015. 9:58 am

RESEARCH

APT CYBER ESPIONAGE TURLA

Stefan Tanase
@stefant

Have you ever watched satellite television? Were you amazed by the diversity of TV channels and radio stations available? Have you ever looked in wonder at satellite phones or satellite-based Internet connections wondering what makes them tick? What if we told you that there's more to satellite-based Internet connections than entertainment, traffic and weather? Much, much more.

When you are an APT group, you need to deal with many different problems. One of them, and perhaps the biggest, is the constant seizure and takedown of domains and servers used for command-and-control (C&C). These servers are constantly appropriated by law enforcement or shut down by ISPs. Sometimes they can be used to trace the attackers back to their physical locations.

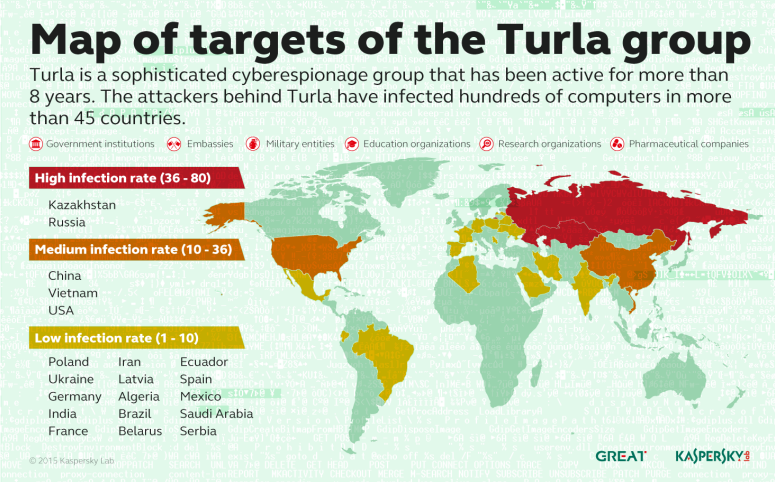
Some of the most advanced threat actors or users of commercial hacking tools have found a solution to the takedown problem — the use of satellite-based Internet links. In the past, we've seen three different actors using such links to mask their operations. The most interesting and unusual of them is the Turla group.

Also known as Snake or Uroburos, names which come from its top class rootkit, the Turla cyber-espionage group has been active for more than 8 years. Several papers have been published about the group's operations, but until the Epic Turla research was published by Kaspersky Lab, little information was available about the more unusual aspects of their operations, such as the first stages of infection through watering-hole attacks.

What makes the Turla group special is not just the complexity of its tools, which include the Uroboros rootkit, aka "Snake", as well as mechanisms designed to bypass air gaps through multi-stage proxy networks inside LANs, but the exquisite satellite-based C&C mechanism used in

the latter stages of the attack.

In this blog, we hope to shed more light on the satellite-based C&C mechanisms that APT groups, including the Turla/Snake group, use to control their most important victims. As the use of these mechanisms becomes more popular, it's important for system administrators to deploy the correct defense strategies to mitigate such attacks. For IOCs, see the appendix.



Technical details

Although relatively rare, since 2007 several elite APT groups have been using — and abusing — satellite links to manage their operations — most often, their C&C infrastructure. Turla is one of them. Using this approach offers some advantages, such as making it hard to identify the operators behind the attack, but it also poses some risks to the attackers.

On the one hand, it's valuable because the true location and hardware of the C&C server cannot be easily determined or physically seized. Satellite-based Internet receivers can be located anywhere within the area covered by a satellite, and this is generally quite large. The method used by the Turla group to hijack the downstream links is highly anonymous and does not require a valid satellite Internet subscription.

On the other hand, the disadvantage comes from the fact that satellite-based Internet is slow and can be unstable.

In the beginning, it was unclear to us and other researchers whether some of the links observed were commercial Internet connections via satellite, purchased by the attackers, or if the attackers had breached the ISPs and performed Man-in-the-Middle (MitM) attacks at the router level to hijack the stream. We have analyzed these mechanisms and come to the astonishing conclusion that the method used by the Turla group is incredibly simple and straightforward, as well as highly anonymous and very cheap to operate and manage.

