RELATÓRIO / AVISO nº 01-2018,
sobre Tentativa de Invasão e Uso não-autorizado de sistemas online

1. - Ato:
Tentativa de invasão e uso, sem permissão, de servidor e serviço smtp (domínio alvo: rdc.pro.br)

2. - Datas:
16/08/2018: percepção do ataque em razão de análise de log nesta data, feita para detectar sobrecarregamento do sistema
15/07/2018: data mais distante de log na qual se encontrou rastros do ataque

3. - Análise humana de Logs relacionados ao ataque:
/var/log/mail.log
Primeira Análise:
mail.log [de 13/08/2018, 07h:53:29 até 17/08/2018, 08h:08:01]
termo de pesquisa: “SASL LOGIN authentication failed”
nº de tentativas: 6305
abaixo (4) amostra de 43 IPs referentes as tentativas de acesso não autorizado
2º Análise:
mail.log.4; mail.log.3; mail.log.2; mail.log.1 [a partir de 15/07/2018, 07:55:41]
termo de pesquisa: “SASL LOGIN authentication failed”
nº de tentativas: 6019 + 65810 + 40015 + 38921 = 181472
nº de tentativas = 187777

/var/log/auth.log (em análise conjunta com o Log anterior)
Primeira Análise:
auth.log [de 15/07/2018, 07h:58:00 até 17/08/2018, 13h:30:04]
termo de pesquisa: “Authentication failure”, depois “user unknown”, baseando-se nº de tentativas neste termo
nº de tentativas: 12849 + 39953 + 40721 + 69150 + 40721 = 203394 (excluindo-se 1 user, pois sabe-se que incorre neste erro)

Cruzamento de análise de logs:
aproximadamente, entre 180 mil e 200 mil ataques, no período aproximado de 1 mês

4. - Amostra de 43 IPs do ataque e respectiva Geolocalização* (de 13/08/2018 até 17/08/2018)**:**

Endereço IP	*País*	*Localização*	*ISP*	*Organização*
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

Endereço IP	*País*	*Localização*	*ISP*	*Organização*
		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. - Medidas tomadas:
- checagem de regras main.cf no Postfix, relativamente as restrições de smtpd
- estancamento via iptables
    -- os seguintes IPs foram ‘dropados’ nos dias 16 e 17/08/2018:
    (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
    -- optou-se pelo risco de bloquear eventuais usuários legítimos destes IPs que pudessem estar enviando e-mails para o sistema
- update do sistema (Linux 3.13.0-153-generic, Postfix 2.11.0, Dovecot 2.2.9)
- aumento do armazenamento de log para 20 (padrão do software = 4), relativamente aos logs analisados – *Compliance:* Lei 12.965/2014, Art. 15 e ss.
- checar log com maior frequência, considerando ataques que não sobrecarregam o sistema em processamento, como foi o presente ataque relatado durante a maior parte em que ocorreu.

6. - Resultado das Medidas de tecnologia / Resultado do Ataque:
- as tentativas de uso não autorizado (aproximadamente 190 mil em 1 mês) não foram bem sucedidas enquanto ocorreram; durante o período de 1 mês analisado retroativamente a data de percepção do ataque, não se verificou dano relevante ao sistema; as tentativas de ataque estão sendo bloqueadas na presente data do dia 17/08/2018, tendo se notado redução drástica das mesmas a partir de 09h:00 deste dia; o monitoramento destes logs deve continuar nos próximos dias, bem como os bloqueios.

7. - Potenciais normas criminais infringidas pelos atacantes:
- Brasil: Código Penal, 154-A
- EUA: 18, U.S.C., §1037 (a) (1) (2)
- Alemanhã, membro da UE: Código Penal Alemão, Seção 303b (Sabotagem de computador)

8. - Possibilidade real, e não em tese, de reparação cível? Como chegar no real atacante?
- Dificuldade de se chegar ao real atacante. Mesmo sabendo-se qual o provedor de serviço de internet que atribui um IP para o atacante que realizou o ataque ora relatado, pode ser que a máquina deste atacante imediato tenha sido invadida pelo real atacante, e assim por diante, tendo o real atacante se utilizado de várias máquinas intermediárias, colocando diversos IPs na sua frente. Esta situação, dependendo da expertise do atacante real, pode levar a inviabilidade da investigação, que pode facilmente ter que vir a passar por várias jurisdições. Transferência de responsabilidade presumida para o atacante imediato, que passa a ter o ônus de provar que não agiu criminosamente, mas sim que foi sabotado, usado, no presente momento parece inviável. Custo elevado de comunicações e ações diante dos provedores de serviço, que não são obrigados a entregar o usuário do IP a não ser sob ordem judicial fundamentada.

17 de agosto de 2018

É o Relatório,
s.m.j.

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