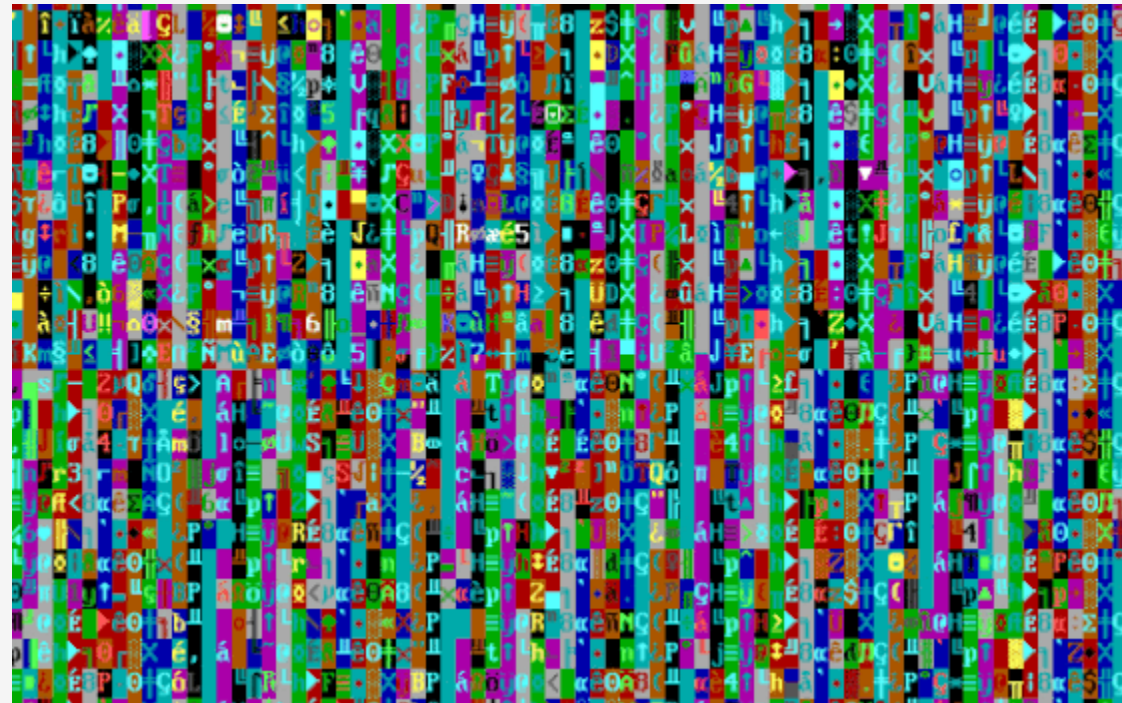


Evolution of APTs



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

Very Old Days



Very Old Days



```
AMBULC  COM          1,886 11-22-13    1:12a
Press any key to continue . . .
```

```
(continuing C:\DOS)
```

```
ASSIGN  COM          6,399 85-31-94     6:22a
CV       COM          716 85-31-94     6:22a
GRAFTAB COM         11,285 85-31-94     6:22a
HIBROR  COM         18,281 85-31-94     6:22a
HSHERC  COM          6,934 85-31-94     6:22a
PRINTFX COM          234 85-31-94     6:22a
DOSHELL COM          4,628 85-31-94     6:22a
      26 file(s)          372,682 bytes
      124,936,192 bytes free
```

```
C:\DOS>dir loadfix
```

```
Volume in drive C is MS-DOS_6
Volume Serial Number is 4912-7931
Directory of C:\DOS
```

```
LOADFIX COM          1,927 85-31-94     6:22a
      1 file(s)          1,927 bytes
      124,936,192 bytes free
```

```
C:\DOS>
```

Very Old Days



```

      YYY
      ttt
      ttt
      ttt  ttt  ttttt
      ttttt ttt  ttt
      ttt  ttt  ttttttt
      xxx  xxx  xxx  xxx
      ooooo  ooooo  ooooo  ooooo
      oooooooo  oooooo  oooooooo  oooooo

```

version A

Botnets



- Botnets
 - Command
 - Stealing
 - Abusing
 - Etc.

