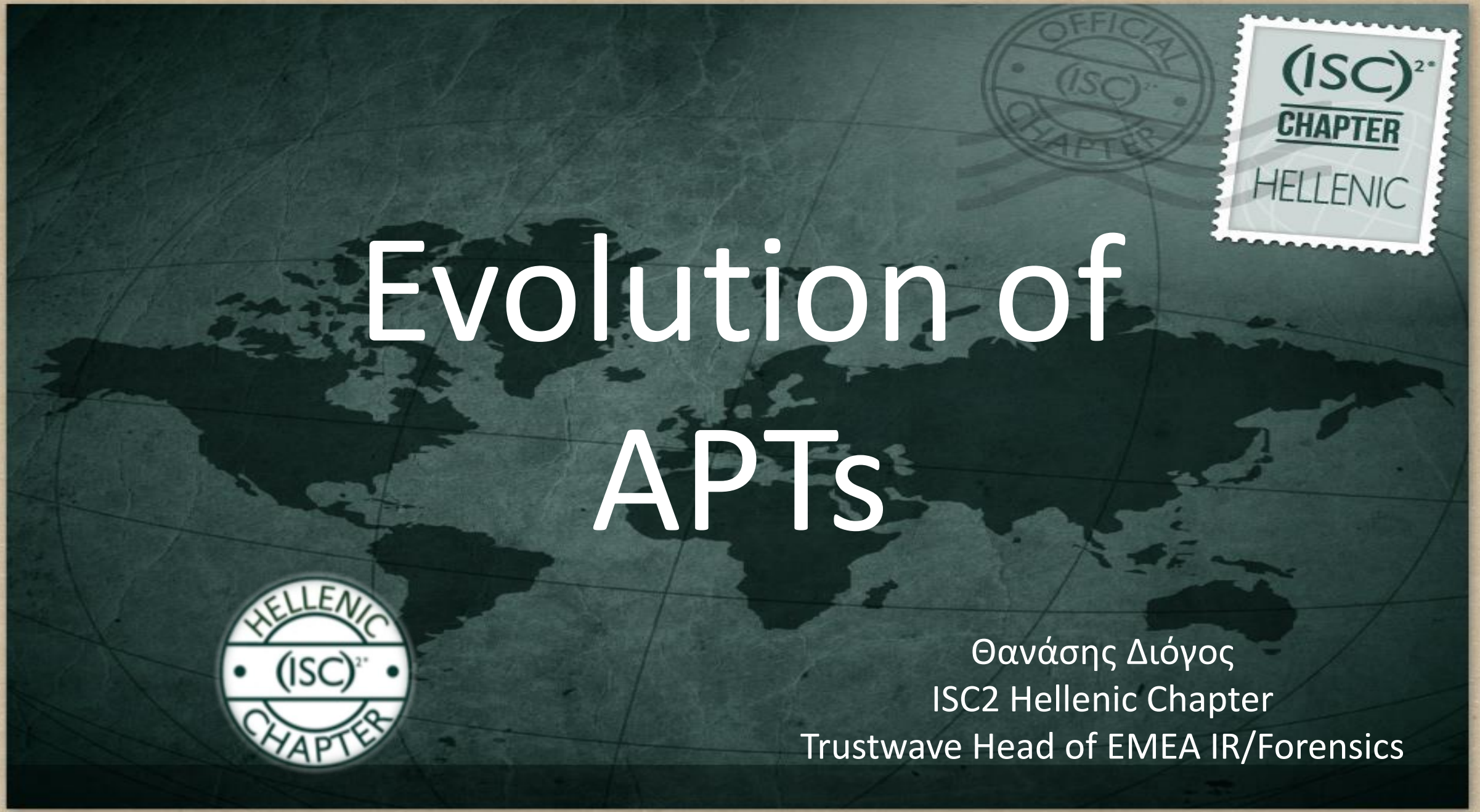
