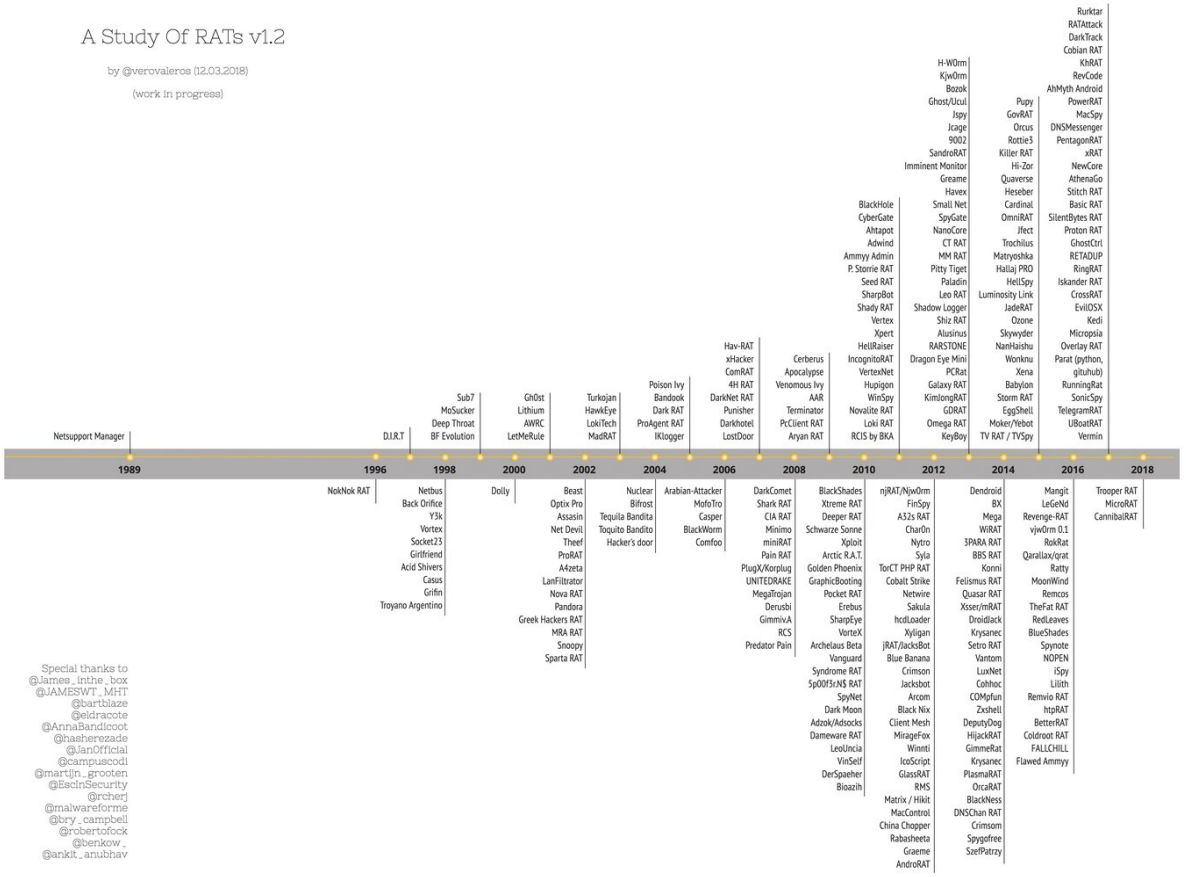
A Study of RATs: Third Timeline Iteration