ZeuS :: Bots

Information:
Profile:
GMT date: 11.03.2009
GMT time: 09:26:39

Statistics:
Summary

Botnet:
→ Online bots
Remote commands

Logs:
Search
Search with template
Uploaded files

System:
Profiles
Profile
Options
Logout

Filter
Countries: CompID's:
Botnets: IP's:
Type: **Outside NAT**

Result:

#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Kill OS	Online time	Lag
1	user_1d9ce10c45_01d6e996	1.1.1.0/main	213.1.1.1	RU	213.1.1.1:38345	213.1.1.1:10051		Kill	96:13:39	0.968
2	fic_000ebb9b	1.1.2.2/main	94.1.1.1	--	94.1.1.1:1025	94.1.1.1:34451		Kill	96:32:47	0.765
3	family_01207eeb	1.1.2.2/main	86.1.1.1	GB	86.1.1.1:1027	86.1.1.1:22093		Kill	98:58:44	0.328
4	d719sf2j_0019064f	1.1.2.2/main	87.1.1.1	GB	87.1.1.1:1025	-		Kill	96:49:07	0.235
5	218_u_1_00ac3738	1.1.2.2/main	195.1.1.1	RU	195.1.1.1:1025	195.1.1.1:10359		Kill	96:27:06	0.141
6	illusion_f2243e_00576c9d	1.1.2.2/main	124.1.1.1	TH	124.1.1.1:1025	-		Kill	104:12:36	0.844
7	brian_ally_0228d16c	1.1.2.2/main	82.1.1.1	GB	82.1.1.1:1027	-		Kill	97:49:55	0.313
8	telekit_7482b02_00b07900	1.1.2.2/main	94.1.1.1	--	94.1.1.1:1025	94.1.1.1:33846		Kill	98:00:42	0.157
9	your_jaxvxjzedk_00a364bc	1.1.2.2/main	82.1.1.1	GB	82.1.1.1:1025	-		Kill	96:10:44	26.75
10	home_881b31b48d_00170f87	1.1.2.2/main	58.1.1.1	TH	58.1.1.1:1048	58.1.1.1:32353		Kill	103:14:13	1.042
11	your_	1.1.2.2/main	68.1.1.1	--	68.1.1.1:1025	68.1.1.1:17992		Kill	104:12:03	0.578
12	blackxp_000325d8	1.1.2.2/main	124.1.1.1	TH	-	124.1.1.1:47:37760	-	-	98:38:15	0.187
13	b154bc1afca840e_00397f1d	1.1.2.2/main	77.1.1.1	RU	77.1.1.1:1027	77.1.1.1:14804		Kill	104:11:25	0.078
14	xp_0051dba0	1.1.2.2/main	58.1.1.1	TH	58.1.1.1:1025	58.1.1.1:37112		Kill	97:37:17	3.938
15	desktop_02659af2	1.1.2.2/main	190.1.1.1	AR	190.1.1.1:1025	190.1.1.1:32639		Kill	107:20:49	0.657
16	davie_0085eb43	1.1.2.2/main	62.1.1.1	GB	62.1.1.1:1036	62.1.1.1:37719		Kill	96:34:49	0.188
17	1_d07192a7a4944_0025f597	1.1.2.2/main	95.1.1.1	--	95.1.1.1:1026	95.1.1.1:10385		Kill	100:53:01	3.25
18	microsof_886bea_01bd77ea	1.1.2.2/main	92.1.1.1	--	92.1.1.1:1025	92.1.1.1:10278		Kill	96:36:01	3.266
19	mircik_00069abc	1.1.2.2/main	193.1.1.1	SK	193.1.1.1:1025	193.1.1.1:2664		Kill	96:41:51	0.187
20	ammo_00135651	1.1.2.2/main	82.1.1.1	GB	82.1.1.1:1025	82.1.1.1:15589		Kill	96:31:56	0.156
21	freedom_867dc59_000050cf	1.1.2.2/main	82.1.1.1	RU	82.1.1.1:1027	-		Kill	98:18:30	0.078
22	pc_fec662b1943d_00153eae	1.1.2.2/main	86.1.1.1	GB	86.1.1.1:1027	-		Kill	104:11:26	0.15
23	pen_003f0760	1.1.2.2/main	95.1.1.1	--	95.1.1.1:1025	95.1.1.1:31003		Kill	96:39:22	0.312
24	home_	1.1.2.2/main	24.1.1.1	--	24.1.1.1:54537	24.1.1.1:27755		Kill	104:12:37	0.624
25	bsaftpz_7e2bb74_017743b0	1.1.2.2/main	89.1.1.1	HU	89.1.1.1:1025	89.1.1.1:18514		Kill	97:55:18	0.266
26	client_df77fa69_0d6210d8	1.1.2.2/main	89.1.1.1	RO	89.1.1.1:1025	89.1.1.1:38462		Kill	96:14:16	0.701
27	acer_4d30879900_004dbca2	1.1.2.2/main	202.1.1.1	TH	-	202.1.1.1:25983	-	-	97:16:11	0
28	abc_67365a4e5b6_00204191	1.1.2.2/main	115.1.1.1	--	115.1.1.1:1027	115.1.1.1:34129		Kill	98:45:29	8.437
29	skz_fd19c55e0a2_003d5664	1.1.2.2/main	61.1.1.1	TH	61.1.1.1:1025	61.1.1.1:35502		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

