REPORT nº 01-2018,
on Attempted Invasion and Unauthorized use of Online Systems

1. - Fact:
Attempted Invasion and Unauthorized use of server and smtp service (domain: rdc.pro.br)

2. - Date:
16th August 2018: perception of the attack due to log analysis on this date, made to detect system overload
15th July 2018: most distant log date on which traces of the attack were found

3. - Human Analysis of Logs related with the Attack:
/var/log/mail.log
First Analysis:
mail.log [from 13th August 2018, 07h:53:29 to 17th August 2018, 08h:08:01]
research term: “SASL LOGIN authentication failed”
nº of attempts: 6305
below (4) sample of 43 IPs regarding unauthorized access attempts
Second Analysis:
mail.log.4; mail.log.3; mail.log.2; mail.log.1 [from 15th July 2018, 07:55:41]
research term: “SASL LOGIN authentication failed”
nº of attempts: 6019 + 65810 + 40015 + 38921 = 181472
nº of attempts = 187777

/var/log/auth.log (em análise conjunta com o Log anterior)
First Analysis:
auth.log [from 15th July 2018, 07h:58:00 to 17/08/2018, 13h:30:04]
research term: “Authentication failure”, after “user unknown”, based on the number of attempts with this term
nº of attempts: 12849 + 39953 + 40721 + 69150 + 40721 = 203394 (excluding 1 user, because it is known that he occurs in this error)

Crossing Log Analysis: between 180,000 and 200,000 attacks in the estimated period of 1 month

4. - Sample of 43 IPs of the attack and respective Geolocation* (from 13th August 2018 to 17th August 2018)**:**

IP Address	*Country*	*Location*	*ISP*	*Legal Entity*
181.214.206.18	US	Sioux Falls, Dakota do Sul, Estados Unidos, América do Norte	HOST1PLUS hosting services. Brazil.	HOST1PLUS hosting services. Brazil.
181.214.206.39	US	Sioux Falls, Dakota do Sul, Estados Unidos, América do Norte	HOST1PLUS hosting services. Brazil.	HOST1PLUS hosting services. Brazil.
181.214.206.233	US	Sioux Falls, Dakota do Sul, Estados Unidos, América do Norte	HOST1PLUS hosting services. Brazil.	HOST1PLUS hosting services. Brazil.
181.214.206.200	US	Sioux Falls, Dakota do Sul, Estados Unidos, América do Norte	HOST1PLUS hosting services. Brazil.	HOST1PLUS hosting services. Brazil.
181.214.206.111	US	Sioux Falls, Dakota do Sul, Estados Unidos, América do Norte	HOST1PLUS hosting services. Brazil.	HOST1PLUS hosting services. Brazil.
181.214.206.103	US	Sioux Falls, Dakota do Sul, Estados Unidos, América do Norte	HOST1PLUS hosting services. Brazil.	HOST1PLUS hosting services. Brazil.
116.196.121.103	CN	Pequim, Beijing, China, Ásia	China Unicom Beijing	China Unicom Beijing
181.198.19.219	EC	Guaiaquil, Provincia del Guayas, Equador, América do Sul	Telconet S.A	Telconet S.A
45.125.66.168	LT	Kaunas, Kaunas, Kaunas,	Tele Asia Limited	Tele Asia Limited

