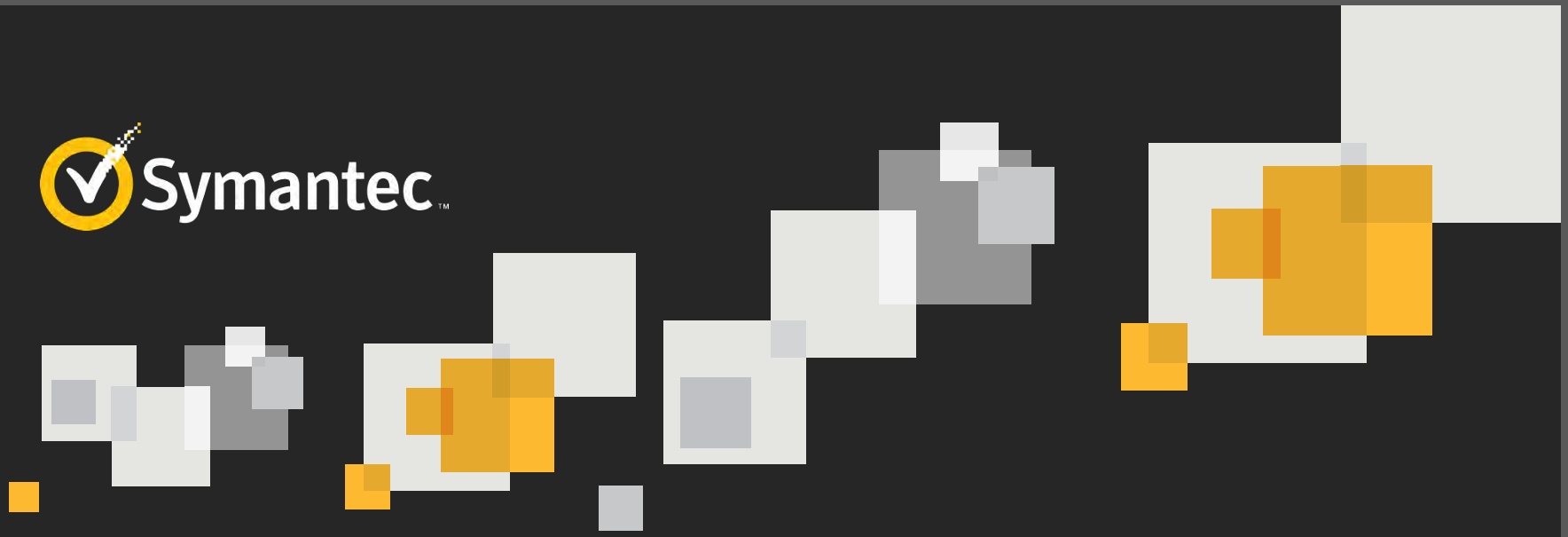


CosmicDuke

Stephen Doherty

Senior Threat Intelligence Analyst

CosmicDuke Agenda

1	Identification
2	Tools, Tactics, Procedures
3	Target Profile
4	Attribution

Identification

Identification

- F-Secure, July 2, 2014
  - CosmicDuke: Cosmu With a Twist of MiniDuke
    - Used Miniduke Stage III Loader, March 2011
    - Attacks against NATO and European government agencies
- Backdoor.Tinybaron (Symantec Detection)
  - Observed in Spear-Phishing attacks since 2010
    - PDF Exploit document CVE 2010-2883
    - Subject: “Press release MFA TJ”

➢ Advisory:	September 8th,	2010
➢ Spear Phish:	September 16th	2010
➢ Patch :	October 5th	2010

  - Earliest variants identified by Symantec data circa 2008

Tools, Tactics, Procedures

Symantec.

Infection Vector

Tools, Tactics, Procedures

Spear-phishing email:

- Typically Politically themed content
- PDF Documents (2011 – 2014)
  - CVE-2010-2883 (Adobe Reader)
  - CVE-2011-0611 (Adobe Flash)
- Word Documents (2015)
  - CVE-2014-0569 (Adobe Flash)
- Right-To-Left-Override (RTLO)
  - Adjust Icon to appear like the “real” document

