Malware Retooled

Moving away from purpose built platforms (Zeus, SpyEye) to general tools (Sunspot) to target specific industries.

Agenda - General

- Revisited – Old Malware
  - Zeus, SpyEye, etc
- Retooled – New Malware
  - Sunspot aka Ambler/NetHell
- Malware Analysis – what malware looks like
- Clustering and Visualization
- Q & A

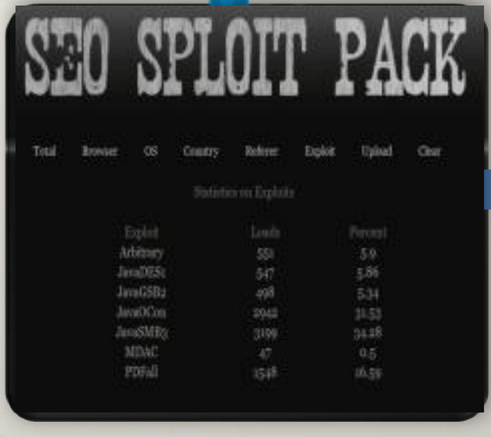
Crime Packs vs. Malware

Starts here - You’re the Manager

- Offered through black market
- Feeds malware business
- Exploit packs, botnet

Ends here – PWNED

- Fake AV, Malicious PDF’s or attachments, Hacked Websites, Social Media outlets allow the bad guys to get in.

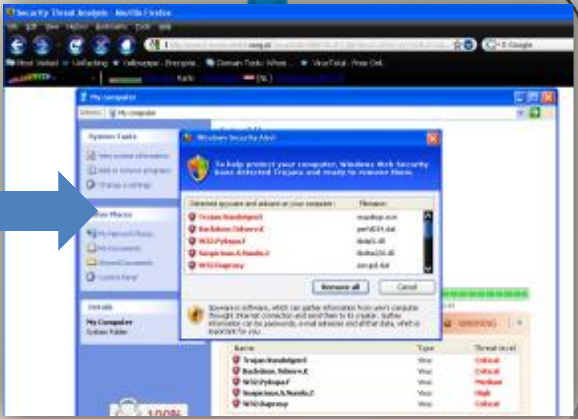


SEO SPLOIT PACK

Total Browser OS Country Referer Exploit Upload Clear

Statistics on Exploits

Exploit	Loads	Percent
Arbitrary	551	5.9
JavaDES1	547	5.86
JavaGSB2	498	5.34
JavaOCon	2942	31.53
JavaSMB3	3199	34.28
MDAC	47	0.5
PDFall	1548	16.59



Security Threat Analysis - Mozilla Firefox

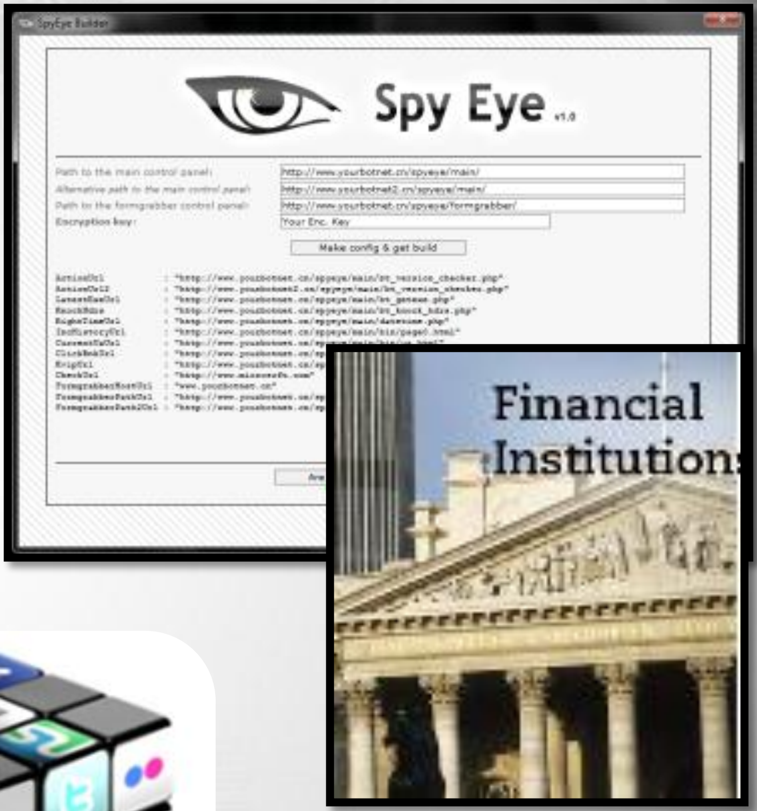
Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Revisited - Malware

Zeus & SpyEye

- Behavior
  - Trojan
  - Banking
- Infection Point
  - Web Browser
- Origin
  - Crime Packs (CrimeWare)