Real satellite links, MitM attacks or BGP hijacking?

Purchasing satellite-based Internet links is one of the options APT groups can choose to secure their C&C traffic. However, full duplex satellite links can be very expensive: a simple duplex 1Mbit up/down satellite link may cost up to $7000 per week. For longer term contracts this cost may decrease considerably, but the bandwidth still remains very expensive.

Another way of getting a C&C server into a satellite's IP range is to hijack the network traffic between the victim and the satellite operator and to inject packets along the way. This requires either exploitation of the satellite provider itself, or of another ISP on the way.

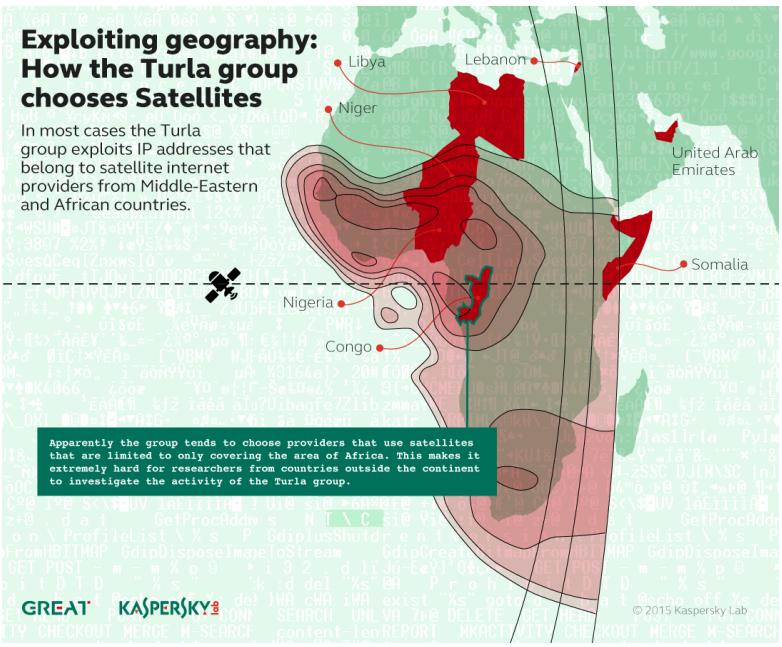
These kinds of hijacking attacks have been observed in the past and were documented by Renesys (now part of Dyn) in a blogpost dated November 2013.

According to Renesys: *"Various providers' BGP routes were hijacked, and as a result a portion of their Internet traffic was misdirected to flow through Belarusian and Icelandic ISPs. We have BGP routing data that show the second-by-second evolution of 21 Belarusian events in February and May 2013, and 17 Icelandic events in July-August 2013."*

In a more recent blogpost from 2015, Dyn researchers

point out that: *"For security analysts reviewing alert logs, it is important to appreciate that the IP addresses identified as the source of incidents can and are regularly spoofed. For example, an attack that appeared to come from a Comcast IP located in New Jersey may really have been from a hijacker located in Eastern Europe, briefly commandeering Comcast IP space. It is interesting to note that all six cases discussed above were conducted from either Europe or Russia."*

Obviously, such incredibly apparent and large-scale attacks have little chance of surviving for long periods of time, which is one of the key requirements for running an APT operation. It is therefore not very feasible to perform the attack through MitM traffic hijacking, unless the attackers have direct control over some high-traffic network points, such as backbone routers or fiber optics. There are signs that such attacks are becoming more common, but there is a much simpler way to hijack satellite-based Internet traffic.



Satellite link (DVB-S) hijacking

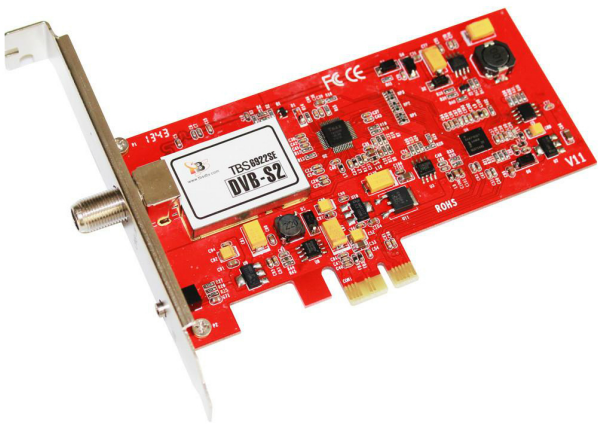
The hijacking of satellite DVB-S links has been described a few times in the past and a presentation on hijacking satellite DVB links was delivered at BlackHat 2010 by the

S21Sec researcher Leonardo Nve Egea.

