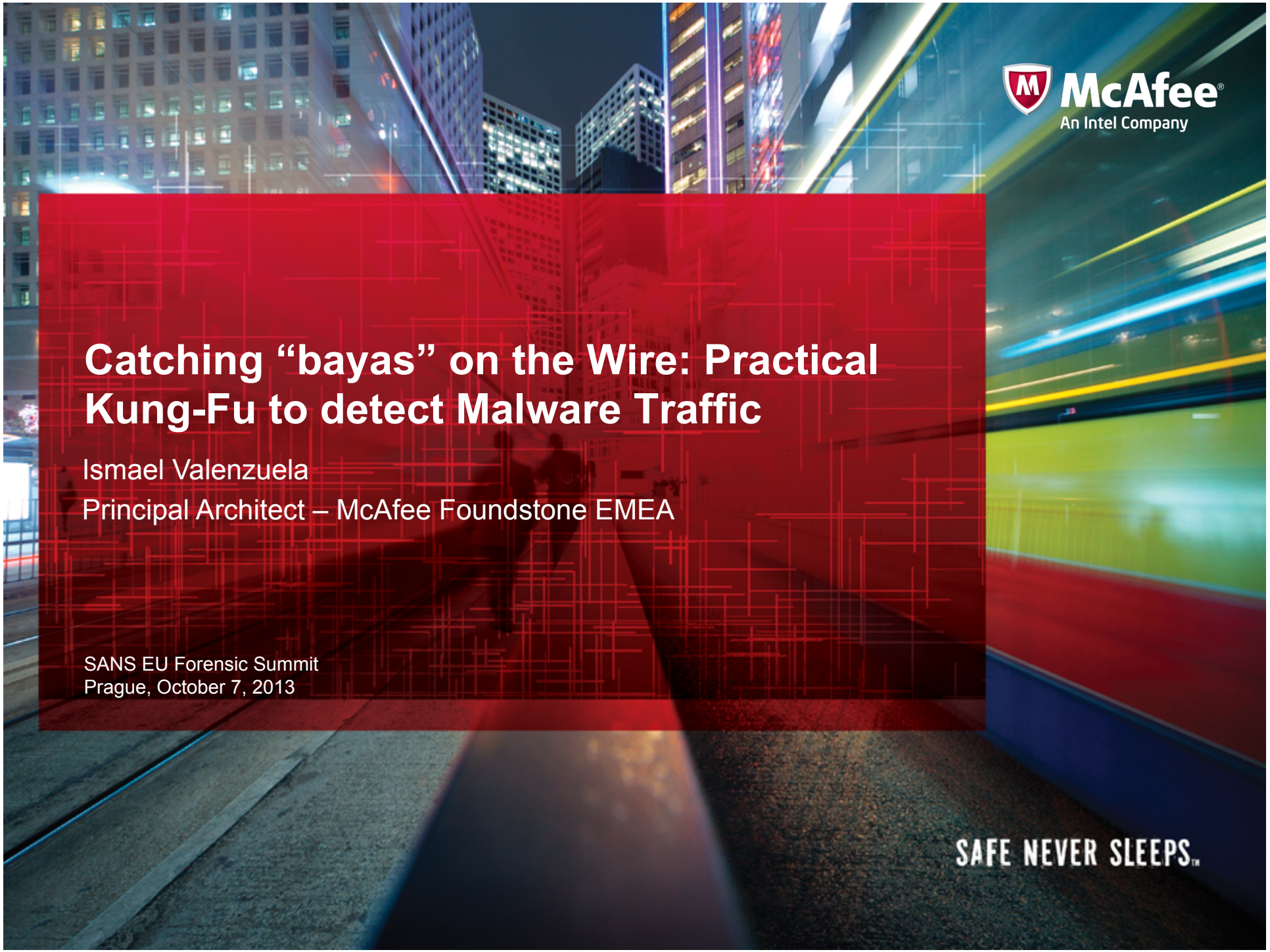


Catching “bayas” on the Wire: Practical Kung-Fu to detect Malware Traffic

Ismael Valenzuela
Principal Architect – McAfee Foundstone EMEA

SANS EU Forensic Summit
Prague, October 7, 2013

Principal Architect, McAfee Foundstone EMEA

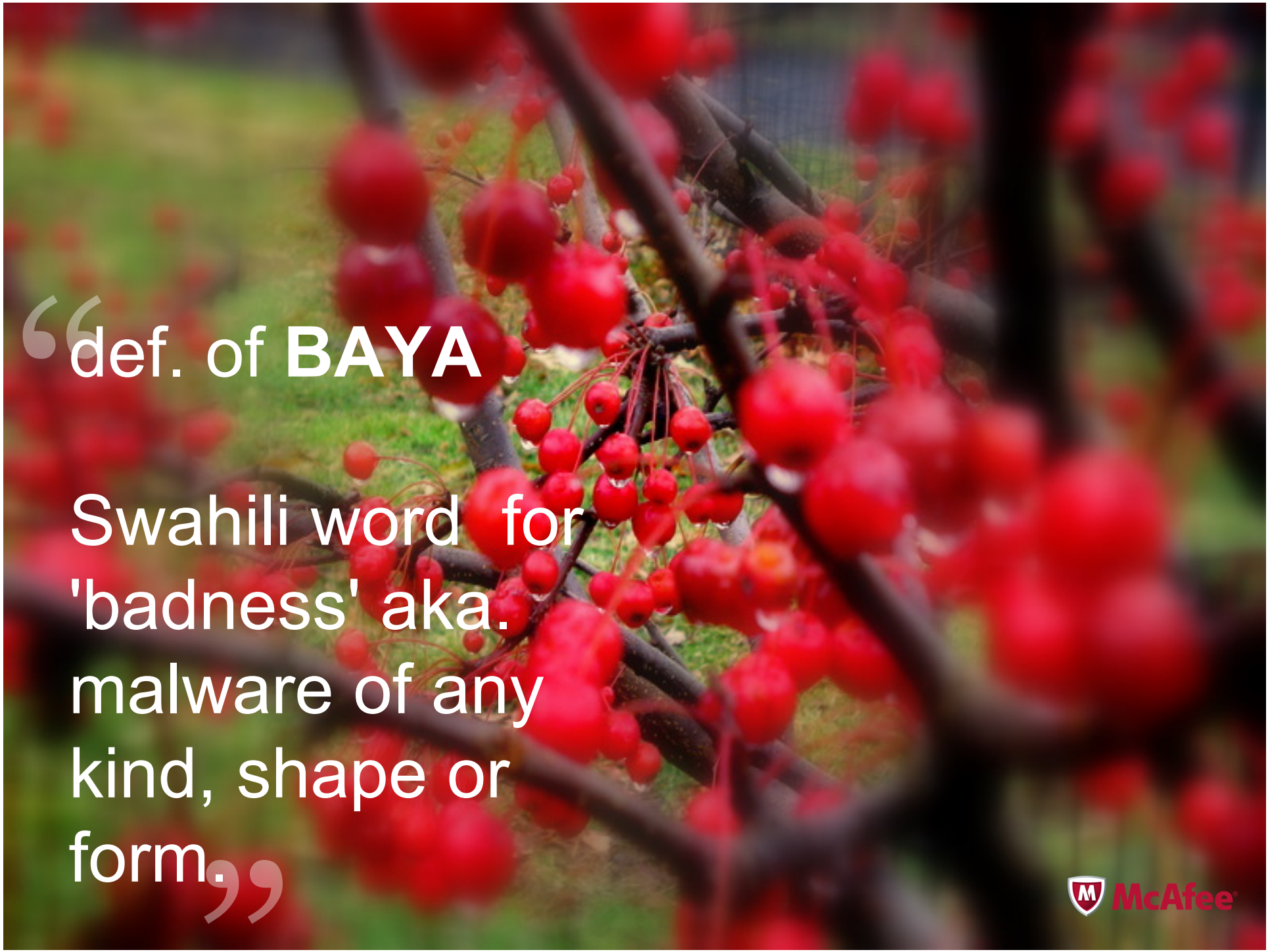
- 13 years of experience in Infosec
- Part of the Incident Response and Malware Forensics team in McAfee Foundstone Services
- Community SANS Instructor
- Author of security articles for Hakin9, INSECURE Magazine, SANS Forensic Blog, Open Security Research blog, etc…
- GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, CISSP, CISM, IRCA 27001 LA, ITIL Certified