Path to the main control panel: http://www.yourbotnet.cn/spyeye/main/
Alternative path to the main control panel: http://www.yourbotnet2.cn/spyeye/main/
Path to the formgrabber control panel: http://www.yourbotnet.cn/spyeye/formgrabber/
Encryption key: Your Enc. Key

```
ActiveUrl             : "http://www.yourbotnet.cn/spyeye/main/bt_version_checker.php"
ActiveUrl2            : "http://www.yourbotnet2.cn/spyeye/main/bt_version_checker.php"
LatestExeUrl          : "http://www.yourbotnet.cn/spyeye/main/bt_getexe.php"
KnockBdrs             : "http://www.yourbotnet.cn/spyeye/main/bt_knock_bdrs.php"
RightTimeUrl          : "http://www.yourbotnet.cn/spyeye/main/datetime.php"
InoHistoryUrl         : "http://www.yourbotnet.cn/spyeye/main/bin/page0.html"
CurrentVeUrl          : "http://www.yourbotnet.cn/sp
ClickBakUrl           : "http://www.yourbotnet.cn/sp
KripUrl               : "http://www.yourbotnet.cn/sp
CheckUrl              : "http://www.microsoft.com"
FormgrabberHostUrl    : "www.yourbotnet.cn"
FormgrabberPathUrl    : "http://www.yourbotnet.cn/sp
FormgrabberPath2Url   : "http://www.yourbotnet.cn/sp
```

Malware Behavior Traits

Common To Both

DLL Hooking/Injection

Disable AV/Firewall

Dynamic Process – (random file names)

AutoRun –

(registry mod)

SpyEye

Function Hashing

Custom Obfuscation

Plugin Driven

Kill Zeus

Kill AV

Zeus

Packer

Later

Vista/7 aware

Support for FireFox

Zeus Code - Exposed

ZeuS Killer code This is the C++ source code for the Zeus Killer #include <windows.h> #pragma warning(disable : 4005) // macro redefinition #include <ntdll.h> #pragma warning(default : 4005) #include <shlwapi.h> #include <shlobj.h> void GetZeusInfo(ULONG dwArg, PCHAR lpOut, DWORD dwOutLn, PCH M_HANDLE_INFORMATION shi = 0; NTSTATUS Status = 0; ULONG len = 0x2000; P DLE proc = 0, thandle = 0, hFile = 0; BOOLEAN enable = FALSE; UCHAR nhttp://www.opensc.ws/trojan-malware-samples/9634-c-zeus-killer-source.htmlame[300] = {0}; ULONG temp = 0, rw = 0; do http://www.opensc.ws/trojan-malware-samples/9634-c-zeus-killer-source.html