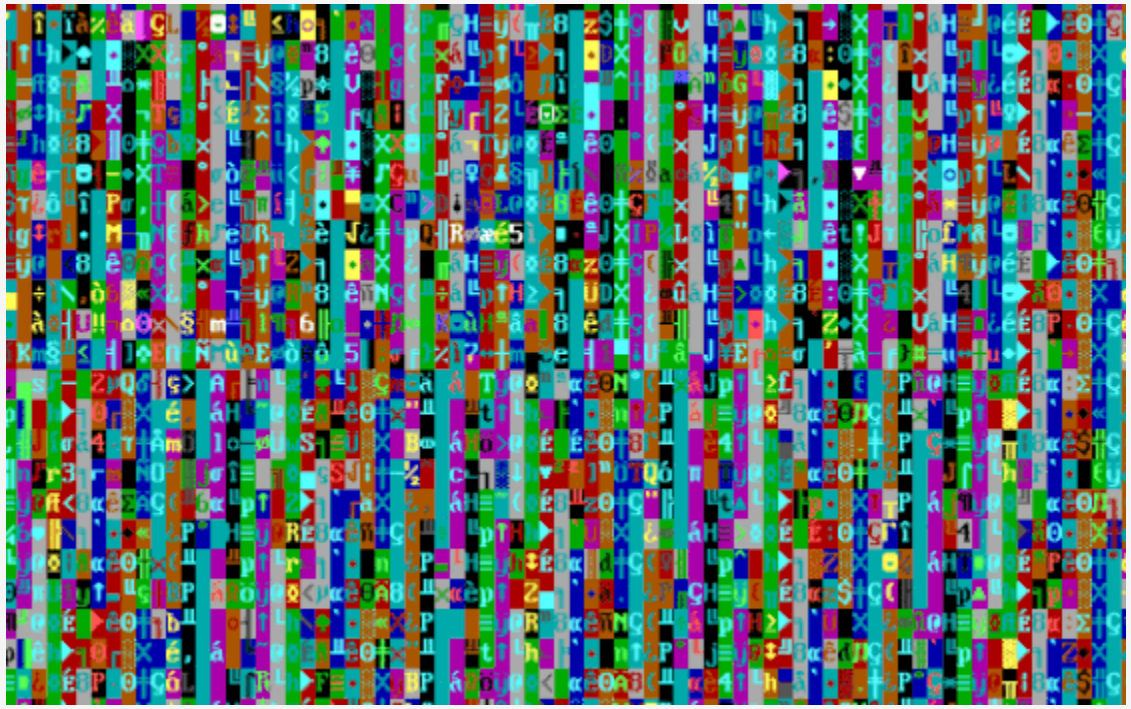