To hijack satellite DVB-S links, one needs the following:

- A satellite dish – the size depends on geographical position and satellite
- A low-noise block downconverter (LNB)
- A dedicated DVB-S tuner (PCIe card)
- A PC, preferably running Linux

While the dish and the LNB are more-or-less standard, the card is perhaps the most important component. Currently, the best DVB-S cards are made by a company called TBS Technologies. The TBS-6922SE is perhaps the best entry-level card for the task.



TBS-6922SE PCIe card for receiving DVB-S channels

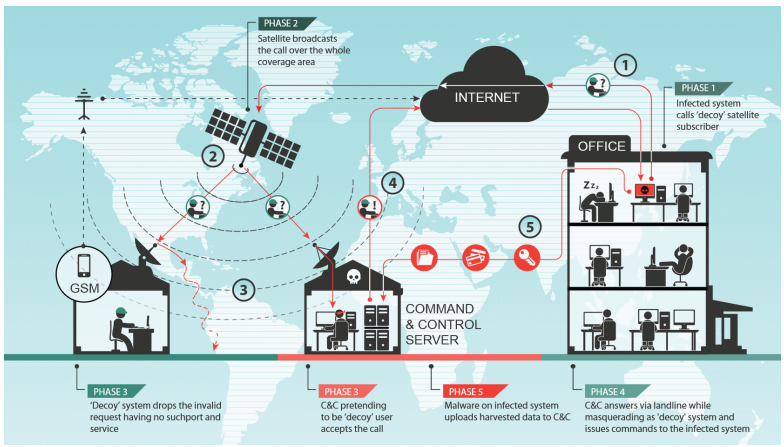
The TBS card is particularly well-suited to this task because it has dedicated Linux kernel drivers and supports a function known as a brute-force scan which allows wide-frequency ranges to be tested for interesting signals. Of course, other PCI or PCIe cards might work as well, while, in general the USB-based cards are relatively poor and should be avoided.

Unlike full duplex satellite-based Internet, the downstream-only Internet links are used to accelerate Internet downloads and are very cheap and easy to deploy. They are also inherently insecure and use no encryption to obfuscate the traffic. This creates the

possibility for abuse.

Companies that provide downstream-only Internet access use teleport points to beam the traffic up to the satellite. The satellite broadcasts the traffic to larger areas on the ground, in the Ku band (12-18Ghz) by routing certain IP classes through the teleport points.

How does satellite internet hijacking work?



To attack satellite-based Internet connections, both the legitimate users of these links as well as the attackers' own satellite dishes point to the specific satellite that is broadcasting the traffic. The attackers abuse the fact that the packets are unencrypted. Once an IP address that is routed through the satellite's downstream link is identified, the attackers start listening for packets coming from the Internet to this specific IP. When such a packet is identified, for instance a TCP/IP SYN packet, they identify the source and spoof a reply packet (e.g. SYN ACK) back to the source using a conventional Internet line.