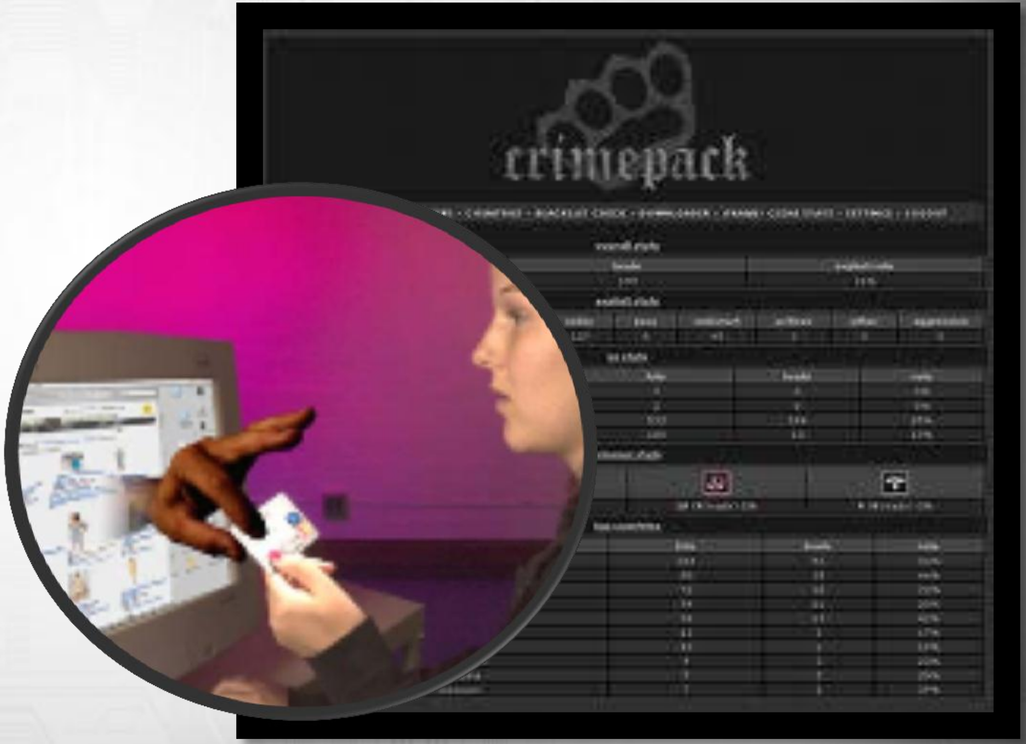
State of AV Industry

IIKARUS Security- GmbH

Retooled Malware

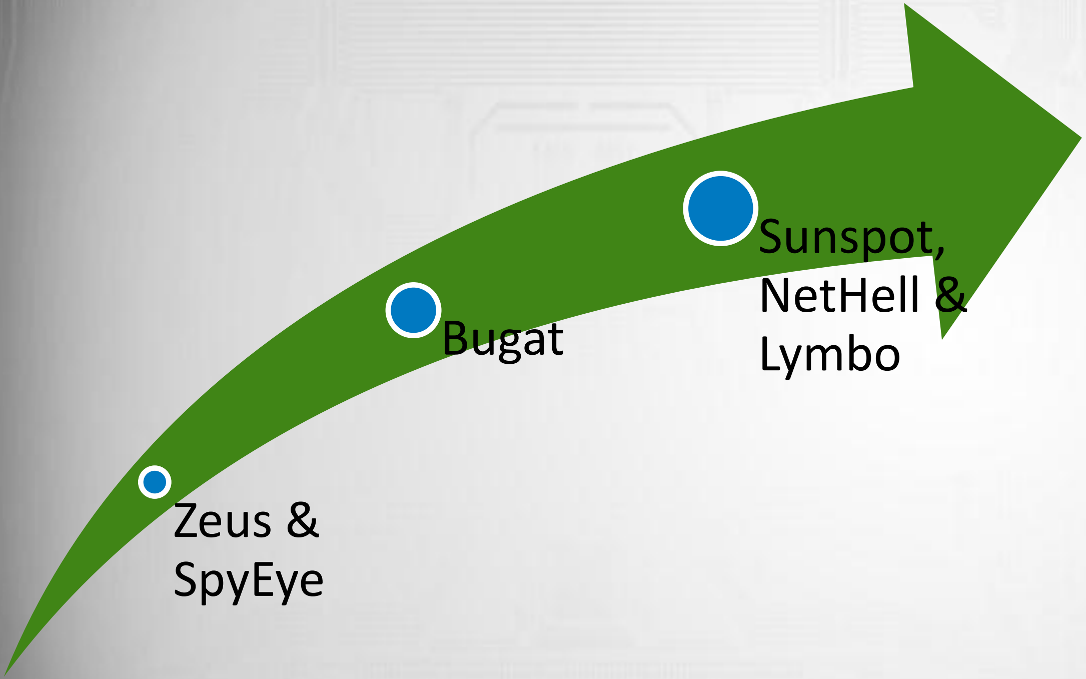
Sunspot (Limbo , Ambler)

- HTML Injection
- 7 aware (App Dir)
- Dynamic Process
- Steals Data



What does this mean?

Money



Zeus & SpyEye

Bugat

Sunspot, NetHell & Lymbo

Government SECRETS

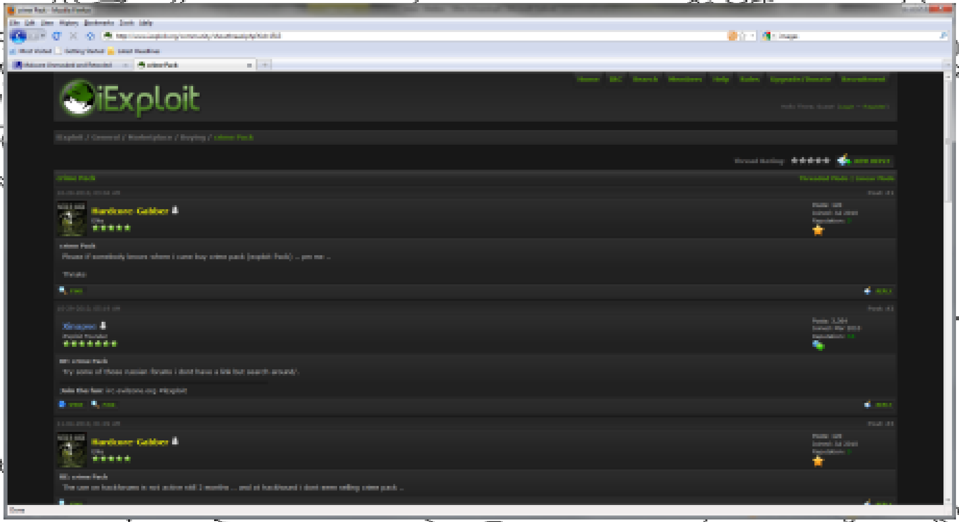
★ ★ ★ ★ ★ ★

What You NEED To Know–

- Tax Loopholes
- Special Discounts & Free Stuff
- Hidden Medicare Benefits
- Real Estate & Auction Deals

And Much, Much More...

Crime Packs come from Virtual Shopping Centers



crime Pack

Hardcore Gabber

crime Pack

Please if somebody knows where i cane buy crime pack (exploit Pack) .. pm me ..

Thnaks

RE: crime Pack

Try some of those russian forums i dont have a link but search around.

Join the fun! irc.evilzone.org #iexploit

Hardcore Gabber

RE: crime Pack

The one on hackforums is not active still 1 months ... and at hackhound i dont seen selling crime pack ..