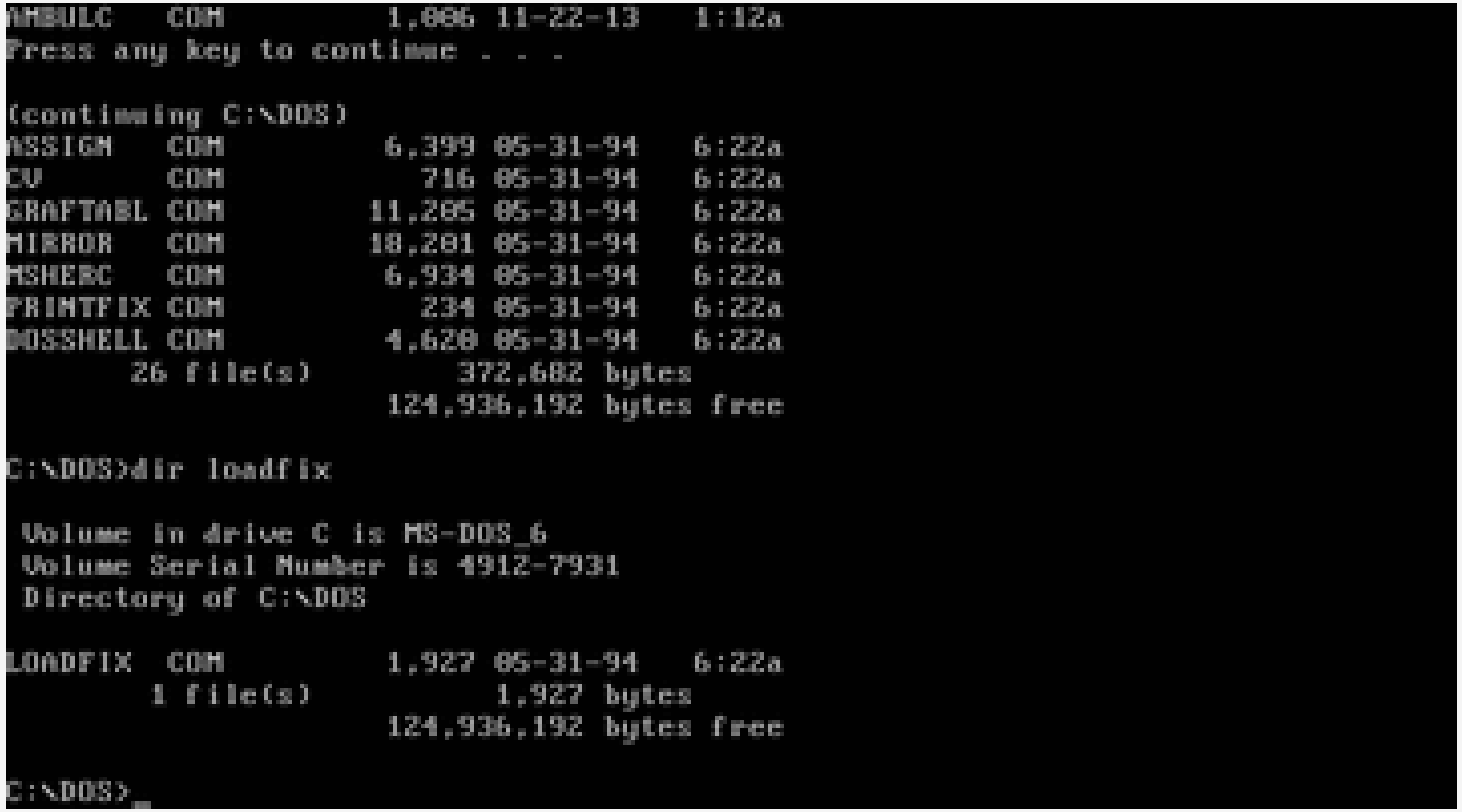
Evolution of APTs

Θανάσης Διόγος
ISC2 Hellenic Chapter
Trustwave Head of EMEA IR/Forensics

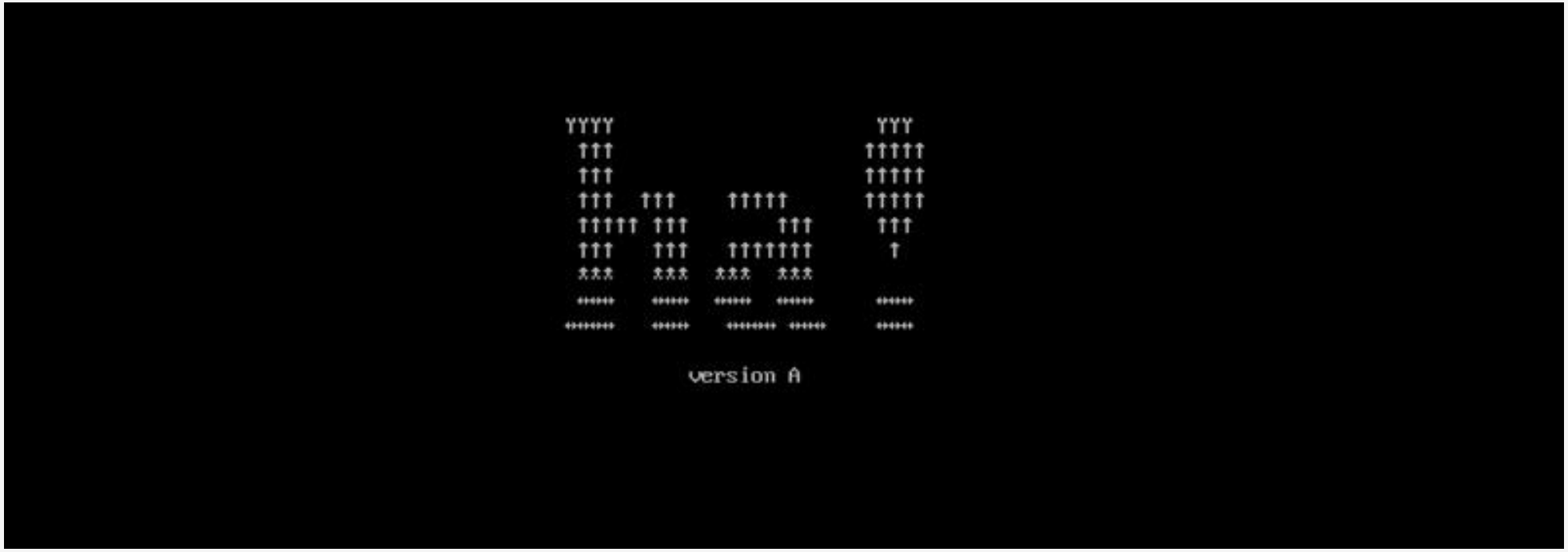