#	Sender Name	Sender Exchange	Recipients	Subject	Creation Date/Time - (UTC+1.00) (dd/MM)	Delivery Date/TL	Body	Folder Name	CC	B.	Attachments	Header
3957	Adam Kronz <ada...>			reserve	20/10/2016 15:58:37	20/10/2016 15:58...	<click to view>	outlook.ost -> Boil.			1-list.docx	<click to view>

Go To Page: Showing results 1 - 10000 of 51995

Details	Hex	Text	Body	Headers	Attachments
File Name					
1-list.docx					

Trustworthy Services



formFirstPingBotList

Η απάντησή σας

ΥΠΟΒΟΛΗ

Μην υποβάλετε ποτέ κωδικούς πρόσβασης μέσω των Φορμών Google.

Αυτό το περιεχόμενο δεν έχει δημιουργηθεί και δεν έχει εγκριθεί από την Google. Αναφορά κακής χρήσης - Όροι Παροχής Υπηρεσιών - Πρόσθετοι όροι

Google Φόρμες

formLogBotList

Your answer

SUBMIT

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Additional Terms

Google Forms

Trustworthy Services



<https://script.google.com/macros/s/AKfycbyHCvQKeEwmgQqB661-...CyKi> Unknown IP Search

This application was created by another user, not by Google.

[Report abuse](#) - [Terms of Service](#)

spreadsheetkey

formkey

entry

1elkSdEMny9FemOeji_...nsdsGmlXvs\$\$\$1yKSO9V5w1x0mHlkqGuV_...sVg0\$\$\$entry.724901072