RE: crime Pack I can sell crime pack to you msn – FakeName@hotmail.com

Crime Packs are Affordable

Entry Fees

- Windows7/Vista compatibility module – $2,000
- Backconnect module – $1,500
- Firefox form grabbing – $2,000
- Jabber notification – $500
- FTP clients saved credentials grabbing module – $2,000
- VNC module — $10,000 (reportedly no longer being sold/supported

Krebs on Security - www.krebsonsecruity.com

Language: English

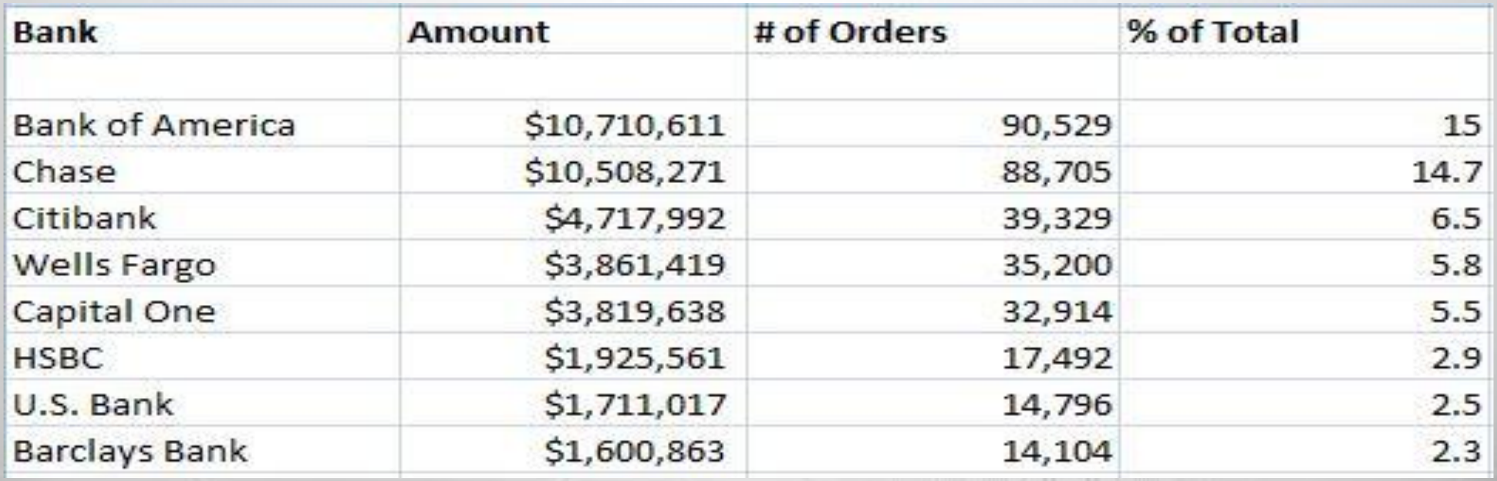
Malware is Money Motivated

"Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls" *Federal Financial Institutions Examination Council*

Nearly $70m in sales – from rogue pill buys!

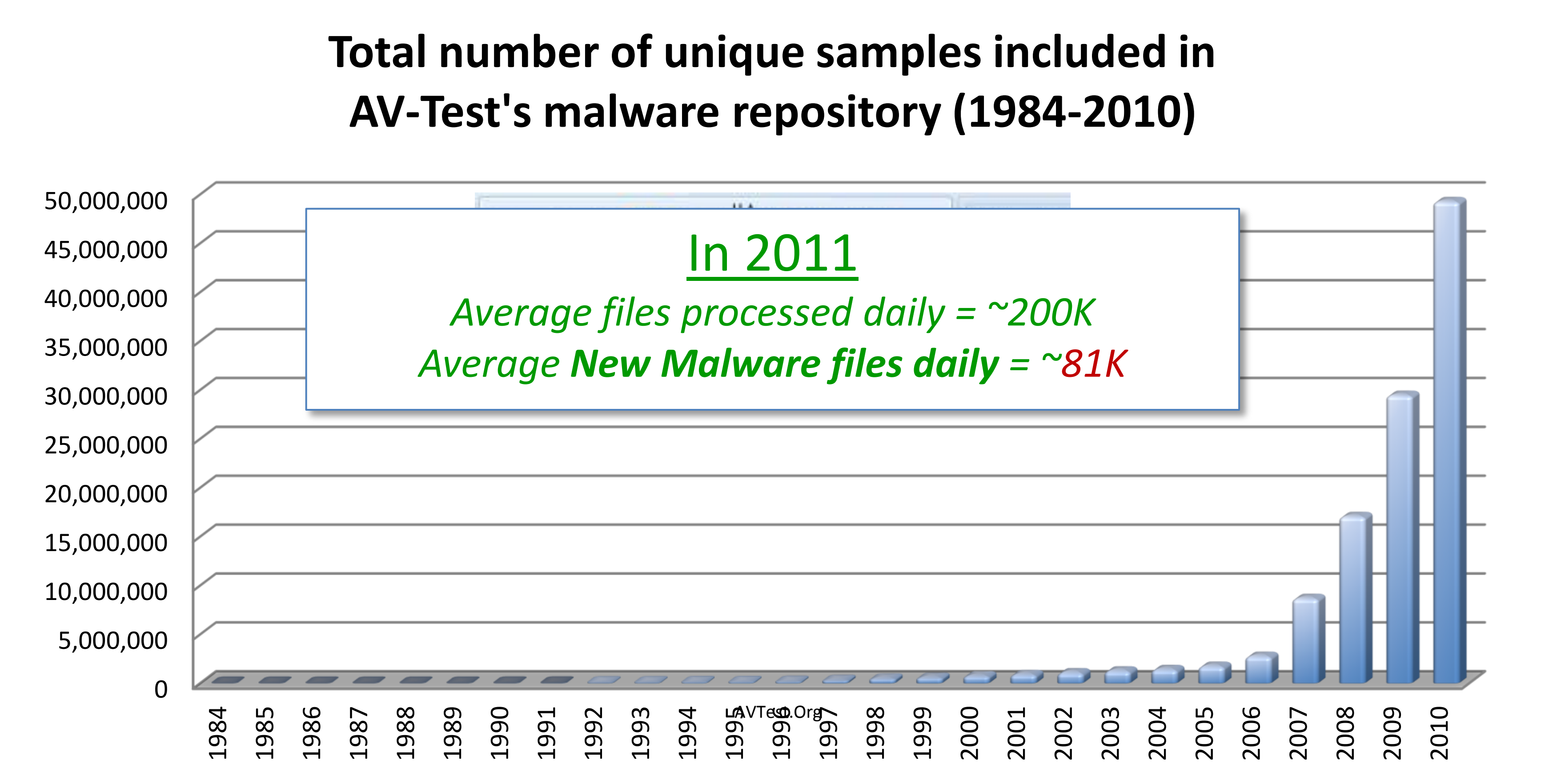
The figures shown below come from sales data stolen from **Glavmed**, a Russian affiliate program from 2006-2010

