17th International Conference on Space Operations, Dubai, United Arab Emirates, 6 - 10 March 2023.

SpaceOps-2023, ID # 118

THE ANOMALIES DETECTION BY BOTNETS IN THE OPERATIONAL PROCESS OF SPACE DATA

Jamel Metmati

[a] *Department of Cyber*, djamel.metmati@thalesgroup.com

Abstract

The data volume from Space is going to catch the levels need to be managed by others tools and methodologies. The levels of data are orchestrated by several criterias : nature, type, volume, form. And the receivers and the transmitter determine the path to store them a system or an equipment. The data Space combines the multi-criterias and the technologies need to used to stock it should be able to integrate the huge volume. As the monitoring as operational process are performed at the ground segment, the data process shall be automated to improve the Space management to commercial, science and exploration missions. In pursuing this purpose, the Space team incident response shall integrate the anomalies detection by the artificial intelligence by the botnets. The tools and the methodology require the introduction of botnets in the specific configuration to react at the moment where the data process adopts an abnormal behaviour. This operational process is linked with data model expected for the missions at the beginning of its development. This step is the result of simulationg processing in which the key performance indicator appears to fulfill the missions. The implementation of this processing is applicable in the Cloud systems for they own the computation capacity to initiate the detection process thanks to the orchestration mecanisms from DevSecOPs technologies.

Keywords: botnets, anomalies, data, detection

1. Introduction

The objectives of the work is to propose the detection methodology applicable to Space networks in the New Space context.

2. Methods

2.1 The botnets methodology

A botnet is the contraction of "robot network" and is a network of computer robots. It is a set of any machines compromised by unexpected stakeholders and manageable remotely, which are referred to as "zombie machines". Initially, they were networks of IRC bots that were assigned various tasks such as the automated management. There are two possible configurations: the infected terminal only responds to the commands of the botnet manager, or it can take orders from other infected machines integrated into the botnet [1] (like a decentralized network). In the first case, it is enough to neutralize the control center, easily identifiable, to bring down the botnet.

The orders can both come from the hacker's system and be relayed by one of the infected devices in the network. Identifying the master source within a network of thousands of machines is then much more complicated, giving the botnet a longer lifespan. Some botnets use updates that allow them to modify their viral signature and thus escape the surveillance of the most efficient antivirus programs.

In addition, all of them implement measures to perpetuate their influence and discretion (installation of rootkits, system modifications, protection against other malware that could hinder their actions). The propagation is most often carried out via already infected machines which in turn spread the virus or scan their original network for a vulnerability or backdoor.

In addition to the malicious actions performed on other devices through the botnet, the malware can also attack the infected device. In particular, it will try to retrieve activity and contact data of its target in order to find new victims that are easy to infect.

The potentiallity of botnets in the conttext of fusion networks including the optical and radio frequency equipment requires to think the architecture as the cluster of network in which the key components made the interface from a network to another. Moreover, the automatic data processing between the machine introduce the taxonomy of risks

to identify the botnets incoming and outcoming from the machines. And the role of the algorithm facilitates the detection methodologies [2].
The example of the GNSS receiver illustrates the features of the botnets methodology at the moment where the signal makes the go-between to the Space segment towards the ground segment and inversely. It should be considered the modulation with the binary sequencies through the receivers and with time slot to respect the system figur of merit. The figure II shows the generic communication between the ground and the Space segment.