veronicavaleros.com/blog/2018/3/12/a-study-of-rats-third-timeline-iteration

March 12, 2018

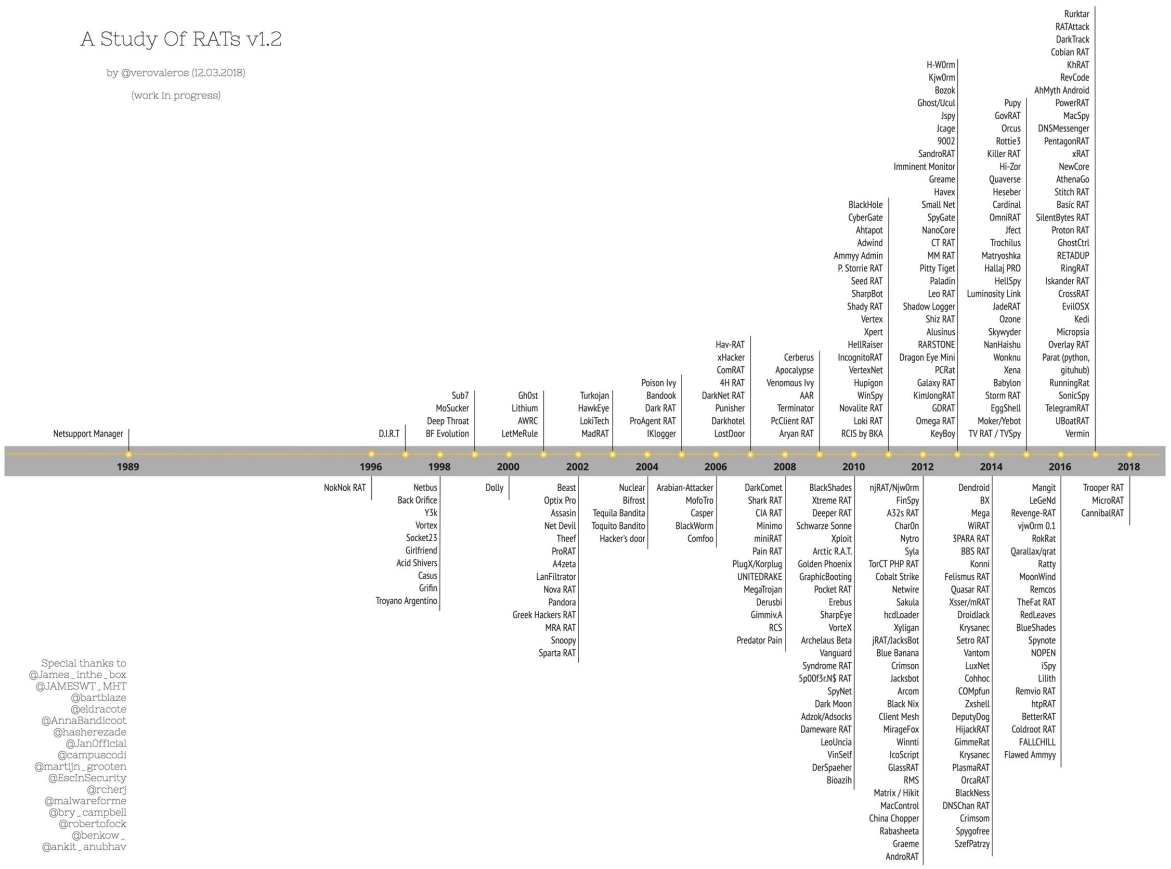


March 12, 2018 Veronica Valeros

It has been already a year since I started this project to study Remote Access Trojans! As a reminder, the goal of this project is to discover possible trends, similarities, and other hidden aspects among RATs observed in the last 30 years. This research is divided in several stages. The first stage is to collect a good population of RAT families. The second stage consists in studying and analysing their offered features and characteristics. The third stage will be defined later, it may go to source code analysis and evolutions per family.

The goal of the first stage was to collect 300 well known RATs, find their time of appearance, and create a timeline to visualise the results. After one year of work, it is now completed. Yes, completed. Here are the results in the hope that you will help me fix the possible mistakes and inaccuracies!

The third timeline iteration is going public on Mar 18, 2018. This version covers 30 years and 300 RATs!



