PROC

Visual Malware Analysis

Christian Wojner, CERT.at

Wh01am

Person

- Christian Wojner
- Malware Analysis, Reverse Engineering, Computer Forensics
- CERT.at / GovCERT.gv.at

Publications

- Papers
  - Mass Malware Analysis: A DIY Kit
  - An Analysis of the Skype IMBot Logic and Functionality
  - The WOW-Effect
- Articles
  - HITB Online Mag
    - The Art of DLL Injection
    - Automated Malware Analysis - An Introduction to Minibis
  - HAKIN9 Online Mag
    - Minibis
- Software
  - Minibis
  - Bytehist (REMnux)
  - Densityscout (REMnux)
  - ProcDOT (REMnux)

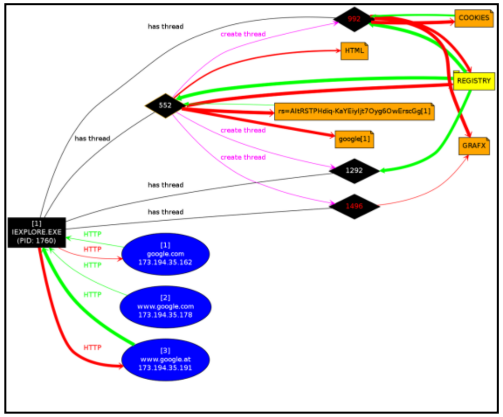
Speaker

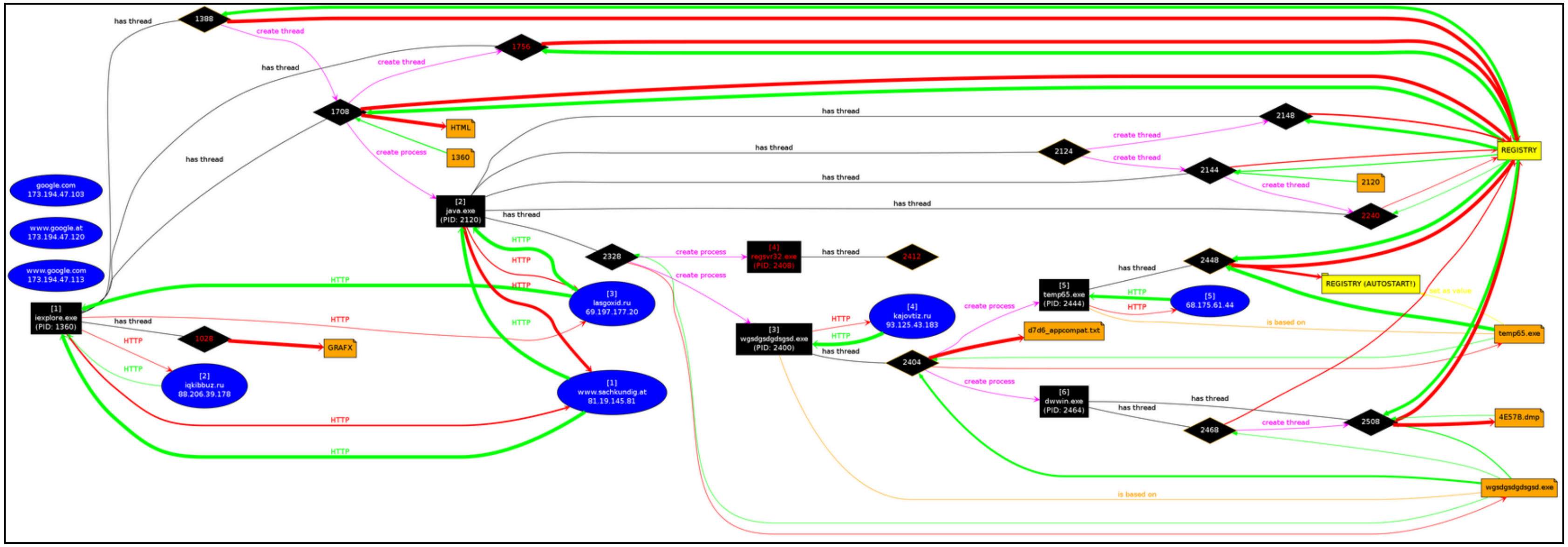
- FIRST Symposium 2010
- CertVerbund-DE 2010
- Deepsec 2010
- Teliasonera 2011
- Joint FIRST/TF-CSIRT Technical Seminar 2012
- CanSecWest 2012
- CertVerbund-DE 2012
- 0ct0b3rf3st 2012
- SANS Forensic Summit Prague 2012
- Deepsec 2012