IP Address	*Country*	*Location*	*ISP*	*Legal Entity*
		Lituânia, Europa		
178.141.251.45	RU	Vyatskiye Polyany, Kirovskaya Oblast', Rússia, Europa	MTS PJSC	Mobile Telesystems PJSC, Kirov branch
37.49.230.143	NL	Holanda, Europa	Estro Web Services Private Limited	Estro Web Services Private Limited
80.82.70.225	SC	Anse aux Pins, Anse-aux-Pins, Ilhas Seychelles, África	Incrediserve LTD	Quasi Networks LTD.
185.125.159.250	LB	Beirute, Beyrouth, Líbano, Ásia	Gulf Research & Development Company	Gulf Research & Development Company
190.111.24.194	GT	Cidade da Guatemala, Departamento de Guatemala, Guatemala, América do Norte	Navega.com S.A.	Navega.com S.A.
160.119.159.140	MZ	República de Moçambique, África	Voiptech-limitada	Voiptech-limitada
192.99.203.89	US	Newark, Nova Jérsia, Estados Unidos, América do Norte	OVH Hosting	OVH Hosting
80.82.65.169	SC	Ilhas Seychelles, África	Incrediserve LTD	Quasi Networks LTD.
188.82.246.156	PT	Pampilhosa da Serra, Coimbra, Portugal, Europa	MEO	MEO
175.139.184.225	MY	Kuala Lumpur, Kuala Lumpur, Malásia, Ásia	TM Net	TM Net
91.196.212.90	PL	Cracóvia, Pequena Polónia,	TELNET Sp. z o.o.	TELNET Sp. z o.o.

		Polônia, Europa		
179.156.118.223	BR	Ribeirão Preto, São Paulo, Brasil, América do Sul	NET Virtua	NET Virtua
201.59.254.170	BR	Niterói, Rio de Janeiro, Brasil, América do Sul	Oi Internet	Oi Internet
45.125.66.117	LT	Kaunas, Kaunas, Kaunas, Lituânia, Europa	Tele Asia Limited	Tele Asia Limited
200.174.176.146	BR	Belém, Para, Brasil, América do Sul	Claro S.A.	Claro S.A.
177.47.92.229	BR	Pedreiras, Maranhao, Brasil, América do Sul	Novelty Telecom Ltda	Novelty Telecom Ltda
80.11.241.22	FR	França, Europa	Orange	Orange
46.225.129.170	IR	Irã, Ásia	Dadeh Gostar Asr Novin P.J.S. Co.	Dadeh Gostar Asr Novin P.J.S. Co.
200.29.108.214	CO	Cali, Departamento del Valle del Cauca, Colômbia, América do Sul	Empresas Municipales De Cali E.i.c.e. E.s.p.	Empresas Municipales De Cali E.i.c.e. E.s.p.
124.232.164.28	CN	Hunan, China, Ásia	China Telecom Hunan	No.293,Wanbao Avenue
103.218.2.239	CN	China, Ásia	Qinglong Road,Longhua New area,Shenzhen China	hongkong kwaifong information service limited
162.247.99.113	US	Center Point, Iova, Estados Unidos,	Tisp Limited	Cloud Iv Limited

		América do Norte		
103.218.2.239	CN	China, Ásia	Qinglong Road,Longhua New area,Shenzhen China	hongkong kwaifong information service limited
37.156.28.48	IR	Irã, Ásia	Mobin Net Communication Company (Private Joint Sto	Mobinnet WiMAX Users
191.242.116.33	BR	Montes Claros, Minas Gerais, Brasil, América do Sul	Plim Telecom	Plim Telecom
190.213.10.158	TT	Trindade e Tobago, América do Norte	Columbus Communications Trinidad Limited.	Columbus Communications Trinidad Limited.
186.251.225.186	BR	Atibaia, São Paulo, Brasil, América do Sul	Starnet Telecomunicacoes Ltda	Starnet Telecomunicacoes Ltda
203.19.70.166	AU	Sydney, Nova Gales do Sul, Austrália, Oceania	iiNet Limited	iiNet Limited
117.3.171.42	VN	Nha Trang, Tinh Khanh Hoa, Vietnã, Ásia	Viettel Group	Viettel Group
154.73.182.16	ZA	Kempton Park, Gauteng, África do Sul, África	Tesuco Telecommunication (pty) Ltd	Tesuco-Telecommunications
177.47.92.229	BR	Pedreiras, Maranhao, Brasil, América do Sul	Novelty Telecom Ltda	Novelty Telecom Ltda
117.3.171.132	VN	Nha Trang, Tinh Khanh Hoa, Vietnã, Ásia	Viettel Group	Viettel Group
190.144.74.106	CO	Colômbia, América do Sul	Telmex Colombia S.A.	Telmex Colombia S.A.
119.148.13.194	BD	Daca, Dhaka, Dhaka Division, Bangladexe, Ásia	Agni Systems Limited	Agni Systems Limited