Krebs on Security - www.krebsonsecurity.com



Bank	Amount	# of Orders	% of Total
Bank of America	$10,710,611	90,529	15
Chase	$10,508,271	88,705	14.7
Citibank	$4,717,992	39,329	6.5
Wells Fargo	$3,861,419	35,200	5.8
Capital One	$3,819,638	32,914	5.5
HSBC	$1,925,561	17,492	2.9
U.S. Bank	$1,711,017	14,796	2.5
Barclays Bank	$1,600,863	14,104	2.3

Malware Trend



Total number of unique samples included in AV-Test's malware repository (1984-2010)

In 2011

Average files processed daily = ~200K

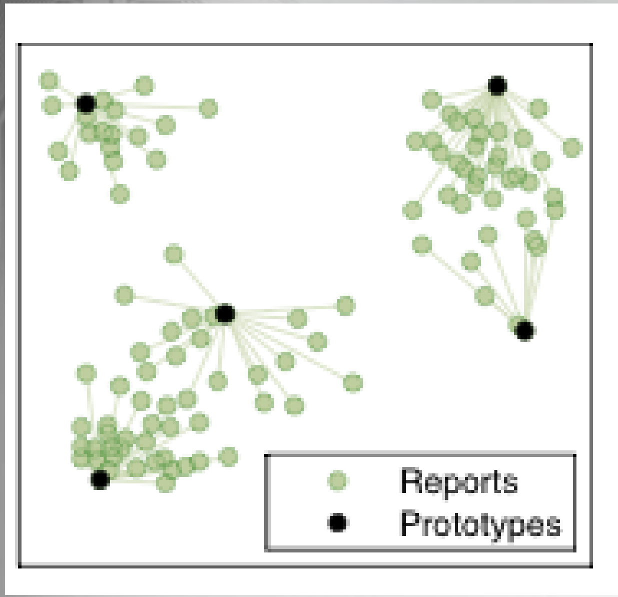
*Average **New Malware files daily** = ~81K*