Infection Vector

Tools, Tactics, Procedures

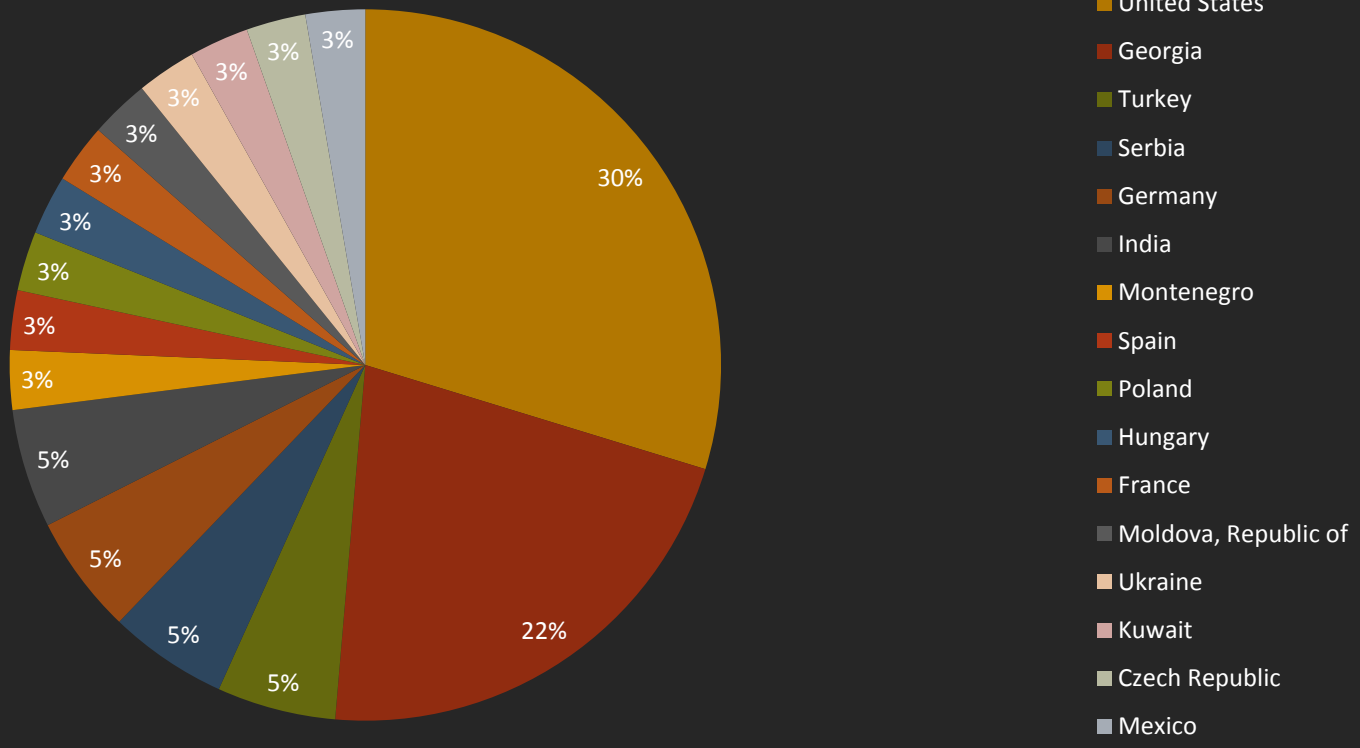
Politically Themed Subject Matter
12th Annual International Conference on Politics & International
DSEi 2013
ESSHBS-2013
Fwd: DSEi 2013
Fwd: ESSHBS-2013/2014
Fwd: FW: pomogite naiti brata
IMDi Report 2010 - Looking at Islam as a danger
Press release MFA TJ
Russias Terrorism: Putins best choice (analytic report for non-partisan organisations)
SOCAR and Nabucco Consortium meeting agreement (draft)
Vesma srochno

Target Profile

Symantec.

Geographic Distribution

Target Profile



Target Industries/Sectors

Target Profile

Target Industry/Sectors		
Policy	Legal	Accountancy
Human Rights	Government	Research
Military/Defense	Manufacturing	Information Technology
Media	Travel	Mining
Energy	Public Relations	Charity

Attribution

Symantec.