I had a dream …

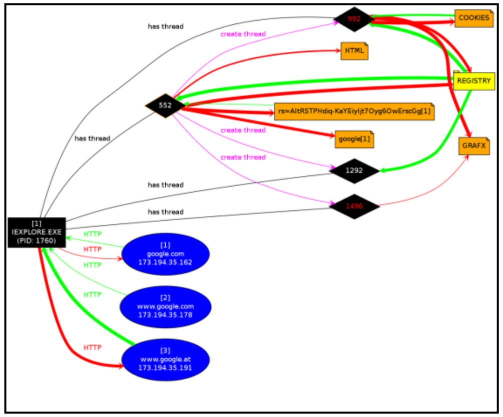
- Malware infections are complex
- Humans are visually oriented
- Pictures tell a 1000 words
- Humans are top in understanding complex pictures
- Goal: Put all aspects of a malware infection in one big picture using the most common of freely available tools
- Goal: Distinguish between good/evil with a glance
- Goal: Gut feeling for an entire situation within minutes
- Goal: Freely available to everyone

Proof of concept



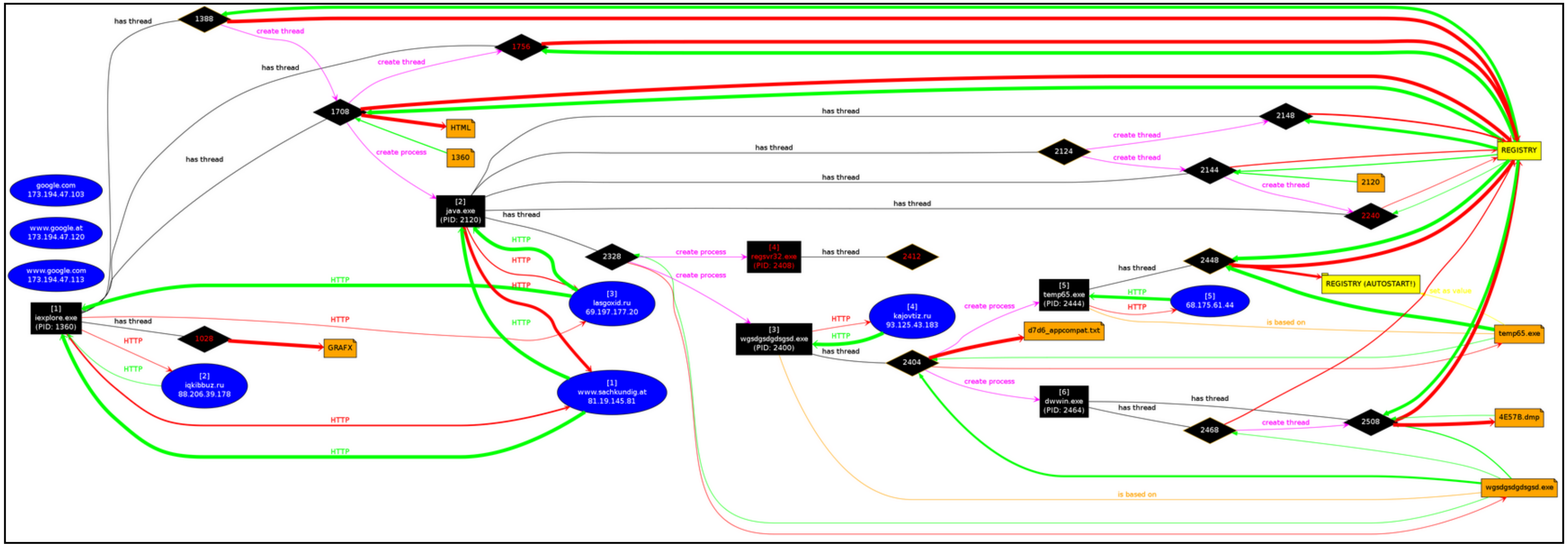


Proof of concept



GOOD

EVIL



ProcDOT – The name

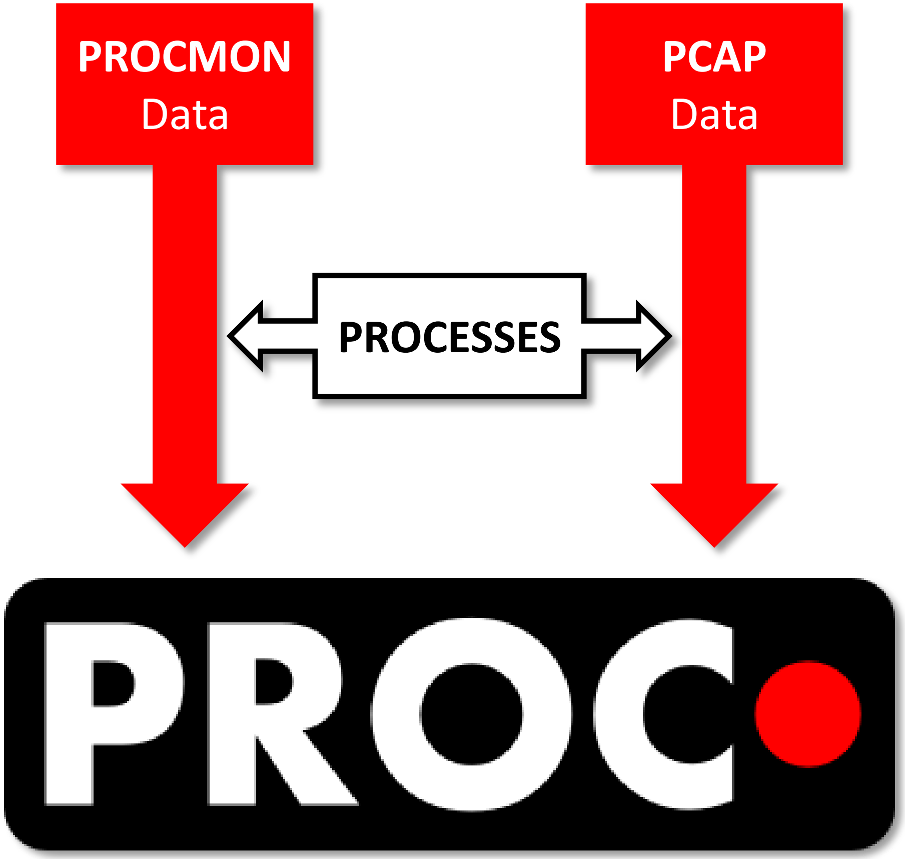
- Proc ...
  - Process Monitor (Procmon) from Sysinternals
- DOT ...
  - DOT module of the Graphviz Suite

Behavioral analysis

- Monitoring activities

Activity	Procmon	PCAP (Windump, Tcpdump, Wireshark)
Filesystem	✓	✗
Network	✓	✓
Windows Messages	✗	✗
Registry	✓	✗
Process-Management	✓	✗
Thread-Management	✓	✗