sred_1.4.NjczNzi3MQ

File Edit View Insert Format Data Tools Add-ons Help

Share

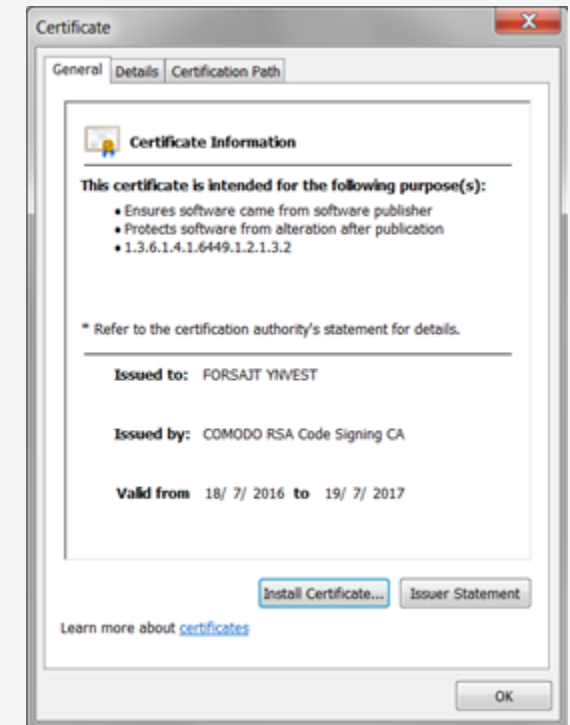
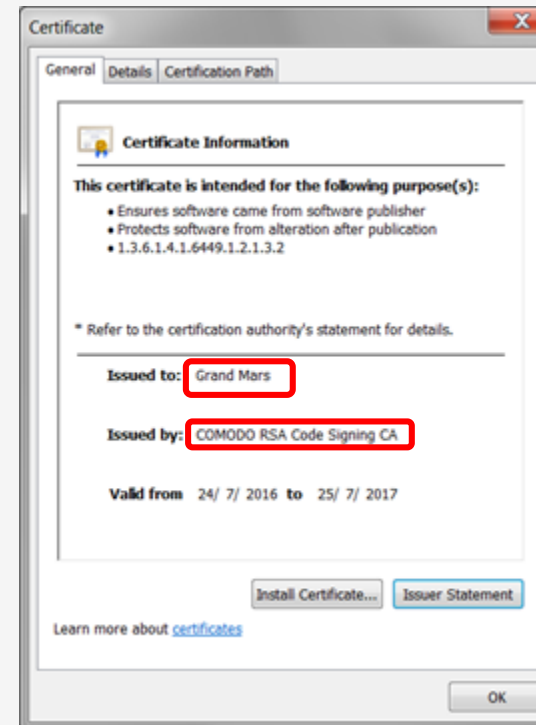
View only