Debug Strings
Attribution

Authentication

- HTTP uses authentication

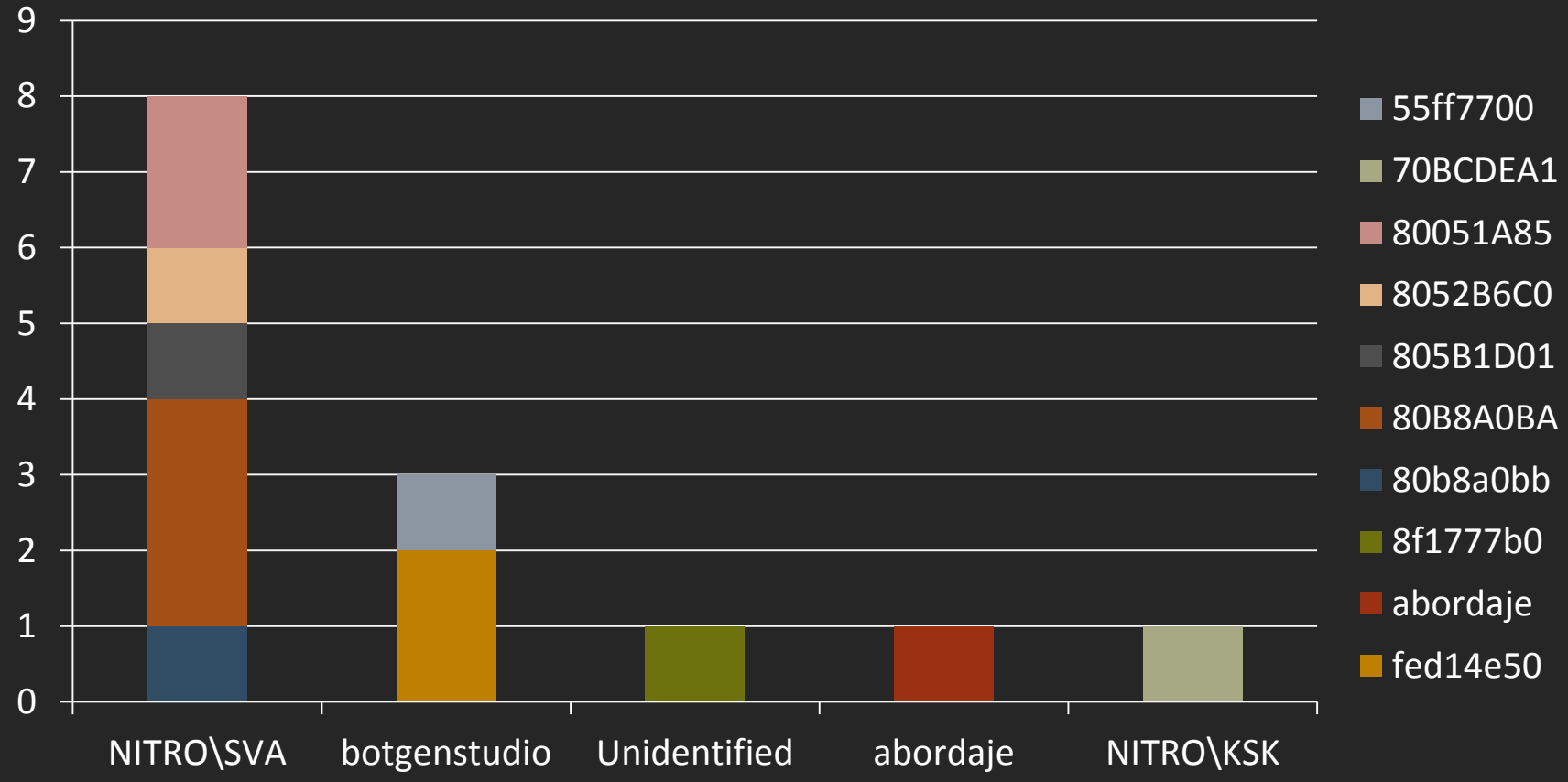
- D:\PRODUCTION\NITRO\SVA\Generations\80B8A0BA\bin\bot.pdb

HTTP Request (2014)

- http://46.246.120.178/modules/db/mgr.php
  - **Auth=80B8A0BA**
  - **Session=11E05099D1D99695**
  - **DataID=100**
  - **FamilyID=C3491B41C10145D191BE0990082EAB3E**

