BfV Bundesamt für Verfassungsschutz

16th NATO Cyber Defence Workshop

05.05 – 07.05.2015

Berlin, Germany

Infrastructure of RIS Cyber Campaigns

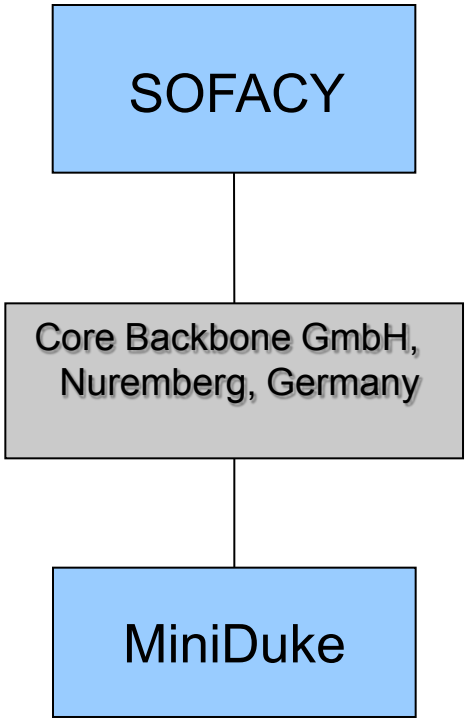
Major Russian Campaigns

- Sofacy / Sednit
  - Governments (APEC / G20), MFA / Embassies, NATO, Defence Industry, Energy Sector, „Ukraine“
- Energetic Bear / Havex / Dragonfly
  - Energy Sector, Military, Aerospace, SCADA / ICS-Industry,
  - Biotechnology and Pharma-Industry
- MiniDuke / CosmicDuke /OnionDuke
  - Government, MFA / Embassies, Research, Military,
  - Defense Industry, Telecommunications, Security Authorities
  - *Malware shows „mirea.ru“ in source code (Moscow State Institute of Radio Engineering, Electronics and Automation)*
- Black Energy / Sandworm
  - Governments, Research, NATO, Energy Sector, Telecommunications
- Snake / Uroburos (Wipbot)
  - Governments, MFA / Embassies, Research

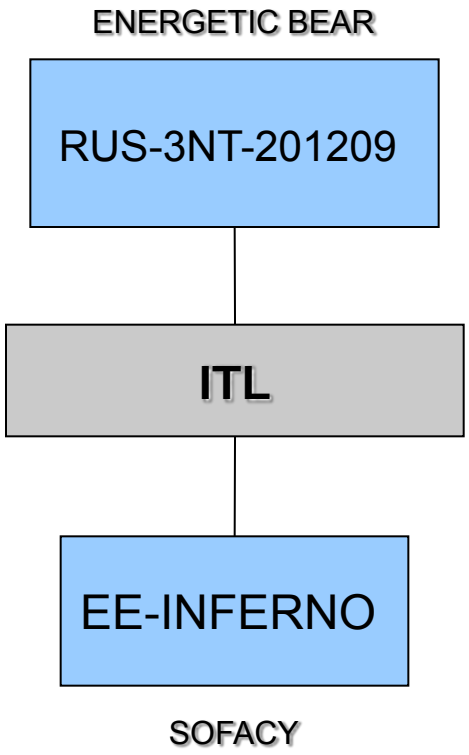
Links between Campaigns: SOFACY & SNAKE

- Sofacy: ns1.carbon2u.com / ns2.carbon2u.com
  - Only Sofacy-Domains and Cyber Crime Domains
  - Coincidence?
- Snake: carbon.dll

Links between Campaigns: SOFACY & MiniDuke



SOFACY & Energetic Bear



ISP ITL

Netrange:	185.4.66.0-*.*.67.255
Netname:	RUS-3NT-201209
	Moscow, VPS/VDS services
MNT-BY:	MNT-3NT
MNT-ROUTES:	AZ62969-mnt
Changed:	**snoop@itl.ua**
Person:	Neil Young
Address:	3nt Solutions LLP, UK
Tel.:	+44 20 8133 3030
Email:	info@3nt.com
Origin:	AS6870

Information Technology Laboratories	Integrated Technology Laboratory LLC
Homepage: itl-g.com	Homepage: itldc.com
USA: West Broadway 600, San Diego, CA 92101	USA: West Sahara Ave unit 223, Las Vegas
Canada: 1 Yonge St., Toronto	Bulgarien: building A, Zornitsa district Suite 1, Sunny Beach, Nessebar, +359 **56** 916881
Bulgarien: building A, Zornitsa district Suite 1, Sunny Beach, Nessebar, +359 89 3705168	Ukraine: Kosmichna street, 26, Kharkiv, +380 57 7630004
Ukraine: Kosmichna street, 26, Kharkov, +380 57 7630004	Czech Republic: Pobrezni 95/74, Praha 8, Karlin, +420 228 880 286

Links between Campaigns: SOFACY & Cyber Crime

- SOFACY DNS
  - Webkevlar.net
  - Used as DNS-Server in internet scam in 2013
    - BTC-ARBS.COM (HYIP)

Links between Campaigns: SNAKE & Bladabindi

- Connection between SNAKE and BLADABINDI (Cyber crime)
  - String “dragifart” in URLs of SNAKE and BLADABINDI
    - easycounter.sytes.net**/?dragifart** SNAKE
    - sajad.no-ip.org**/?dragifart** BLADABINDI

Links between Campaigns: Snake & Miniduke

- Connection between SNAKE and MINIDUKE
  - User names for FTP authentication
    - erika SNAKE
    - upgor SNAKE & Miniduke
    - dlgor SNAKE & Miniduke

Links between Campaigns: SNAKE & Energetic Bear

- New trend in Modus Operandi
  - Use of “FREE” Webspace instead of or additionally to DYNAMIC DNS
- 31.170.160.149 tiger.netii.net "SNAKE"
- 31.170.160.209 nightday.comxa.com "SNAKE"
- 31.170.161.136 winter.site11.com "SNAKE“
- 31.170.162.163 *.net76.net "New Campaign (?)"
- 31.170.167.168 google.zzux.com “Energetic Bear"

- 000Webhost.com = comxa.com = netii.net = site11.com
- All belong to Hostinger -> Cyprus

Possible Link between RIS and SEA

- Spear pishing pages of SEA attacks hosted on 000webhost
  - Same used subnet as in RIS-Campaigns
    - 31.170.160.73
    - 31.170.160.96
    - 31.170.160.97
    - 31.170.160.100
    - 31.170.160.112
    - 31.170.163.246
    - 31.170.163.247
    - 31.170.163.248
    - 31.170.163.249
    - 31.170.163.251
    - 31.170.163.253

Links between Campaigns: ILDUS D. NURIEV