\$\$\$w0nMUHFwBX\$\$\$T24gRXJyb3IqUmVzdW11IE5leHQNCINldCBvYmpTaGVsbCA9IENyZWFOZU9iamVjdCgVlV3NjcmVmdC5TaGVsbClpDQoJb2JqU2hibGwUUmVubUkCJDJOcXAw5kb3dzXHN5c3dvdzY0XFdpbmRvd3NQb3dlclNoZWxsXHYxLjBccG93ZJzaG
EJ5cGFzcYAtQyAilnNhbCBhIE5ldy1PYmptY3Q7aWV4KEgSU8uU3RyZWFIUmVhZGVyKChhIEPlkNvbXBzXNzaW9uLkRlZmxhdGVtdHJlYW0oW0lPLk1lbW9yeVN0cmVhbV1bQ29udmVydF06OkZyb21CYXNlNjRtdHJpbmcuJ3JwaHRUK05JRXy3dvG5
VTJKV2IEOGVkyYmJlQdOeJg5NnRxdhYk1SeU1sZy9fN3E1NnVxcTZydtBPecI4WDF2eDQOQI8wdXY3QmIkODc2RFVzKzH5Vnh2VzPRQGY5S3BS2VzK1BjAg5na2h1bVlUzRBd1ZjdzNTSlaRnU5WVWlZlM3VlNUU0xdSzd1L2dPQjNlMytmbgl5K2V4Z
4NW5u1nJludNEOHnzauVZWVfH4RzeE9PLWE2azJdKYPjRlMmN6NwexZziqUDh2UmY0a1JzbCIRd2JwK1fNcGZKYzhKdJNlOIdWckJcExiQ9BkZD1ThsdH2IL2ZRB0b6IZ0WHPbaK1nE1ZTVKcUImvdkRYUJURlcpcGNHvno1tjB
JxaVWkN1NR1mhZ0R0NFU0MmZWlZQMGxZFJlU9XMS92VDZWS3k3a1JmSHhJRLWXAYOSs2aUlkUINRZUMzMlgrZG1DUW82MwQyK00vZVlVlMXNnRzIdBExONKfCMHrnbgl0YzB0NkZERgdKNIUv2IkQmU4NDgVbXEZYRIL21uLzJKYnBoNhpv
pTYXhwCHmXZU0dUkNKLk01Rno3TnJk1BQOnlySnV1XRRkbK2zeUvab3FBRUdz0bNUWjC5Sm9WRGd0U3ZOVihZUIFZQ09JekIKUinKMFksRkg4WVA4adC4RXINDGR11BYdnZMV1RWcS9WVWU5vUzZoTWZJL01OWTQ1cmpadHpyT1Ub5dlc5dGvWnOV2
0uNWUjckQ1cnRkRzEYbkUjVnEwFfBLVvN3b0p1RwWxe1KRmVwWHfcmWfK11MwMwYVmd3SIZnd3AyaUJlhoNWXUJfU1WF1amVZWUFP1Xd1d1Jxd1Nua0hvc2pw52dHk11ZXFIQStfctZPS00ZaXNlBhWaeNwafFjaluxsYwK05YVC1VJZms1M2l
WdZOGphOUvSk41eGQYjdIY06TE9WMEg0RnRSL2dCU2FvQ3Q0dG5wbTVZK0hFQ25uN1ZJemFhdzdgRWF3d05XWHZUyno2T2NZkywZEKxaXnbGVbD6Gxm3pUZEVSaRUJNWilaVNO1Tms0eGRRVXROa0VlQVJobs59YalUOaXRmcXfzZv06dTFcMm
Z24wOGhGQXNFanVasStIreVJD105sTXhDSVhxVmxYNhdHUEIreKppUfNBam9FclpOdUj25vNDOUW9XSnJal1d5dvZQUJUE5W0D3aF45RzB1NjNUUY1aEdIzWla13NBWEVKSORaR25vUlkzeVRKvKZOSmsxdDJKgkzvFVU11kpb1ludVldTNXAgd1pVb1V1
TKOY1RxaUJGm3nU2xbZVWwKcm0h3dckckJwWRkVcF2YyK11l6R0lMa2hWTD01L003eG9mS34dE5oMpm4wchLWkhbGU3c08WESFVmkza2tmb0lYabZmamoyWk9mV0fHXBP1VbMHhqdmbFKsWcm5U1Z1QxdG2Ulmw3cct3ek2aGRxdlas1b
VVFzTd1Q2MIQcmVaNlubbDBWb3ZKRklMG9GY2J6cFQrU1ZlWpHT3BIRG4fMkzYRGvXOFZoyK1pdm96V1ThKcnBveUQ1eVhaaVIFSlhPbGhIRDRY32naXlFVdNCZG1jd25CUUIMTNvd3J0N2VhVDExK3JTYWFrbWxaktrSi92eTk4Y7WQ2AE8vemppUGH5