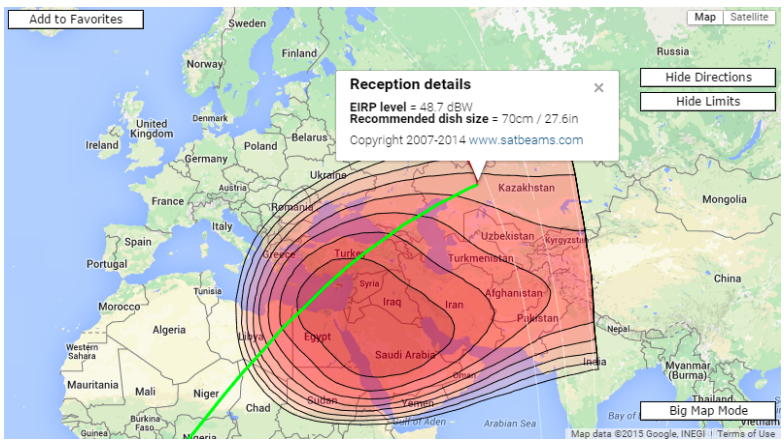
At the same time, the legitimate user of the link just ignores the packet as it goes to an otherwise unopened port, for instance, port 80 or 10080. There is an important observation to make here: normally, if a packet hits a closed port, a RST or FIN packet will be sent back to the source to indicate that there is nothing expecting the packet. However, for slow links, firewalls are recommended and used to simply DROP packets to

closed ports. This creates an opportunity for abuse.

Abused Internet ranges

During the analysis, we observed the Turla attackers abusing several satellite DVB-S Internet providers, most of them offering downstream-only connections in the Middle East and Africa. Interestingly, the coverage of these beams does not include Europe or Asia, meaning that a dish is required in either the Middle East or Africa. Alternatively, a much larger dish (3m+) can be used in other areas to boost the signal.

To calculate the dish size, one can use various tools, including online resources such as satbeams.com:



Sample dish calculation – (c) www.satbeams.com

The table below shows some of the command-and-control servers related to the Turla actor with domains resolving to an IP belonging to satellite-based Internet providers:

IP	First seen	Hosts
84.11.79.6	Nov, 2007	n/a, see note below
92.62.218.99	Feb 25th, 2014	pressforum.serveblog.net music-world.servemp3.com
209.239.79.47	Feb 27th, 2014	pressforum.serveblog.net music-world.servemp3.com
209.239.79.52	March 18th, 2014	hockey-news.servehttp.com

209.239.79.152	March 18th, 2014	hockey-news.servehttp.com
209.239.79.33	January 25th, 2014	eu-society.com
92.62.220.170	March 19th, 2014	cars-online.zapto.org fifa-rules.25u.com forum.sytes.net health-everyday.faqserv.com music-world.servemp3.com nhl-blog.servegame.com olympik-blog.4dq.com supernews.sytes.net tiger.got-game.org top-facts.sytes.net x-files.zapto.org
92.62.219.172	April 26th, 2013	eu-society.com
82.146.174.58	May 28th, 2014	forum.sytes.net hockey-news.servehttp.com leagueoflegends.servequake.com music-world.servemp3.com
82.146.166.56	March 11th, 2014	easport-news.publicvm.com
82.146.166.62	June 24th, 2014	hockey-news.servehttp.com
62.243.189.231	April 4th, 2014	africankingdom.deaftone.com aromatravel.org marketplace.servehttp.com newutils.3utilities.com people-health.net pressforum.serveblog.net weather-online.hopto.org
77.246.76.19	March 17th, 2015	onlineshop.sellclassics.com
62.243.189.187	May 2nd, 2012	eu-society.com
62.243.189.215	January 3rd, 2013	people-health.net
217.20.243.37	July 3, 2014	forum.sytes.net music-world.servemp3.com
217.20.242.22	September	mediahistory.linkpc.net

	1st, 2014	
83.229.75.141	August 05, 2015	accessdest.strangled.net chinafood.chickenkiller.com coldriver.strangled.net developarea.mooo.com downtown.crabdance.com greateplan.ocry.com industrywork.mooo.com radiobutton.mooo.com securesource.strangled.net sportnewspaper.strangled.net supercar.ignorelist.com supernews.instanthq.com

Note: 84.11.79.6 is hardcoded in the configuration block of the malicious sample.