Very Old Days



Very Old Days

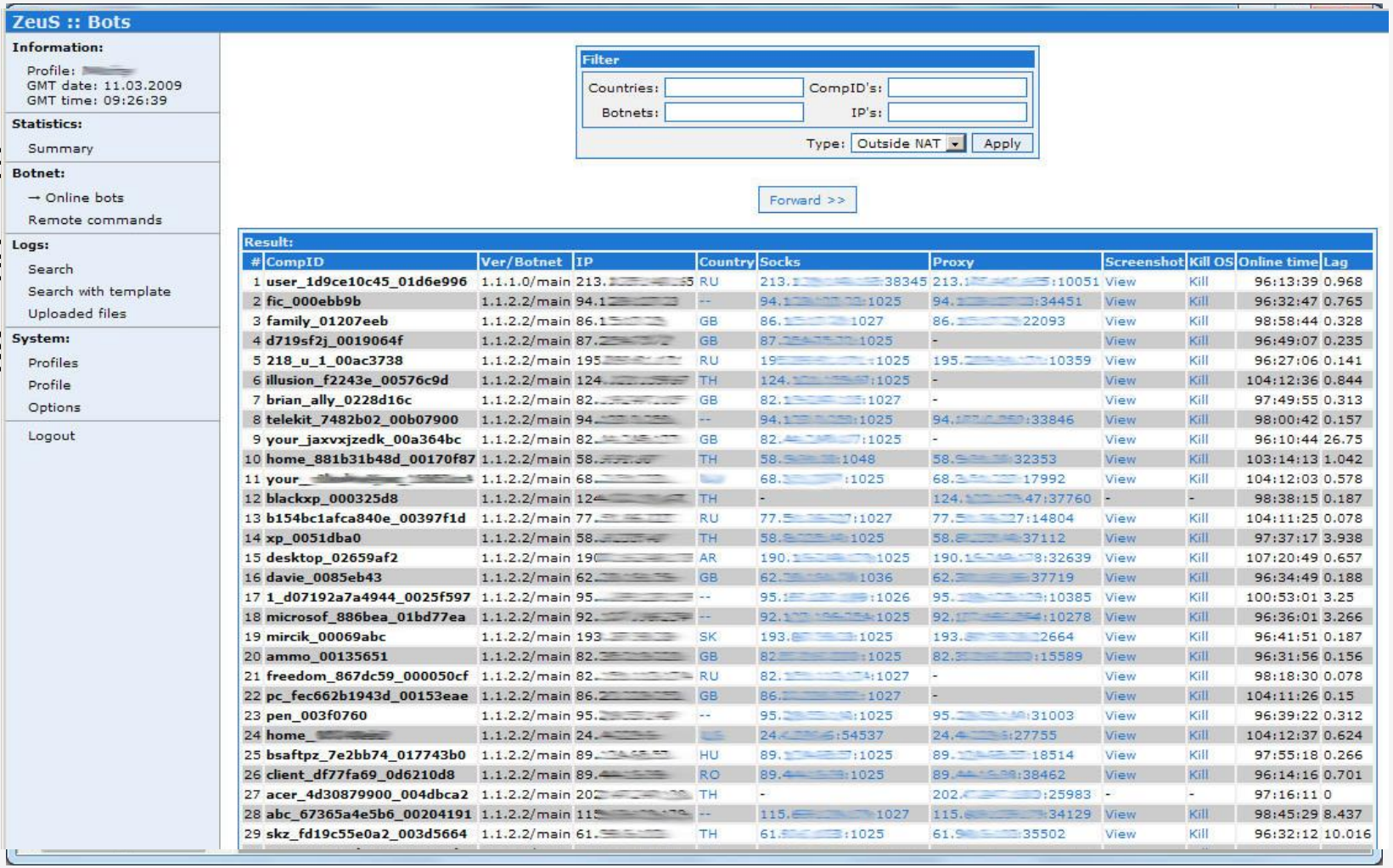


Very Old Days



Botnets

- Botnets
  - Comma
  - Stealing
  - Abusing
  - Etc.