Q1TF21F2d0RTNGlp2HcyRONIV1UydfHCZW9BRFJheHlyNkIMMFA1RUJ2ZWdMzg2R0dVXpsUnkRLTG1TW83dE1McEY4UWZab3V139u091TndsOFFKY014dHRLQJSczkren3FRdkRU16QWabGF1UTNmNSZ1Jp2VWtlb2dRmmdZ03hNYTBYL1g3WDX
ZnYVFKTTQZUOVGbcIBehZWZ2V1V1k4WUHFHQ0d3S0ZjeVJKR1JDTn0MERWZkd1bZNCRW9BK3hoKzRPUgIkD0ZscXciVGNnRJE4dXBwTUc2Z3ZRTIWRnJmQ1dDUG1SS01TgduMKRkdkRCQVDF3YzB0TVN3UFP0QVpdc3BXCdVMlJWcShocUc4OUZ
5VYfJbzRPcdSSm9NlUmfHNW1ma0IEVhd5Y1hXeDNBbkYeAHNlMVks5JkV2NIQzc2NzVKEk4cpeBNINIZVZXU2VMWVJ3NzfTS2xadU5DSkpwoWN0eExuRkvJ1TBQSFzveUhyaf-dwvGzUbVE4c3q4VmpjTEduU0JZrk4wNl3ZDRBVXBoSnBEdy9xt
lVDF5N1VQdn4aNXaEJlWFmxd214YVWzTHBua3dsZy9hUzBVctnSFhYwVEdkdKZmorZ2KkE1ZURXbR3J0bDMkdZUeWZyurRTXROa0RwHJkak8c0pQ0Up5OFUJWZVvmls0TbpcJn1T2S1HJyT2VvdKZTEFXnmf0bDruUv5YnNsT1Rv2
BmYTE0Z0FTWZMTNuOW5ZL3JlOU51ZlVW1JRLZFZeZvKbGFAvMuraGdBD1UOWE1rc1NaU2INSZSeDlPWVXZorWVWPY3VxY0dwmp61B2U1VXxeXVubk5uOUtheUw5U1F5sMRhV1dZdUhhKZJuRnfAkZw1Ulpas2FqRGZIOUXCaGdsSRXV07ktsvYTFSt
YkhlNmNabfPL2tcv05LzbPNkpMcE5VWVGdNZJFDWFhPMS0lcFNWSZpKZRoK1dvc1Vn1WdpM2fjdTY5c0h5NzMXwDdyVjB0Q1lnbHFKTQJQWVzwZnNOQ00rT2pxUEZ4Z250LzNoOU50ME9EcTcraktsT21EZxovdkRpN05lUbG4waWdyQzFwK2J0THN
BuQ29tcHJk3Npb24uQ291clHJk3Npb25Nb2RlXToRqVb21wcmVzcycpLFIUZXh0LkVvY29kaW5hXToQVNDNSUpkKSSZWfKvG9FbmQoKSillikeMcwplU11ZQ0KcW9iaNoZWxsL11b9jG83ZXJzaQVsb35leGUglU5vUcA1TmkuSSARXdy3V0aW9uUG
4KGEgSU8uU3RyZWFIUmVhZGVyKChhIEPlkNvbXBzXNzaW9uLkRlZmxhdGVtdHJlYW0oW0lPLk1lbW9yeVN0cmVhbV1bQ29udmVydF06OkZyb21CYXNlNjRtdHJpbmcuJ3JwaHRUK05JRXy3dvG5RVRXWfXQ2F3RWWh0R0swWGBY94VRF5QWlV
Zy9fN3E1NnVxcTZydtBPecI4WDF2eDQOQI8wdXY3QmIkODc2RFVzKzH5Vnh2VzPRQGY5S3BS2VzK1BjAg5na2h1bVlUzRBd1ZjdzNTSlaRnU5WVWlZlM3VlNUU0xdSzd1L2dPQjNlMytmbgl5K2V4Zl0lNTlPdw82OHpRT3RKQXgrMtJxazGYR3ZsTE9kA
azJdKYPjRlMmN6NwexZziqUDh2UmY0a1JzbCIRd2JwK1fNcGZKYzhKdJNlOIdWckJcExiQ9BkZD1ThsdH2IL2ZRB0b6IZ0WHPbaK1nE1ZTVKcUImvdkRYUJURlcpcGNHvno1tjBZDhaS0J2MhdW5Kf1TERfmlt3JXRkbHfcoQYHn
Uj8XMS92VDZWS3k3a1JmSHhJRLWXAYOSs2aUlkUINRZUMzMlgrZG1DUW82MwQyK00vZVlVlMXNnRzIdBExONKfCMHrnbgl0YzB0NkZERgdKNIUv2IkQmU4NDgVbXEZYRIL21uLzJKYnBoNhpvdtIQNHlpWm92OWNOd3Z1Y0xuY0lStUR6QUINZWLk
VVTXRRkbZ2aUvab3FBRUdz0bNUWjC5Sm9WRGd0U3ZOVihZUIFZQ09JekIKUinKMFksRkg4WVA4adC4RXINDGR11BYdnZMV1RWcS9WVWU5vUzZoTWZJL01OWTQ1cmpadHpyTYUIM5dlc5dGvWnOVX53dKSHQ1SHJlYDwldRVFw1JazhD0TVISIEGYld