The observed satellite IPs have the following 'WHOIS' information:

IP	Country	ISP
92.62.220.170 92.62.219.172 92.62.218.99	Nigeria	Skylinks Satellite Communications Limited
209.239.79.47 209.239.79.52 209.239.79.152 209.239.79.33	UAE	Teleskies, Telesat Network Services Inc
82.146.174.58 82.146.166.56 82.146.166.62	Lebanon	Lunasat Isp
62.243.189.231 62.243.189.187 62.243.189.215	Denmark	Emperion
77.246.71.10 77.246.76.19	Lebanon	Intrasky Offshore S.a.l.
84.11.79.6	Germany	IABG mbH
217.20.243.37	Somalia	Sky Power International Ltd
		Sky Power

217.20.242.22	Nigeria	International Ltd
83.229.75.141	United Kingdom	SkyVision Global Networks Ltd
217.194.150.31	Niger	SkyVision Global Networks Ltd
41.190.233.29	Congo	Orioncom

One interesting case is probably 84.11.79.6, which falls into the satellite IP range of IABG mbH.

This IP is encrypted in the C&C of the following backdoor used by Turla group, known as "Agent.DNE":

md5	0328dedfce54e185ad395ac44aa4223c
size	91136 bytes
type	Windows PE

Agent.DNE C&C configuration

This Agent.DNE sample has a compilation timestamp of Thu Nov 22 14:34:15 2007, meaning that the Turla group has been using satellite-based Internet links for almost eight years.

Conclusions

The regular usage of satellite-based Internet links by the Turla group represents an interesting aspect of their operation. The links are generally up for several months,

but never for too long. It is unknown if this is due to operational security limitations self-imposed by the group or because of shutdown by other parties due to malicious behavior.

The technical method used to implement these Internet circuits relies on hijacking downstream bandwidth from various ISPs and packet-spoofing. This is a method that is technically easy to implement, and provides a much higher degree of anonymity than possibly any other conventional method such as renting a VPS or hacking a legitimate server.

To implement this attack methodology, the initial investment is less than $1000. Regular maintenance should be less than $1000 per year. Considering how easy and cheap this method is, it is surprising that we have not seen more APT groups using it. Even though this method provides an unmatched level of anonymfor logistical reasons it is more straightforward to rely on bullet-proof hosting, multiple proxy levels or hacked websites. In truth, the Turla group has been known to use all of these techniques, making it a very versatile, dynamic and flexible cyber-espionage operation.

Lastly, it should be noted that Turla is not the only APT group that has used satellite-based Internet links. HackingTeam C&Cs were seen on satellite IPs before, as well as C&Cs from the Xumuxu group and, more recently the Rocket Kitten APT group.

If this method becomes widespread between APT groups or worse, cyber-criminal groups, this will pose a serious problem for the IT security and counter-intelligence communities.

** A full paper on the Turla group's use of satellite-based Internet links is available to the customers of Kaspersky Intelligence Services.*

Indicators of compromise:

IPs:

84.11.79.6
41.190.233.29
62.243.189.187
62.243.189.215
62.243.189.231
77.246.71.10
77.246.76.19
77.73.187.223
82.146.166.56
82.146.166.62
82.146.174.58
83.229.75.141
92.62.218.99
92.62.219.172
92.62.220.170
92.62.221.30
92.62.221.38
209.239.79.121
209.239.79.125
209.239.79.15
209.239.79.152
209.239.79.33
209.239.79.35
209.239.79.47
209.239.79.52
209.239.79.55
209.239.79.69
209.239.82.7
209.239.85.240
209.239.89.100
217.194.150.31
217.20.242.22
217.20.243.37

Hostnames:

accessdest.strangled[.]net
bookstore.strangled[.]net
bug.ignorelist[.]com
cars-online.zapto[.]org
chinafood.chickenkiller[.]com