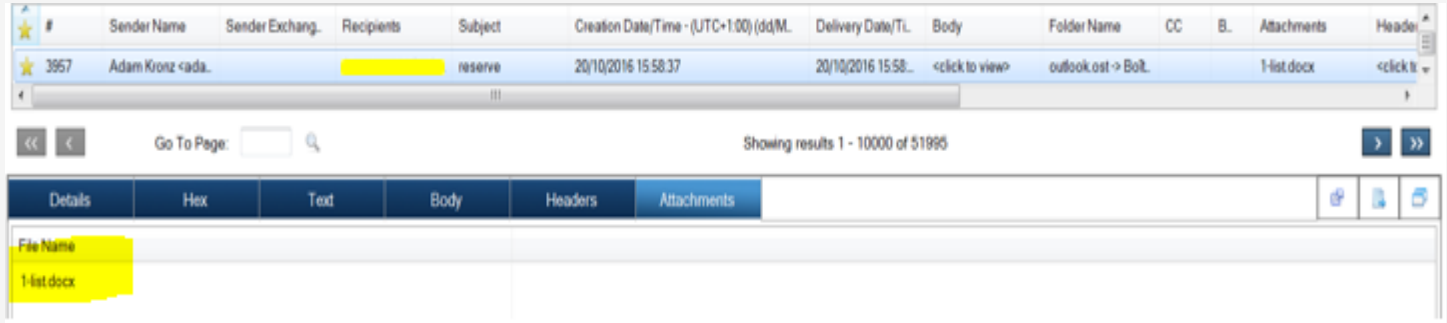


#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Kill OS	Online time	Lag
1	user_1d9ce10c45_01d6e996	1.1.1.0/main	213.	RU	213. :38345	213. :10051	View	Kill	96:13:39	0.968
2	fic_000ebb9b	1.1.2.2/main	94.1	--	94. :1025	94. :34451	View	Kill	96:32:47	0.765
3	family_01207eeb	1.1.2.2/main	86.1	GB	86. :1027	86. :22093	View	Kill	98:58:44	0.328
4	d719sf2j_0019064f	1.1.2.2/main	87.	GB	87. :1025	-	View	Kill	96:49:07	0.235
5	218_u_1_00ac3738	1.1.2.2/main	195	RU	19 :1025	195. :10359	View	Kill	96:27:06	0.141
6	illusion_f2243e_00576c9d	1.1.2.2/main	124.	TH	124. :1025	-	View	Kill	104:12:36	0.844
7	brian_ally_0228d16c	1.1.2.2/main	82.	GB	82. :1027	-	View	Kill	97:49:55	0.313
8	telekit_7482b02_00b07900	1.1.2.2/main	94.	--	94. :1025	94. :33846	View	Kill	98:00:42	0.157
9	your_jaxvxjzedk_00a364bc	1.1.2.2/main	82.	GB	82. :1025	-	View	Kill	96:10:44	26.75
10	home_881b31b48d_00170f87	1.1.2.2/main	58.	TH	58. :1048	58. :32353	View	Kill	103:14:13	1.042
11	your_	1.1.2.2/main	68.		68. :1025	68. :17992	View	Kill	104:12:03	0.578
12	blackxp_000325d8	1.1.2.2/main	124	TH	-	124. :37760	-	-	98:38:15	0.187
13	b154bc1afca840e_00397f1d	1.1.2.2/main	77.	RU	77. :1027	77. :14804	View	Kill	104:11:25	0.078
14	xp_0051dba0	1.1.2.2/main	58.	TH	58. :1025	58. :37112	View	Kill	97:37:17	3.938
15	desktop_02659af2	1.1.2.2/main	190	AR	190. :1025	190. :32639	View	Kill	107:20:49	0.657
16	davie_0085eb43	1.1.2.2/main	62.	GB	62. :1036	62. :37719	View	Kill	96:34:49	0.188
17	1_d07192a7a4944_0025f597	1.1.2.2/main	95.	--	95. :1026	95. :10385	View	Kill	100:53:01	3.25
18	microsof_886bea_01bd77ea	1.1.2.2/main	92.	--	92. :1025	92. :10278	View	Kill	96:36:01	3.266
19	mircik_00069abc	1.1.2.2/main	193	SK	193. :1025	193. :2664	View	Kill	96:41:51	0.187
20	ammo_00135651	1.1.2.2/main	82.	GB	82. :1025	82. :15589	View	Kill	96:31:56	0.156
21	freedom_867dc59_000050cf	1.1.2.2/main	82.	RU	82. :1027	-	View	Kill	98:18:30	0.078
22	pc_fec662b1943d_00153eae	1.1.2.2/main	86.	GB	86. :1027	-	View	Kill	104:11:26	0.15
23	pen_003f0760	1.1.2.2/main	95.	--	95. :1025	95. :31003	View	Kill	96:39:22	0.312
24	home_	1.1.2.2/main	24.		24. :54537	24. :27755	View	Kill	104:12:37	0.624
25	bsaftpz_7e2bb74_017743b0	1.1.2.2/main	89.	HU	89. :1025	89. :18514	View	Kill	97:55:18	0.266
26	client_df77fa69_0d6210d8	1.1.2.2/main	89.	RO	89. :1025	89. :38462	View	Kill	96:14:16	0.701
27	acer_4d30879900_004dbca2	1.1.2.2/main	202	TH	-	202. :25983	-	-	97:16:11	0
28	abc_67365a4e5b6_00204191	1.1.2.2/main	115	--	115. :1027	115. :34129	View	Kill	98:45:29	8.437
29	skz_fd19c55e0a2_003d5664	1.1.2.2/main	61.	TH	61. :1025	61. :35502	View	Kill	96:32:12	10.016