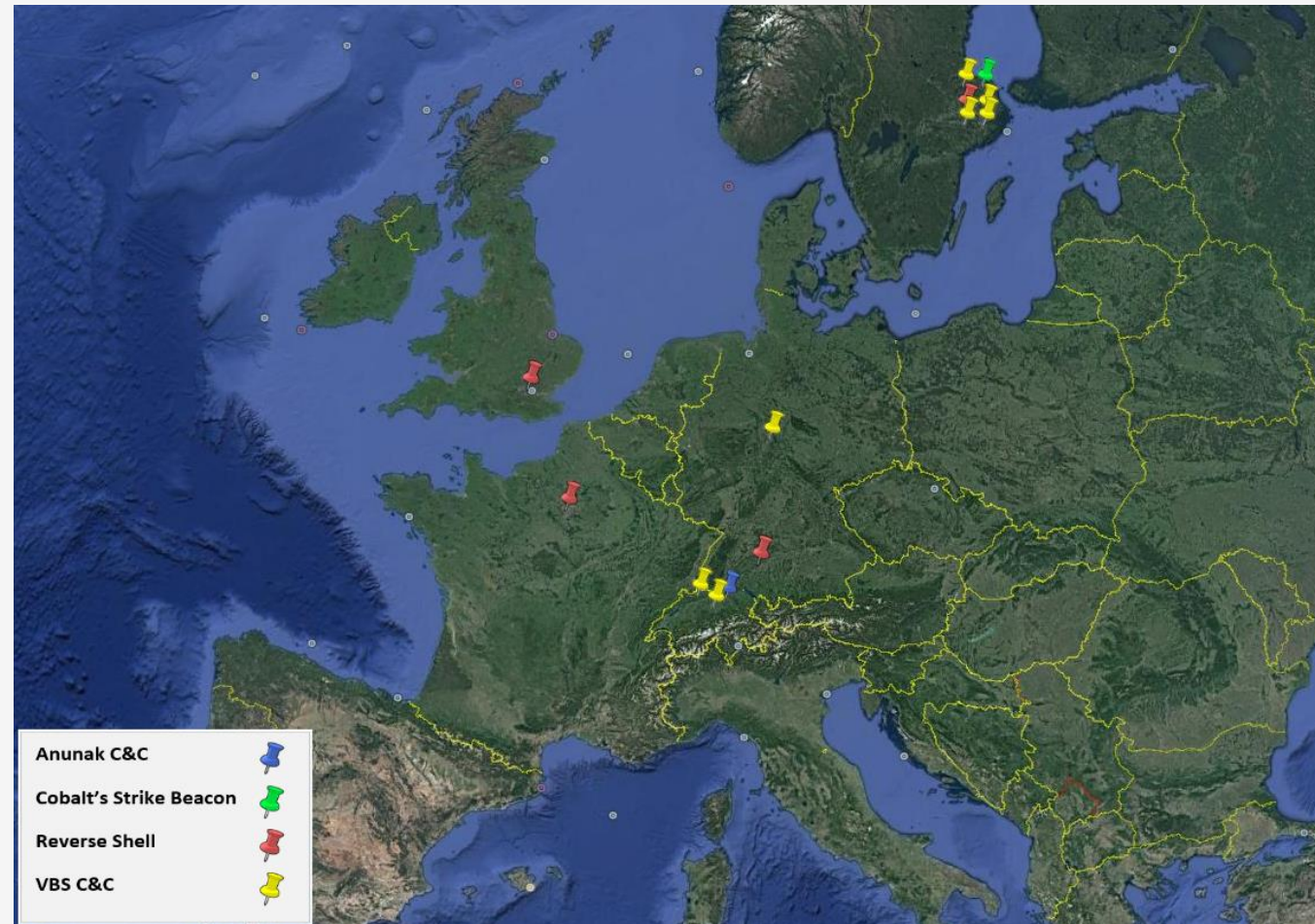
Trustworthy executables



- 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!