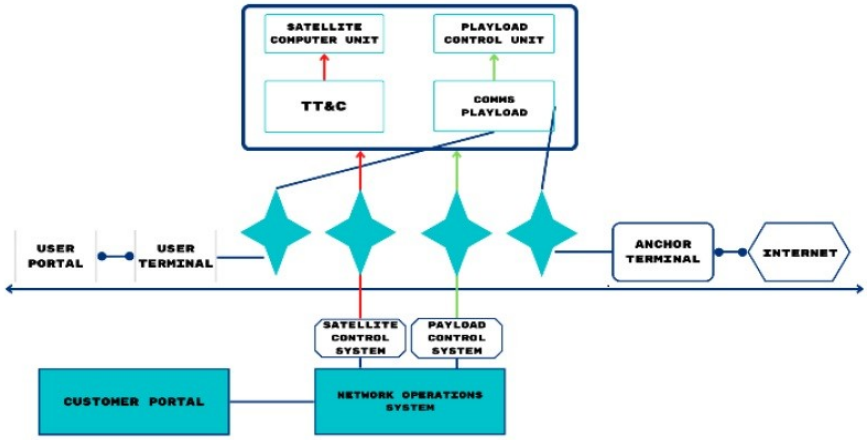

Fig. II: Ground segment for communications satellites

The features of commercial receivers in open sources with hardening solution demonstrate the methodology for the software system and flight requirements. The new features introduced by OS SIS ICD 2.0 [3] is the secondary synchronisation pattern for the errors estimation is lower, below 0,5m and 1,0m. These provide the inputs to built botnet to follow the anomalies from the unexpected behaviour of the receivers.
The improvements capabilities on I/NAV implemented is the FEC-2 and the SSP algorithms. Further, it explains the reasons for the RedCED could be a need for the implementation at the moment where the parameters in the receiver provide the Time to First Fix with the specific conditions of starting. Considering that the Galileo satellites transmit RedCED, if the E1-B data validity and signal health status flags are set to 0, the receiver doesn't output information on the demodulated RedCED parameters. It means the receiver is capable of providing a message containing the decoded RedCED at two moments: when the flag status change to 1 and in the case where the receiver uses a cold start and the hot start. Just the warm start needs to demodulate the CED and the RedCED transmitted during the I/NAV transmission.
The receiver distingues between PVT solutions evaluated by means of CED and those from RedCED are the conditions of starting according to the parameters: T warmup + T tracking+ T acquisition + T Time To data + T PVT to have the first position fix. The CED is used in the PVT solutions for Clock correction, Time and Ephemerides parameters. The link with CED is to indicate the position of satellite and to compute the pseudo-range. The time parameter T0e for Ephemeris data set is included in the receiver with 14 bits in the ROM.
The rest Clock correction and Ephemerides is also included with 10 bits associated with SISA IODnav. The RedCED takes account 122 bits of data parameters. In case of I/NAV words 1 to 4 are not available by the SHS flag and the DVS flag from SIS status flags during the transmission to carry the navigation data, it considers the RedCED intervenes automatically each 15 seconds in the T0 GST0 sync in the PVT solutions. Yes, the means combined Ethernet and Serial to ensure the availability of the data. The protocol is binary linked with a frame structured transmission protocol.
The algorithm implementation is able to exploit either the FEC Error&Erasure Correction. For both, it introduces the error correction code before the transmission or the storage of data in the receiver. The Reed Solomon Parity Words is then able to recover the signal by its capacity to gather multiple bits including the 8 bits Secondary Synchronisation Pattern of the 120 bits I/NAV message. Considering the wrong symbols produces noise in the

channel, the parameters "<=30" and "<=60" shall be included in the Viteri algorithm to initiate the restoration process for Error correction and Erasure. The Reed Solomon Parity shall reduce the time to restore because it provides Erasure and Error correction capabilities. To solve the local time uncertainly in case of receiver meets the synchronization requirement with respect to GST time, the time ambiguity by using only SSP can be solved by detection of single SSP. It is enough by using the symbol level through weak signal without demodulated the transmission. There is two types of receiver. The one combines the GNSS system [4] in order to collect, to fuse data from different constellations.

The second one that proposed works in Galileo only with the mode to catch both the specificity of precision and the data protection from the constellation. The receiver implements a decision tree inspiring from the Galileo broadcast SIS health status by the SSP at the moment the users get the possibility to reconstruct the GST broadcast. The content of E1 signal get SSP3, SSP1, SSP2 that follows the T0 synchronised with GST modulo 30 seconds.
The logic of health status flags management is based on the flags SHS "ok", DVS "NDV", SISA "not NAPA" completed by the CED sub-frame of E1-B message. For this last point, if there is 2 CED in the interval of 30 seconds, it shall be considered the health status flags management is nominal. The logic implemented on the interpretation of the health status parameters considers the link between the T0 (GST0 sync) (s) and the E1-B content. The first parameter gives the time in seconds and the E1-B content is given by the SSP frame. Under the PVT solution, it shall be considered the RedCED transmitted within 1 single I/NAV word, twice every 30s. It means the absence of the RedCED page in the sub-frame give the sign of health status. For example, the T0 (GST0 sync) (s) for 2 seconds is linked with SSP1. The T0 (GST0 sync) (s) for 4 seconds is linked with SSP2. And the T0 (GST0 sync) (s) for 15-16 seconds is linked with RedCED. All these parameters provide the health status parameters under the PVT solution.

In this context, the botnet methodology is based on the presence of a valid word type 16 appears three times. It constitutes one of the parameters of the health status management. For the second point, the broadcast may also be due to operational reasons unrelated to aforementioned SIS flags. In this case, it shall be considered healthy as marginal. The cold start is available in the context of the time to fix processing. And the receiver doesn't accept commands to force the cold start. Then, the NMEA sentences are "fix hours", "GSV frame", "satellites number", "first satellite identification", "azimuth of first satellite", "elevation of first satellite", "signal power". The interfaces are RF antenna through a chip. The RF connector is an internal antenna type JCN. In order to identify the proper uphill amplification stage to be used in the test set-up, the signal power level input at the receiver uses the E1 range 1559-1591 Mhz. The dissemination of data on the ground to the infrastructures provides the same requirements as any critical facilities which store data at rest and at transit. The botnets methodology can be adjusted by the documentation existing [5] ENISA to manage the traffic.