Data-Correlation

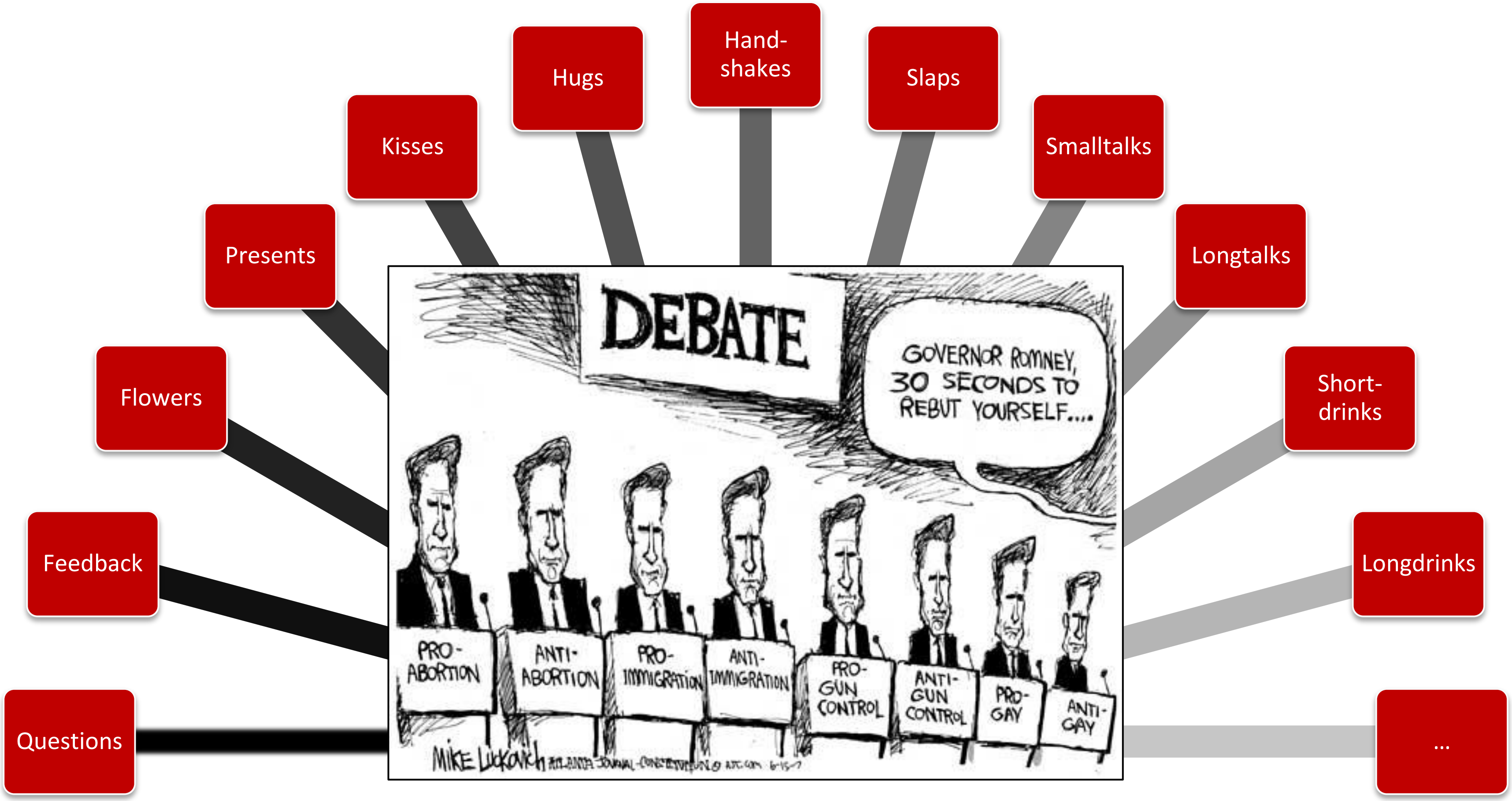


Noise (-reduction)

- Relevance: Smart-Following-Algorithms
- Paths
- Compression
  - Registry
  - Files
  - Networktraffic
- Filters
  - Files
  - Registrykeys
  - Servers
  - (Longnames/Shortnames)
- Contents
  - Nodes
  - Edges

LIVE DEMO

Reactions?



Questions

Feedback

Flowers

Presents

Kisses

Hugs

Hand-shakes

Slaps

Smalltalks

Longtalks

Short-drinks

Longdrinks

…

asko
bayarlalaa
thank
agat
you
tänan
väga
mersi
terima
salamat
leat
dziakuju
siyabonga
gracias
hvala
kiitos
vinaka
kakhulu
misaotra
tack
diolch
muchas
asante
lava
sagolun
díky
obrigada
motashakkeram
merci
wel
dankewol
takk
arigatô
khob
mauruuru
raibh
obrigado
mochchakkeram
dankie
nirringrazzjak
spacibo
paldies
hajr
kyay
grazie
hamnida
tau
spas
graciñas
tin
gràcies
dhanyavad
kha
gratias
chnorakaloutioun
maith
tapadh
dank
faleminderit
sag
aciu
mèsi
kam
dhanyabaad
blagodaram
milesker
köszönöm
diakuiu
xièxie
chokrane
multumesc
ngiyabonga
gratzias
teşekkür
mahalo
eskerrik
edirem
nizzik
sah
dankon
chai
khun
mamnun
olun
ago
dziekuje
dakujem
blagodaria
go
kop
danke
sana
thint
faafetai
kasih
dekuji
grazzi
tzu
ederim
çox

Website:
http://www.cert.at/downloads/software/procdot_en.html

News:
https://twitter.com/ProcDOT

Forum:
https://groups.google.com/forum/#!forum/procdot

Contact:
team@cert.at