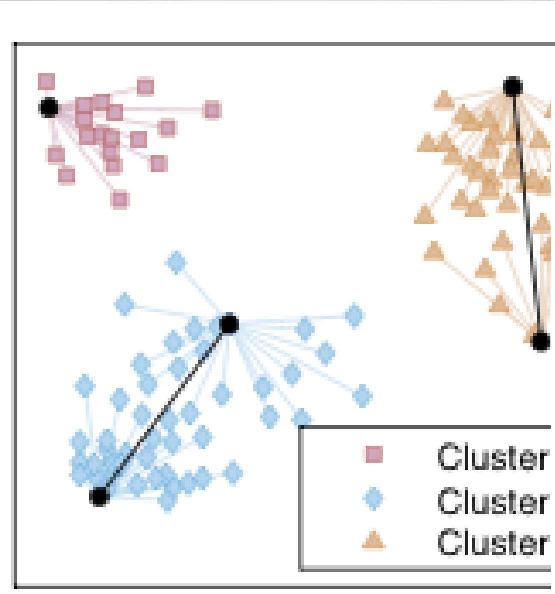
Profiles of Contemporary Threats

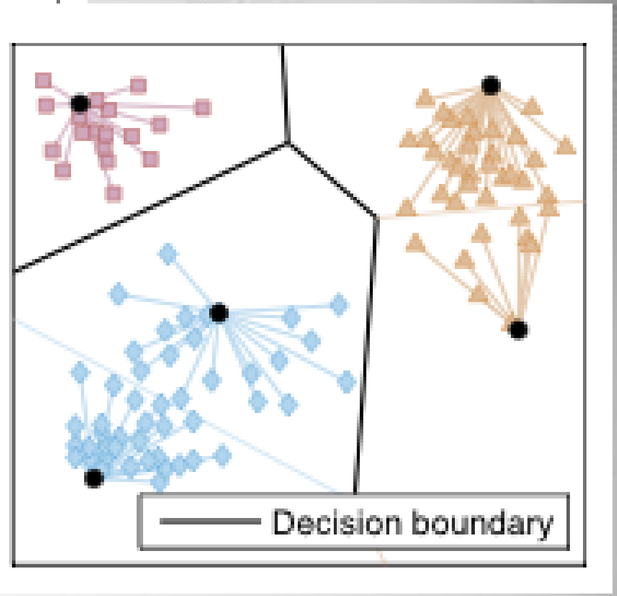
Threat Type	What it does…	How money is made
Rogue Software	False Scanning Service and discovery of threats and/or problems	Payment for "fake" security software.
Bots and Botnets	Send/Relay Spam DDoS Attacks	$$/spam Bot Army rental
Phishing and Scams	Captures Personal/Financial information	Directly stealing using financial info gathered
Ransomware	Encrypts critical files (docs, etc), and only provide decryption key when ransom is settled	Ransom payment from victimized users.

Clustering
&
Classification

Clustering and Visualisation







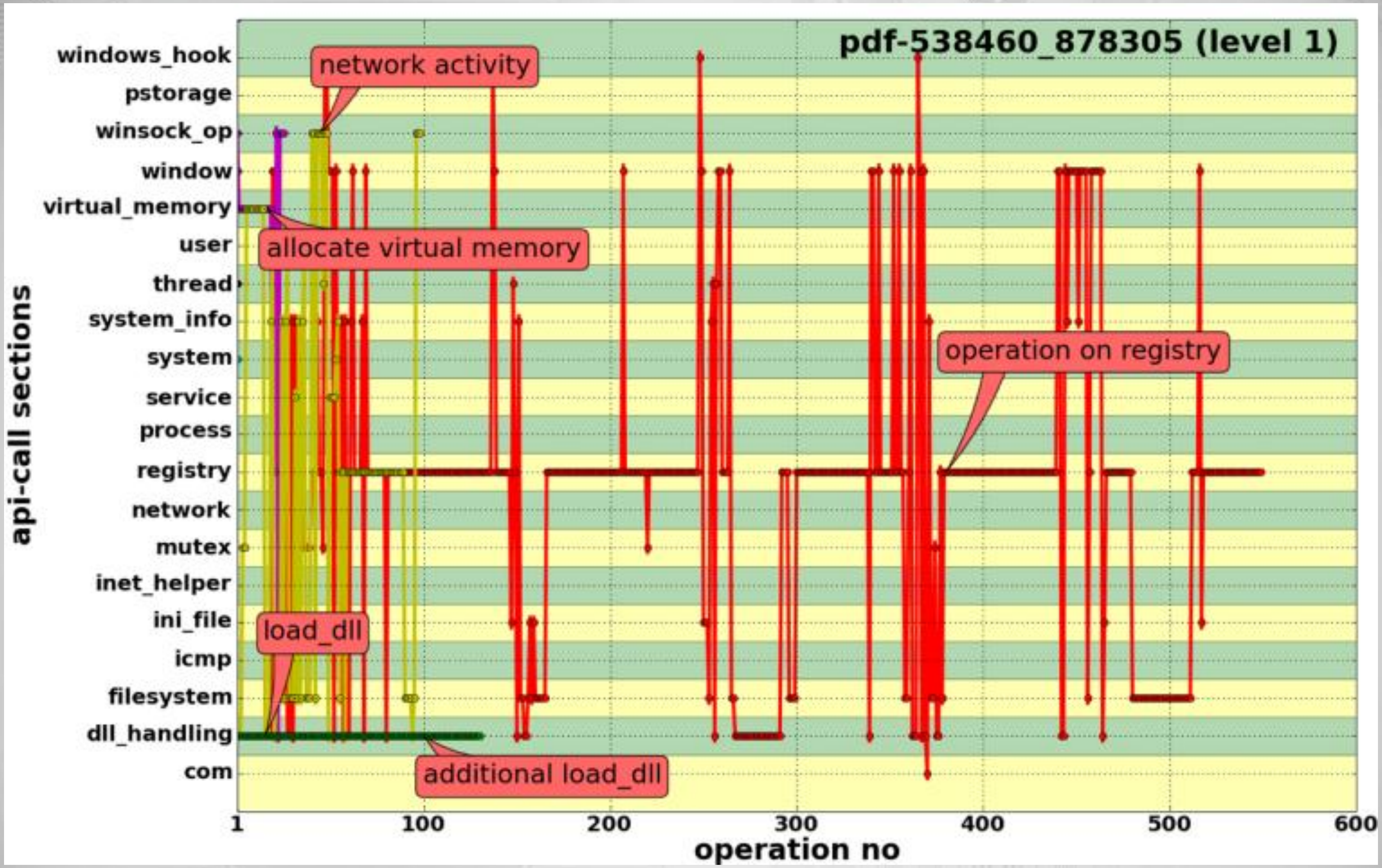
- *Extraction of prototypes*. From a given set of reports, identify a subset of prototypes representative for the full data set. The prototypes provide a quick overview of recorded behavior and can be used to guide manual inspection.