3. Results

3.1-The figur of merit anomalies detection

The performance of anomalies detection is based on the control agent on what the capacity of the botnets can do in the structure of networks. The detection shall be considered out of the data protection and the cryptography. The navigation message authentication (NMA) and Chips Message Robust Authentication (CHIMERA), which allow you to secure GPS signals using asymmetric elliptic curve digital signature algorithm (ECDSA). There is the Galileo GNSS system, as part of message authentication of its public open service, will incorporate the established Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol. The performance model are multiples. The performance can be realised by the zero trust security mode (ZTNA). It is a comprehensive security project based on strong authentication of each employee and software user in the network. A provision has been formed according to which each participant can be compromised. The botnet is introduced in the authentication process from small requests to test the sequences to get the access. The performance can be realised after the botnets effects in the complex network of Space-to-ground thanks to microsegmentation. This principle allows you to divide network flows so that potential attacks and threats can be easily localized and stopped on a specific segment. In addition, the Software Defined Perimeter (SDP) and VPN are security cyberarchitecture systems that can also be used internationally.
Considering the botnet agent, its configuration depends on its localisation in the complex networks according to the threats identified or the vulnerabilities which could make the damages for the components of the system and those of

satellites. The botnet can be autonomous or managed by a SIEM with the access right limited to be activate, to test the reaction of the networks to detect others potential botnets ennemies.
The algorithm existing detects the anomalies and the telemetry monitoring like NOSTRADAMUS or ADDICT on the spacecraft behaviour thanks to a datamodel. Others algorithm shall be performed with the integrated solution inside the networks Ground-to-Space for unexpected signature from the design and the simulation. The means to complete these events is the botnet algorithm which give the overview to monitor the anomalies in a data model expected and the one in an unexpected in the different technical context : the ground segment, the space segment on the spacecraft itself, the connectivity between the two segments, in or out a cloud provider solution. As the bots is ensured through the Command and Control server. The botnets can be used to achieve technical move in applying the interior activities in the depth networks.
The two-level monitoring allows an effective detection of bot malware activity which consists in sending data and receiving commands from bot master, at network level, and executing control commands,
The entropy variation shall be taken account in the network traffic : logical signature design based on anomaly model, it suppose the simulation of the networks with high value of computation test including the scenarios of the maintenance and the work of the networks. It means each porcessing of data for Space operation is itsef a model. The Cloud pipeline give an access to botnet agent networks inside the architecture itself. It forms the input command give an output expected connected with another bot agent located in the equipment specific location of the networks. The equipment can be physic in the hardware and logic in its configuration and in the binary data packets associated at the time windows of the sequences. Against re-built of ICD messages, the kill a process from the bytes size in transit in a case the system is on danger and the frame reforward the frame without authentication, the botnet ensure the legitimate transmission.
To do it, The botnet algorithm called ALBERAN integrates the parameters following : the network ID, the value of time, the number of network nodes, the max speed, the ICD and IP traffic, the propagation model, the packets size, the number of Bot agent. It considers the SIEM module from environment tunnelized and the Ghost script configuration applying on the traffic and configurated in the equipments from the Algorithm 1 on below.

Algorithm 1: Bot Agent

```
BEGIN
Input :  NF(Network flow), BA (Bot Agent)
Variables :  NF (Network frame), ID_BA (ID Botnet in the network location )
if (NF  is captured) then
    Extract Features from (NF );
    Generate (NF );
    Preprocess (NF );
    Send (NF ) to SIEM module ;
end if
if ( NF is captured) then
    Extract Frame from ( NF );
    Send (NF ) to BA (Bot Agent);
    Connect ( BA) to SIEM module;
end
```

4. Discussion

4.1-The data model

The connectivity in Space provide the challenges for the critical infrastrustures to manage the data of the networks and the fusion of several variety of network cluster. One of the major event is the beginning of the convergence of space technology and the Internet. The leading private corporations, such as SpaceX, Softbank, Amazon, Google, Virgin and Facebook are planning to place their spacecraft in Earth orbit, which will lead increase the number of satellites from 2000 to 20.000. This for the development of new services for the ground segment through the technologies are able to provide a quality of data transmission. The report of the Advisory Committee on Space Data Systems (CCSDS) - "On the threat to the safety of space missions"[7] describes a comprehensive overview of the basic fundamental which should take account to spacecraft and also the ground segment. It concerns the machine-to-machine exchange, the machine-to-human exchange, the human-to-machine exchange, the particle exchange in all context of the exchanges.