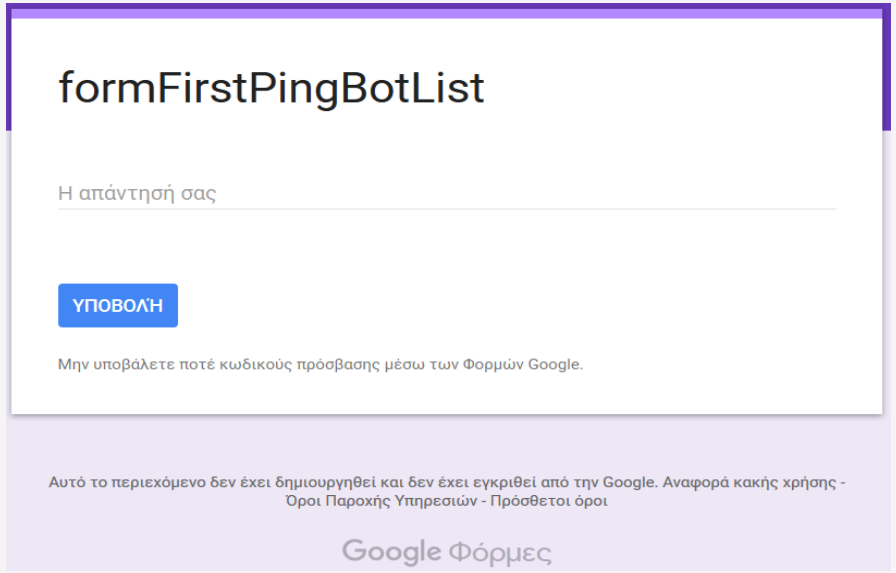
APT: Grand Mars

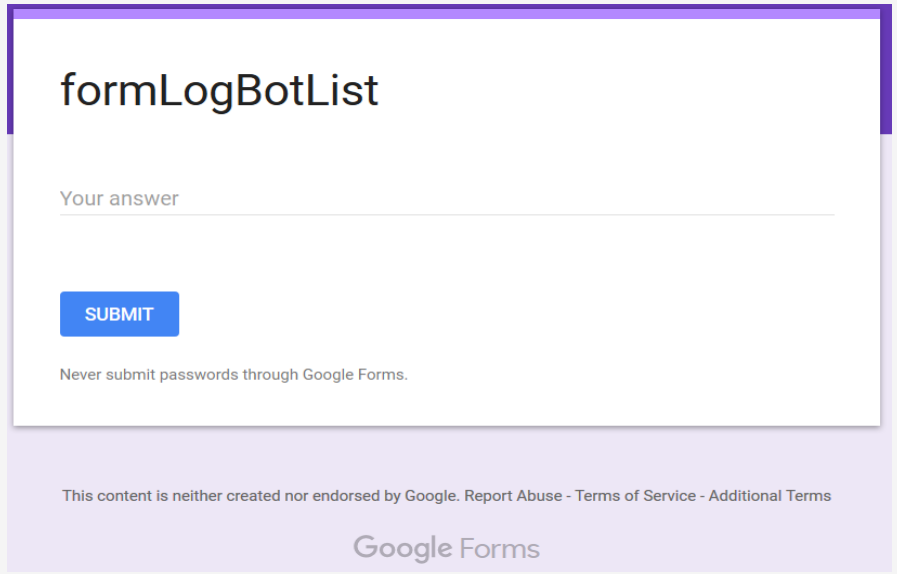
- Social engineering
- Email followed by phone call