- *Clustering of behavior*. Identify groups (clusters) of reports containing similar behavior. Clustering allows for discovering novel classes of malware and provides the basis for crafting specific detection and defense mechanisms

- *Classification of behavior*. Based on a set of previously clustered reports, assign unknown behavior to known groups of malware. Classification enables identifying novel variants of malware and can be used to filter program behavior prior to manual inspection

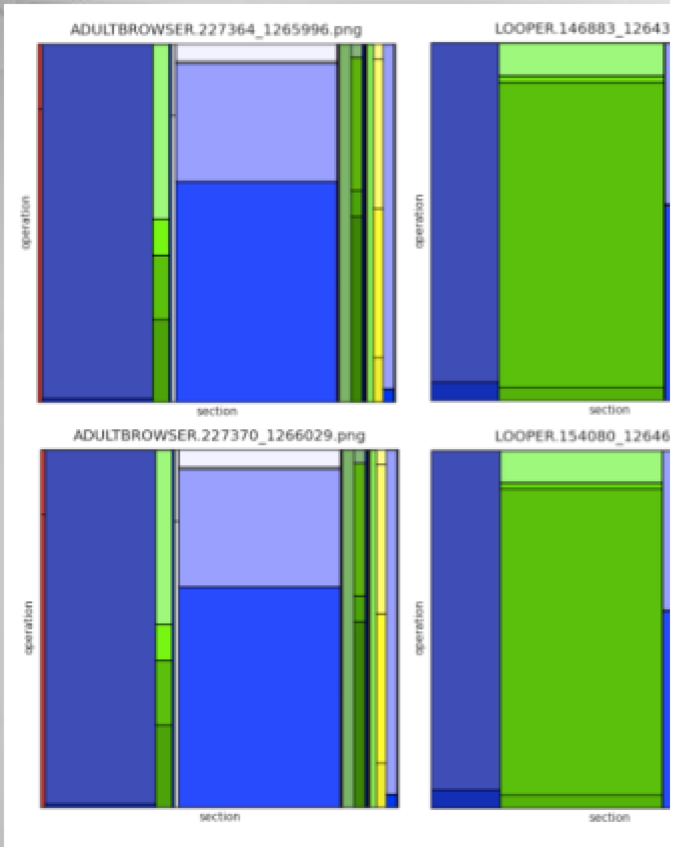
Ref. http://www.mlsec.org/malheur/

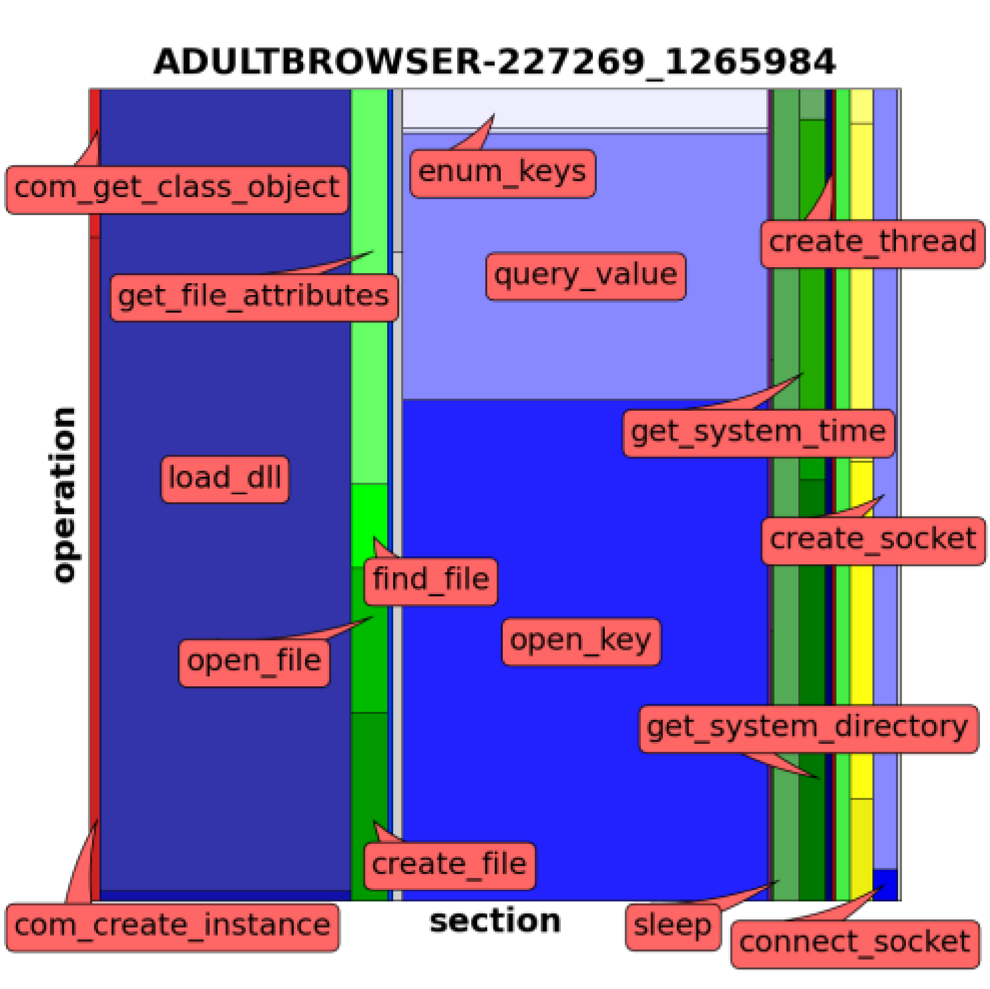
ThreadGraphs



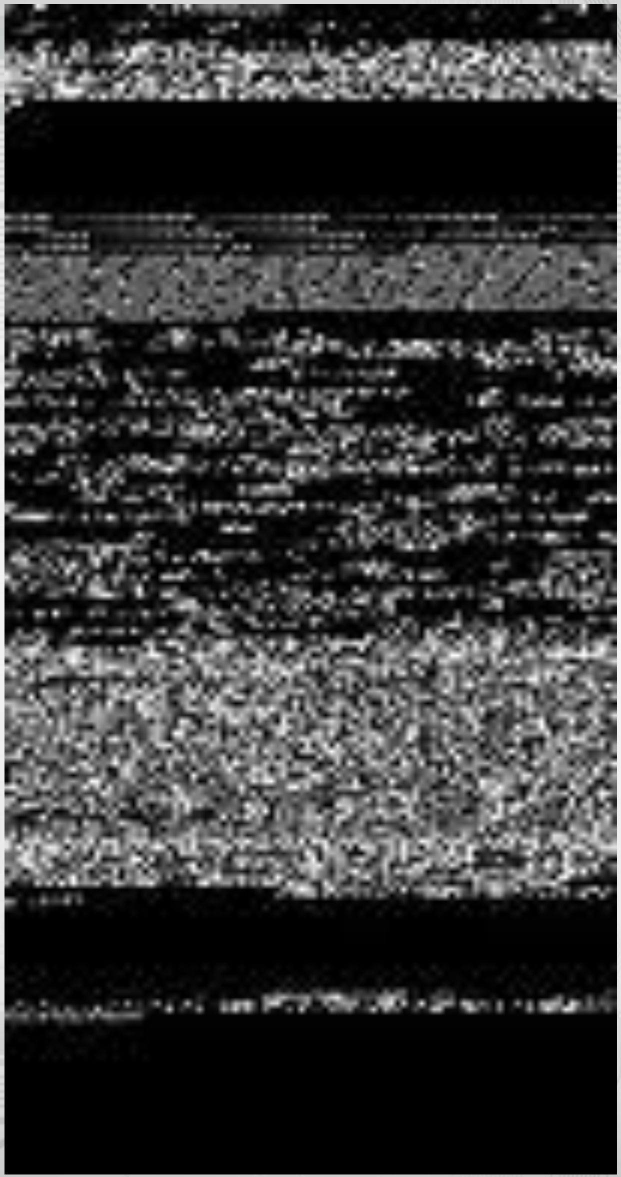
Malicious PDF

Treemap


ADULTBROWSER.227364_1265996.png
LOOPER.146883_12643
operation
section
operation
section
ADULTBROWSER.227370_1266029.png
LOOPER.154080_12646
operation
section
operation
section


ADULTBROWSER-227269_1265984
operation
section
com_get_class_object
enum_keys
create_thread
get_file_attributes
query_value
get_system_time
load_dll
create_socket
find_file
open_key
open_file
get_system_directory
create_file
com_create_instance
sleep
connect_socket

Visualization



Clustering and Visualisation – so what?

Criteria to create a cluster:

- Commonality of:
  - Mutex creation
  - Registry changes
  - Network traffic
  - Other…

Clustering gives us:

- Identify new malware by old authors
- Quickly, automatically identify new malware families
- Verify if new malware constitutes a new technique or threat, or merely a repackaging of an old threat

Old Malware Retooled to New Malware
More Malware Authors

- Old malware is new malware :
  - – Malware Authors are getting sophisticated
- Latest threats:
  - – Old malware code – new behavior

What's in the wild today can easily change tomorrow!

Q & A