The discussion mentions the physical impact on the spacecraft and the attempted attack on an unearthly station in order to obtain data. The other possibilities for damage depends on the context and the fonctions of the spacecraft. Nevertheless, the taxinomy familiy of the damages include the Jamming, the Eavesdropping, the Electronic INTelligence, the Hijacking, the Spoofing, the Phishing. Each family items introduce the scenarios for which the data model should consider the networks science. It means the capacity to understand the structure of the data circulation in an architecture. As each structure is not the same, the data circulation uses several critical path which must be used and controlled to avoid any failure or damage for the activities supported. In Space for a direct communication to the spacecraft, one of mechanism of the data circulation to be understood is a Software-defined radio (SDR) module with an automatic and calibration unit (ACU).
In regard of the ground facilities, the data model is also applicable even more with the introduction of new technologies for the data circulation. Both in Space exploration and ground facilities for the commercial services, the connectivity considers the fusion networks in many technical context. In the case of the improving Entoto Observatory Optical Telescope (figure 3) for Space Surveillance and Tracking Application, the telescope gets several system interface from the observations sensors, the GNSS constellation and the command and control connecting with the users through Internet plus the external sources. It should be mentioned the GPS time server is itself linked with a complex sub-network from Space-to-ground. The signal path covers several equipements and the network structure requires the flags in the transmission and in the modulation. The internal structure demonstrates the TCP/IP interface to manage the tools used for the instruments and to store the scientific data.

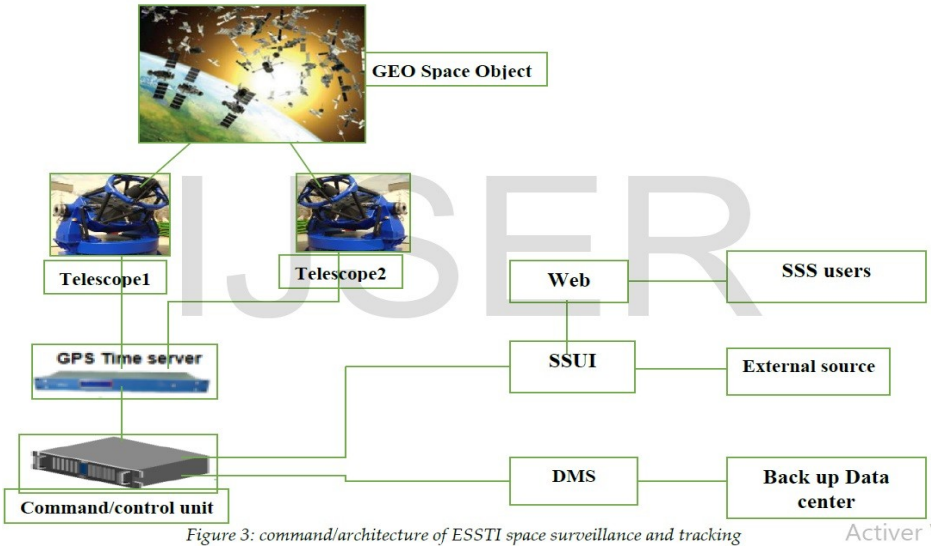

Figure 3: command/architecture of ESSTI space surveillance and tracking

5. Conclusion : The anomaly detection by botnet provide the requirements to be applied in the operational data space. The solution is suitable in the context where the services from Space increase the data exchange between the assets in Space and the one with the ground. The methodology shall be also applicable for the networks to the Moon to ensure the RAMs and to limit the FDIR.

References

Reference to a journal publication:

[1] Jason Fritz. "Satellite Hacking: A Guide for the Perplexed". In: *Culture Mandala* 10.1 (2013), p. 5906. url: https://cm.scholasticahq.com/article/5906- satellite-hacking-a-guide-for-the-perplexed.

[4] Jessica A Steinberger. "A Survey of Satellite Communications System Vulnerabilities". Air Force Institute of Technology, June 2008. url: https://core.ac.uk/download/pdf/288295156.pdf.

Reference to a conference/congress paper:

[2] Nils Ole Tippenhauer et al. "On the Requirements for Successful GPS Spoofing Attacks". In: *Proceedings of the 18th ACM Conference on Computer and Communications Security*. ACM Conference on Computer and Communications Security (CCS) (Chicago, Illinois, USA). CCS '11. 2011, pp. 75–86.

Reference to a book:

[3] European GNSS (Galileo) open service : signal in space interface control document, European Union, Publications Office of the European Union, Luxembourg et 2010

[5] Good practices guide for deploying DNSSEC. Saragiotis, P. ENISA Technical Report, 2010. [Online] http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssecp

[6] CCSDS. *Security Threats Against Space Missions*. Report concerning space data system standards. Dec. 2015. url: https://public.ccsds.org/Pubs/350x1g2.pdf.