I would like to specially thank the following people for all the help provided during the last year: @James_inthe_box @JAMESWT_MHT @bartblaze @eldracote @AnnaBandicoot @hasherezade @Jan0fficial @campuscodi @martijn_grooten @EscInSecurity @rcherj @malwareforme @bry_campbell @robertofock @benkow_ @ankit_anubhav. Without you, this work wouldn't have come this far! Thank you!

Limitations of this research

While 300 RATs seems a lot, there are online forums like www.megasecurity.org, which have listed more than 4000 RATs on their site. I learnt that during 1980s and 1990s, almost every kid on the planet was coding their own RAT for fun. As with any research, setting limitations and a concrete scope was mandatory. I decided not to process these RATs and only take the most well known, documented, and those for who there was some additional report outside these forums.

As a colleague from the community made me notice, there is malware with RAT features that may be added to this list or not depending on which features we want to focus on. For this reason, right now I decided not to include Client Maximus banker/rat here. Questionable? Absolutely. I needed to draw the line somewhere.

What is next?

The second phase will focus on studying each of these 300 RATs features: targeted platform, functionalities, if they were used in targeted attacks, number of known versions, etc. The end result of this phase would be, as Edward Tufte suggested, a series of small multiples to visualise these different features and characteristics.

The 300 most well known RATs of the last 30 years

Nº	Year	Remote Access Trojan
1	1989	Netsupport manager remote control software
2	1996	NokNok
3	1997	D.I.R.T.
4	1998	Socket23
5	1998	Netbus
6	1998	BO2K/Back Orifice/Body Odour
7	1998	Y3k RAT
8	1998	Vortex
9	1998	Girlfriend
10	1998	Acid Shivers
11	1998	Casus
12	1998	Grifin
13	1998	Troyano Argentino
14	1999	Deep Throat
15	1999	Subseven / Sub7 / Backdoor G
16	1999	Mosucker / MiniMo
17	1999	BF Evolution
18	2000	Dolly
19	2001	Gh0st / Moudoor
20	2001	Lithium
21	2001	AWRC / Atelier Web Remote Commander

Nº	Year	Remote Access Trojan
22	2001	LetMeRule
23	2002	Beast
24	2002	Optix Pro
25	2002	Assasin / Assassin
26	2002	Net Devil
27	2002	Theef
28	2002	ProRAT
29	2002	A4zeta
30	2002	LanFiltrator
31	2002	Nova RAT
32	2002	Pandora
33	2002	Greek Hackers RAT
34	2002	MRA RAT
35	2002	Snoopy
36	2002	Sparta RAT
37	2003	Turkojan
38	2003	HawkEye
39	2003	LokiTech
40	2003	MadRAT
41	2004	Bifrost
42	2004	Hacker's door
43	2004	Nuclear RAT
44	2004	Tequila Bandita
45	2004	Toquito Bandito
46	2005	Poison Ivy / Darkmoon

Nº	Year	Remote Access Trojan
47	2005	Bandook
48	2005	Dark RAT
49	2005	ProAgent RAT
50	2005	IKlogger
51	2006	BlackWorm / Blackmal / Nyxem / MyWife
52	2006	Arabian-Attacker
53	2006	Casper
54	2006	MofoTro
55	2006	Comfoo
56	2007	Hav-RAT
57	2007	xHacker RAT
58	2007	Agent.BTZ/ ComRAT
59	2007	Tapaoux / Darkhotel
60	2007	4H RAT
61	2007	DarkNet RAT
62	2007	Punisher
63	2007	LostDoor
64	2008	CIA RAT
65	2008	DarkComet
66	2008	Derusbi
67	2008	MegaTrojan
68	2008	Minimo
69	2008	miniRAT
70	2008	Pain RAT
71	2008	PlugX/Korplug