Debug Strings - Actors

Attribution



Debug Strings - NEMESIS

Actor Attribution

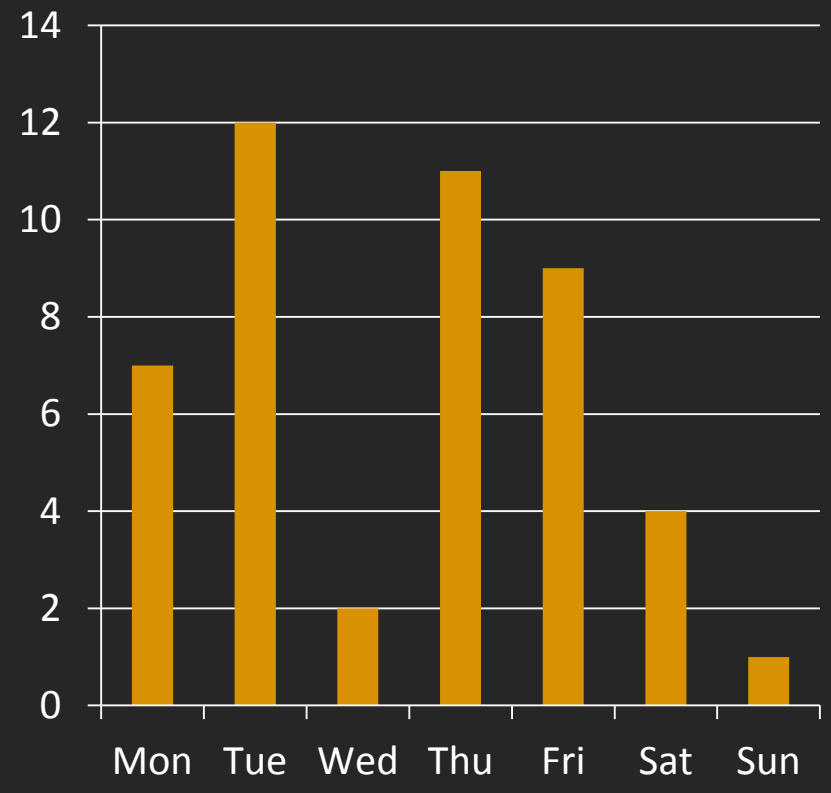
Custom Packer (Private)

- C:\Projects\NEMESIS\nemesis-gemina\nemesis\bin\carriers\ezlzma-boost-karma_x86_exe.pdb
- C:\Projects\NEMESIS\nemesis-gemina\nemesis\bin\carriers\ezlzma_x86_exe.pdb

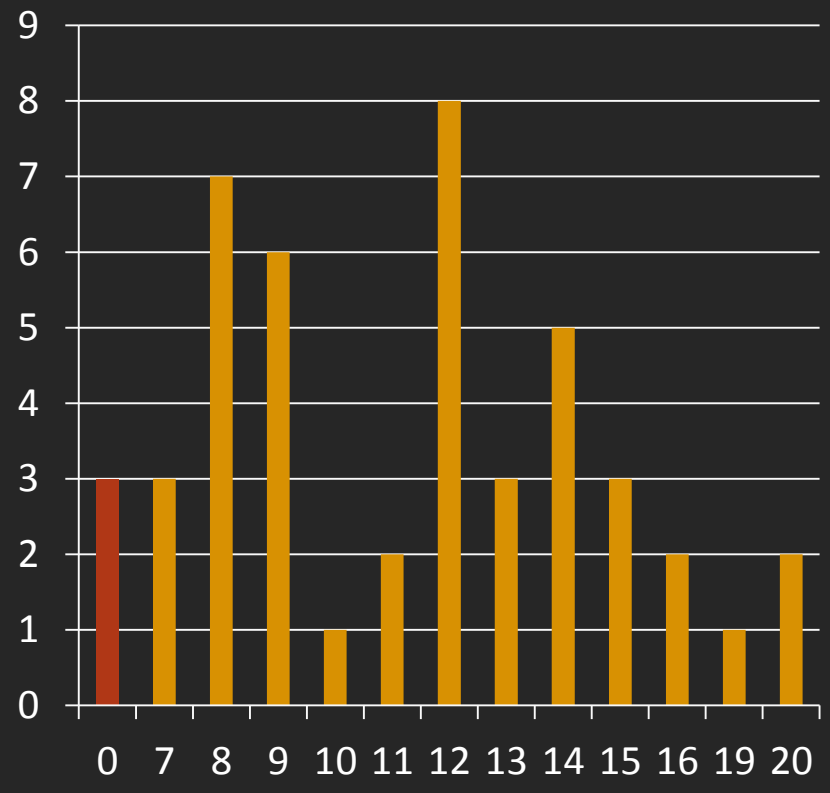
- Cosmic Duke Actors using it?
  - NITRO\SVA
  - NITRO\KSK
- NITRO\SVA and NITRO\KSK also share C2 infrastructure
- NEMESIS is also used by… Miniduke

Days of the Week – Compilation Timestamps

Days of Week



Time of Day(UTC)



Did developers leave a clue?
Attribution

- Memory Artefacts (Kaspersky)
  - **www.mirea.ru**
  - **e.mail.ru**
  - **gmt4**
  - **c:\documents and settings\владимир\local settings\...**
- Moscow State Institute of Radio Engineering, Electronics and Automation
  - Radio technology
  - Electronics
  - Cybernetics
  - Automation

Q&A