* https://www.maxmind.com/pt/geoip-demo

5. - Measures taken:
- checking of main.cf rules in Postfix, concerning to smtpd constraints
- blocking by iptables
    -- the following IPs were blocked at the days 16th and 17th August 2018:
    (iptables -A INPUT -s IP.xx.xx.xx -j DROP)
    181.214.206.18,181.214.206.39,181.214.206.233,181.214.206.200,181.214.206.111,181.214.206.103,116.196.121.103,181.198.19.219,45.125.66.168,178.141.251.45,37.49.230.143,80.82.70.225,185.125.159.250,190.111.24.194,160.119.159.140,192.99.203.89,80.82.65.169,188.82.246.156,175.139.184.225,91.196.212.90,179.156.118.223,201.59.254.170,45.125.66.117,200.174.176.146,177.47.92.229,122.116.29.1,80.11.241.22,187.67.39.153,46.225.129.170,200.29.108.214,124.232.164.28,103.218.2.239,162.247.99.113,103.218.2.239,37.156.28.48,191.242.116.33,190.213.10.158,186.251.225.186,203.19.70.166,117.3.171.42,154.73.182.16,177.47.92.229,117.3.171.132,190.144.74.106,94.79.4.143,117.3.171.132,95.158.150.48,119.148.13.194,154.73.182.16,193.165.55.126,79.147.41.31,190.213.10.158,176.79.86.153,27.118.30.52,122.116.29.1,196.203.109.154,193.165.55.126,95.168.96.77,162.247.99.113,161.132.201.90,119.225.101.53,161.132.201.90,184.71.152.86,200.87.62.142,84.216.36.138,187.162.195.111,184.71.152.86,200.29.108.214,117.2.18.212,200.29.108.214,199.168.141.166,177.37.166.119,82.127.128.117,186.208.221.218
    -- we opted for the risk of blocking any legitimate users of these IPs that might be sending e-mails to the system
- update of the system (Linux 3.13.0-153-generic, Postfix 2.11.0, Dovecot 2.2.9)
- increased log storage for 20 (software default = 4), concerning to the analyzed logs – *Compliance:* Brazilian Law 12.965/2014, Article 15
- check log more frequently, considering attacks that do not overwhelm the system being processed, as was the present attack reported for the most part in which it occurred.

6. - Result of Technology Measures / Result of Attack:
- Attempts of unauthorized use (approximately 190,000 in 1 month) were not successful; during the period of 1 month analyzed retroactively the date of perception of the attack, no relevant damage to the system was verified; the attempted attacks are being blocked on the present date of 08/17/2018, having noticed a drastic reduction thereof as of 09:00 am on this day; the monitoring of these logs should continue in the coming days as well as the blockings.

7. - Criminal rules infringed by the attackers:
- Brazil: Brazilian Criminal Code, Article 154-A
- U.S.A.: 18, U.S.C., §1037 (a) (1) (2), depending of confirmation by a US lawyer
- Germany, member of EU: German Criminal Code, Section 303b (Computer Saboutage), depending of confirmation by a German lawyer

8. - In reality, and not only theoretically, there is chance of indemnity? How to find the real attacker?
- Difficulty to find the true attacker. Even knowing what ISP given an IP to whom has carried out the attack, can happens that the computer of this direct attacker was hacked by the real attacker, and so on, having the true attacker used of several intermediate computers, putting several IPs in front of he/she. This situation, depending on the expertise of real attacker, can make impossible the investigation, that can be necessary in several jurisdictions, or even impossible. The transfer of presumed responsibility to the direct attacker, who comes to bear the duty of proving that he is not a criminal, but that was sabotaged, used, does not appear possible at the present moment. There is a high cost with communications and the actions that shall be taken with the service providers, who are not required to deliver the IP's user without a reasoned judicial order.

17th August 2018

This is the Report and opinion

Rafael De Conti
OAB/SP 249.808
rdc@decontilawoffice.com