coldriver.strangled[.]net
developarea.mooo[.]com
downtown.crabdance[.]com
easport-news.publicvm[.]com
eurovision.chickenkiller[.]com
fifa-rules.25u[.]com
forum.sytes[.]net
goldenroade.strangled[.]net
greateplan.ocry[.]com
health-everyday.faqserv[.]com
highhills.ignorelist[.]com
hockey-news.servehttp[.]com
industrywork.mooo[.]com
leagueoflegends.servequake[.]com
marketplace.servehttp[.]com
mediahistory.linkpc[.]net
music-world.servemp3[.]com
new-book.linkpc[.]net
newgame.2waky[.]com
newutils.3utilities[.]com
nhl-blog.servegame[.]com
nightstreet.toh[.]info
olympik-blog.4dq[.]com
onlineshop.sellclassics[.]com
pressforum.serveblog[.]net
radiobutton.mooo[.]com
sealand.publicvm[.]com
securesource.strangled[.]net
softstream.strangled[.]net
sportacademy.my03[.]com
sportnewspaper.strangled[.]net
supercar.ignorelist[.]com
supernews.instanthq[.]com
supernews.sytes[.]net
telesport.mooo[.]com
tiger.got-game[.]org
top-facts.sytes[.]net
track.strangled[.]net
wargame.ignorelist[.]com
weather-online.hopto[.]org
wintersport.mrbasic[.]com
x-files.zapto[.]org

MD5s:

0328dedfce54e185ad395ac44aa4223c
18da7eea4e8a862a19c8c4f10d7341c0
2a7670aa9d1cc64e61fd50f9f64296f9
49d6cf436aa7bc5314aa4e78608872d8
a44ee30f9f14e156ac0c2137af595cf7
b0a1301bc25cfbe66afe596272f56475
bcfee2fb5dbc111bfa892ff9e19e45c1
d6211fec96c60114d41ec83874a1b31d
e29a3cc864d943f0e3ede404a32f4189
f5916f8f004ffb85e93b4d205576a247
594cb9523e32a5bbf4eb1c491f06d4f9
d5bd7211332d31dcead4bfb07b288473

Kaspersky Lab products detect the above Turla samples with the following verdicts:

Backdoor.Win32.Turla.cd
Backdoor.Win32.Turla.ce
Backdoor.Win32.Turla.cl
Backdoor.Win32.Turla.ch
Backdoor.Win32.Turla.cj
Backdoor.Win32.Turla.ck
Trojan.Win32.Agent.dne

References:

1. Agent.btz: a Source of Inspiration?
2. The Epic Turla operation
3. The ‘Penquin’ Turla

Related Posts

THERE ARE 3 COMMENTS

If you would like to comment on this article you must first login

garahm steele
Posted on September 9, 2015. 6:40 pm

would like more info regarding MITM etc

Reply

ed
Posted on September 10, 2015. 6:06 pm

Have you actually observed outbound c2 like you illustrate in the diagram? Or only downlink data being sent?

Reply

Jens Lechtenbörger
Posted on September 14, 2015. 1:58 pm

Many thanks for sharing these observations!
I believe that part of your analysis is mixed up.

> Once an IP address that is routed through the satellite's downstream link is identified, the attackers start listening for packets coming from the Internet to this specific IP. When such a packet is identified, for instance a TCP/IP SYN packet, they identify the source and spoof a reply packet (e.g. SYN ACK) back to the source using a conventional Internet line.

Say, Alice is the ordinary/legitimate subscriber, Bob sends this SYN packet to her, which is also received by Mallory, and Mallory sends the SYN/ACK. If Bob sends this SYN packet, he probably expects Alice to send the SYN/ACK, which she does. So, both Alice and Mallory send a SYN/ACK. What is Mallory supposed to gain from this?

> At the same time, the legitimate user of the link just ignores the packet as it goes to an otherwise unopened port, for instance, port

80 or 10080.

Huh? Bob opened that connection, so he certainly does not ignore packets. Alice responds to a SYN packet, so she does not ignore either. The port observed by Mallory quite likely is *not* unopened.

Instead, if I were Mallory, I would do the following: I see that Alice is a satellite subscriber and learn her IP address. Thus, I can send TCP SYN to Port 80 on her IP address. If she does not run a web server and is behind a firewall, I won't receive a reply. Thus, I can use her IP address and port 80 for my own server. (In fact, I can port scan on her; if she drops any SYN packet I can use that port instead of 80.) Packets will be delivered to her and me, she (or her firewall) throws away the packets, so my own connection will be stable.

I'd like to point out the lesson to be learned here: If you are on a broadcast network, send your RST packets. Otherwise, everyone is free to hide under your IP address.

(Besides, if there are unassigned IP addresses, Mallory might just use one of those—if they are routed by the satellite network's operator, although they are unassigned.)

Reply