Nº	Year	Remote Access Trojan
72	2008	Shark RAT
73	2008	UNITEDRAKE
74	2008	Gimmiv.A
75	2008	RCS (hacking team)
76	2008	Predator Pain
77	2009	AAR / Albertino Advanced RAT
78	2009	Apocalypse
79	2009	Cerberus
80	2009	Venomous Ivy
81	2009	Terminator RAT / FakeM RAT
82	2009	PcClient RAT
83	2009	Aryan RAT
84	2010	Dameware RAT
85	2010	BlackShades
86	2010	Xtreme RAT
87	2010	Deeper RAT
88	2010	Schwarze Sonne/Daleth RAT
89	2010	Xploit
90	2010	Arctic R.A.T.
91	2010	Golden Phoenix Rat
92	2010	GraphicBooting RAT
93	2010	Pocket RAT
94	2010	Erebus
95	2010	SharpEye
96	2010	VorteX RAT

Nº	Year	Remote Access Trojan
97	2010	Archelaus Beta
98	2010	Vanguard
99	2010	Syndrome RAT
100	2010	5p00f3r.N$ RAT
101	2010	SpyNet
102	2010	Dark Moon
103	2010	Adzok/Adsocks
104	2010	Bioazih
105	2010	LeoUncia
106	2010	VinSelf
107	2010	DerSpaeher / derSphear RAT
108	2011	BlackHole
109	2011	CyberGate
110	2011	Ahtapot
111	2011	Adwind/Frutas/AlienSpy/Unrecom/Sockrat/JSocket/JBifrost
112	2011	Ammyy Admin
113	2011	P. Storrie RAT
114	2011	Seed RAT
115	2011	SharpBot/SB RAT
116	2011	Shady RAT
117	2011	Vertex
118	2011	Xpert RAT
119	2011	HellRaiser
120	2011	IncognitoRAT
121	2011	VertexNet

Nº	Year	Remote Access Trojan
122	2011	Hupigon / MFC Huner
123	2011	WinSpy
124	2011	Novalite
125	2011	Loki RAT
126	2011	RCIS by BKA
127	2012	Rabasheeta
128	2012	MacControl
129	2012	Matrix / Hikit / Gaolmay
130	2012	IcoScript
131	2012	GlassRAT
132	2012	Winnti
133	2012	A32s RAT
134	2012	AndroRAT
135	2012	Arcom
136	2012	Black Nix
137	2012	Blue Banana
138	2012	Char0n
139	2012	Client Mesh
140	2012	Cobalt Strike
141	2012	Crimson
142	2012	FinSpy
143	2012	hcdLoader
144	2012	Jacksbot
145	2012	jRAT/JacksBot
146	2012	Netwire

Nº	Year	Remote Access Trojan
147	2012	njRAT/Njw0rm
148	2012	Nytro Rat
149	2012	Mirage/MirageFox
150	2012	Sakula/Sakurel/Viper
151	2012	Syla RAT
152	2012	TorCT PHP RAT
153	2012	RMS / Remote Manipulator System
154	2012	Xyligan
155	2012	China Chopper
156	2012	Graeme
157	2013	KimJongRAT
158	2013	ShadowLogger
159	2013	Shiz RAT / Mutant
160	2013	Alusinus
161	2013	H-W0rm/Houdini/Dunihi
162	2013	Kjw0rm
163	2013	Bozok
164	2013	Ghost/Ucul
165	2013	Imminent Monitor RAT
166	2013	Jspy
167	2013	Jcage
168	2013	9002/Hydraq/McRAT
169	2013	Sandro RAT
170	2013	Greame
171	2013	Havex

Nº	Year	Remote Access Trojan
172	2013	Small Net
173	2013	SpyGate
174	2013	NanoCore
175	2013	CT RAT
176	2013	MM RAT / Goldsun
177	2013	Pitty Tiger
178	2013	Paladin RAT
179	2013	Leo RAT
180	2013	RARSTONE
181	2013	Dragon Eye – Mini
182	2013	PCRat
183	2013	Galaxy RAT
184	2013	KeyBoy
185	2013	GDRAT
186	2013	Omega RAT
187	2014	Krysanec
188	2014	Setro RAT
189	2014	Vantom
190	2014	Dendroid
191	2014	BX
192	2014	Mega
193	2014	WiRAT/Winner RAT
194	2014	3PARA RAT
195	2014	BBS RAT
196	2014	Konni