> Good day, we would like to book rooms for our employees. 12 people will arrive in Paris on November 24. Room types attached with this email, as well as the names of employees. If you have a room available, we will make a deposit. Waiting for you reply

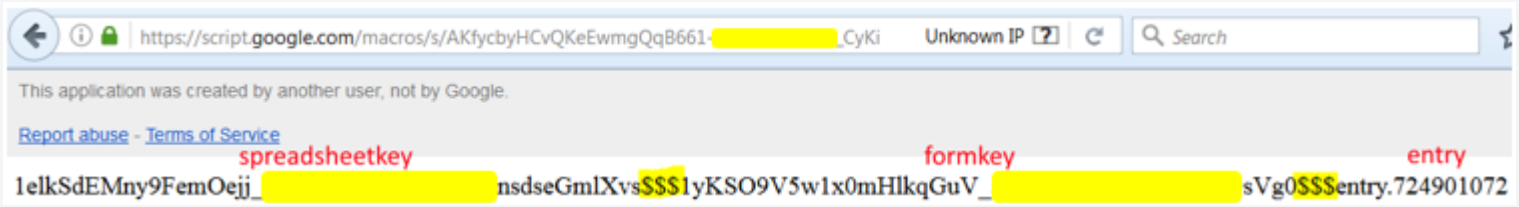


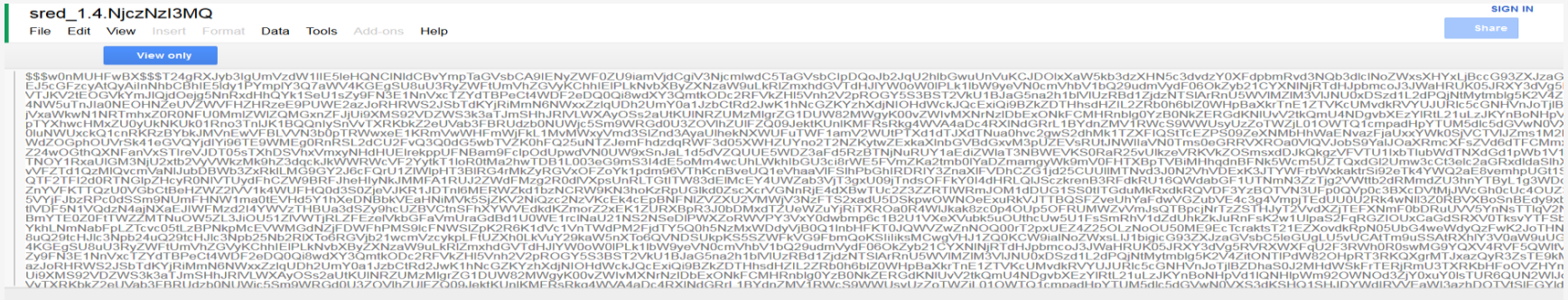
Trustworthy Services





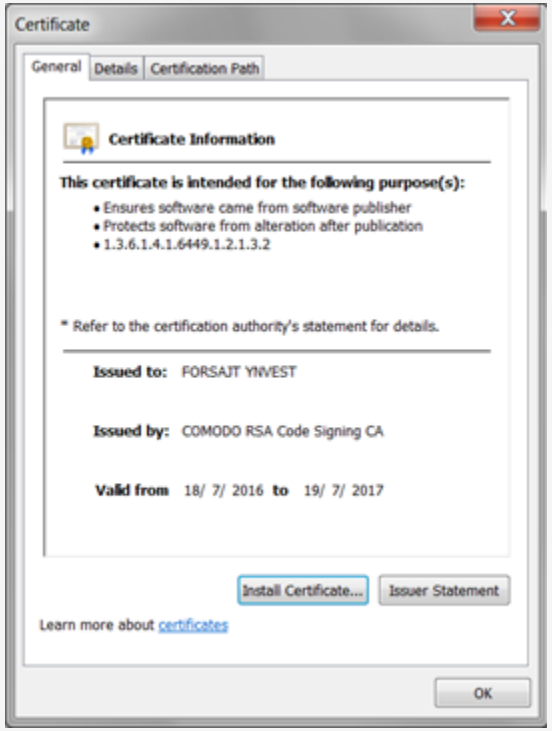
Trustworthy Services



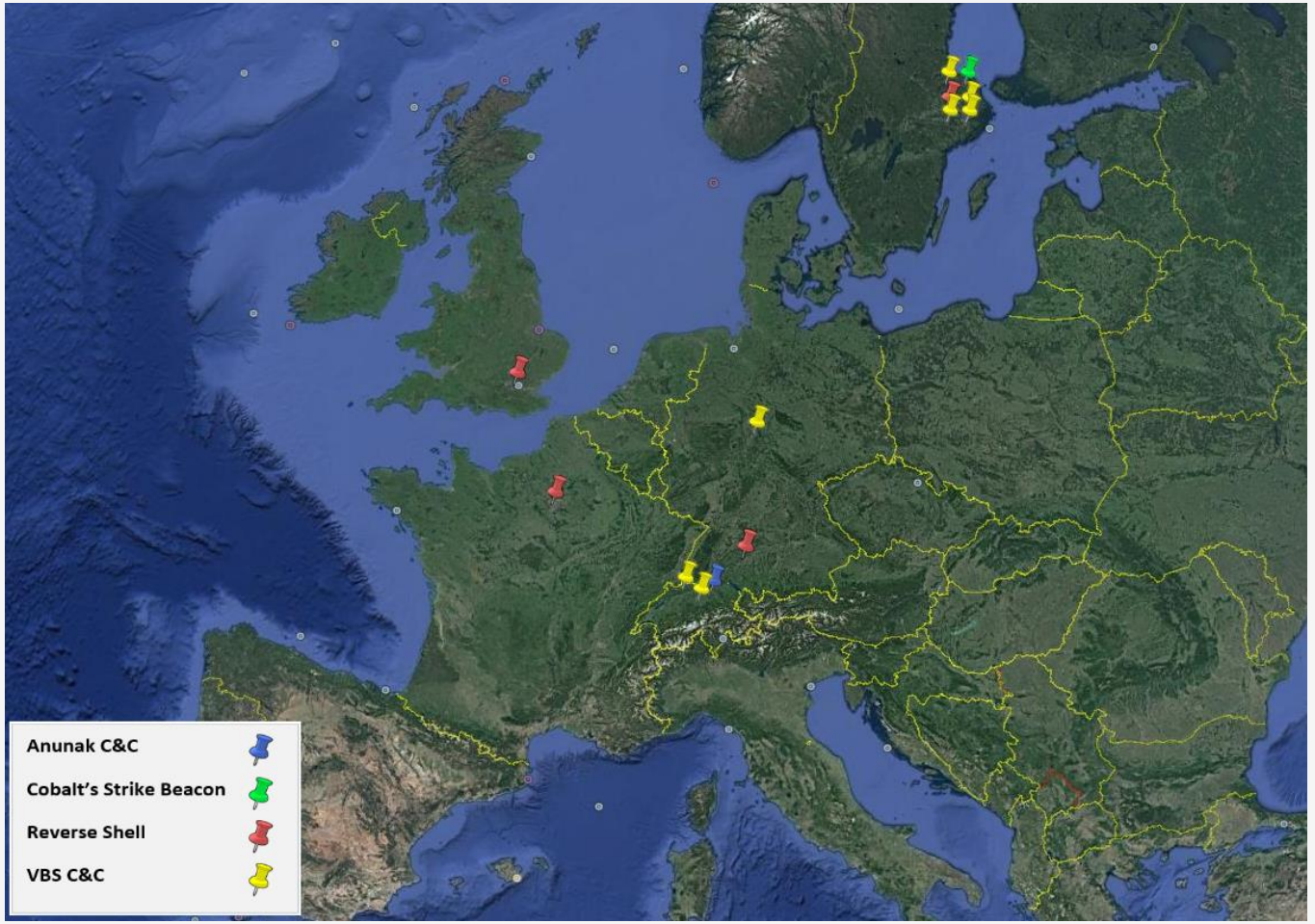


Trustworthy executables

- Spawns new svchost.exe process
- Gathers information of the system
- Anti-reversing
- Terminating specific AVs
- Privilege escalation
- Enables RDP
- POS malware functions
- Local password stealer
- Scrounging Outlook PST files
- Target iFobs banking application
- Backdoor features



Hosts distribution



Conclusions

Victims

- Weak detection security controls
- Missing or poor readiness for security incidents
- Relying on AV but detection low to zero scores

Ευχαριστώ Πολύ!