Nº	Year	Remote Access Trojan
197	2014	Felismus RAT
198	2014	Quasar RAT
199	2014	Xsser / mRAT
200	2014	Crimsom
201	2014	DroidJack
202	2014	LuxNet
203	2014	Cohhoc
204	2014	COMpfun
205	2014	Zxshell / Sensode
206	2014	DeputyDog / Fexel
207	2014	HijackRAT
208	2014	GimmeRat
209	2014	Krysanec
210	2014	PlasmaRAT
211	2014	OrcaRAT
212	2014	BlackNess
213	2014	DNSChan RAT
214	2014	Spygofree
215	2014	SzefPatrzy
216	2015	Ozone
217	2015	Skywyder
218	2015	NanHaishu
219	2015	Luminosity Link
220	2015	Pupy
221	2015	GovRAT

Nº	Year	Remote Access Trojan
222	2015	Orcus
223	2015	Rottie3
224	2015	Killer RAT
225	2015	Hi-Zor
226	2015	Quaverse/QRAT
227	2015	Heseber
228	2015	Cardinal
229	2015	OmniRAT
230	2015	Jfect
231	2015	Trochilus RAT
232	2015	Matryoshka
233	2015	Hallaj PRO
234	2015	HellSpy
235	2015	JadeRAT
236	2015	wonknu
237	2015	Xena
238	2015	Babylon RAT
239	2015	Storm RAT
240	2015	Moker / Yebot / Tilon
241	2015	EggShell
242	2015	TV RAT / TV Spy / Trojan.Pavica / Trojan.Mezzo
243	2016	Remvio RAT
244	2016	Spynote
245	2016	Mangit
246	2016	LeGeNd

Nº	Year	Remote Access Trojan
247	2016	BlueShades
248	2016	Revenge-RAT
249	2016	vjw0rm
250	2016	rokrat
251	2016	Qarallax / Qrat / Quaverse / Qrypter
252	2016	Ratty
253	2016	MoonWind
254	2016	RemCos
255	2016	TheFatRAT
256	2016	RedLeaves
257	2016	NOPEN
258	2016	iSpy
259	2016	Lilith
260	2016	htpRAT
261	2016	BetterRAT
262	2016	Coldroot RAT
263	2016	FALLCHILL
264	2016	FlawedAmmyy
265	2017	GhostCtrl
266	2017	RETADUP
267	2017	AhMyth Android RAT
268	2017	AthenaGo
269	2017	Cobian RAT
270	2017	DarkTrack
271	2017	DNSMessenger

Nº	Year	Remote Access Trojan
272	2017	KhRAT
273	2017	MacSpy
274	2017	NewCore
275	2017	PentagonRAT Ransomware
276	2017	PowerRAT
277	2017	RATAttack
278	2017	RevCode
279	2017	Rurktar RAT
280	2017	Stitch RAT
281	2017	xRAT
282	2017	Basic RAT
283	2017	Proton
284	2017	SilentBytes RAT
285	2017	RingRAT
286	2017	Iskander RAT
287	2017	UBoatRAT
288	2017	SonicSpy
289	2017	Overlay RAT
290	2017	CrossRAT
291	2017	Vermin
292	2017	Kedi
293	2017	Parat
294	2017	EvilOSX
295	2017	Micropsia
296	2017	RunningRat

Nº	Year	Remote Access Trojan
297	2017	TelegramRAT
298	2018	Trooper RAT
299	2018	MicroRAT
300	2018	CannibalRAT

Do you see something that's not right? Let me know!