http://blog.ismaelvalenzuela.com

@aboutsecurity

Feel free to tweet as we go with #DFIRSUMMIT

McAfee
An Intel Company


“def. of **BAYA**
Swahili word for 'badness' aka. malware of any kind, shape or form.”
McAfee

<disclaimer>

BAYA is also the name of my tool that I will introduce later in this talk…

simply because all the good names were already taken!!

</disclaimer>

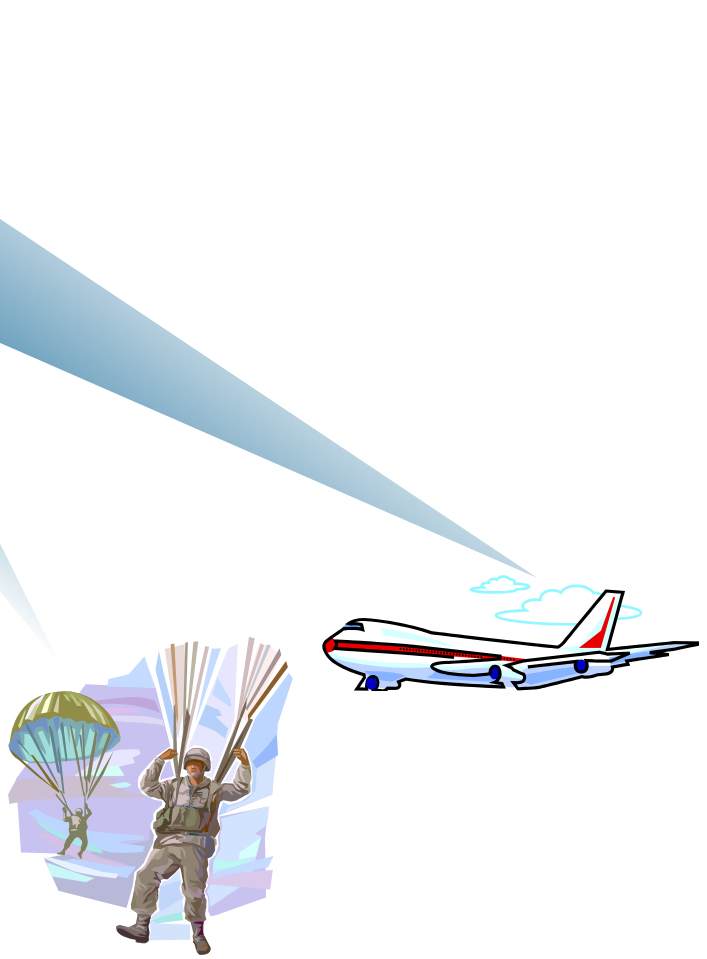
AGENDA

- Malware Patterns & Current Trends
- Effective Investigative Techniques
- Kung-Fu with Open Source Tools
- Behavioral analysis with BRO


McAfee
An Intel Company
Malware Patterns
and
Current Trends
SAFE NEVER SLEEPS.

Stories from the Trenches

What have we found?



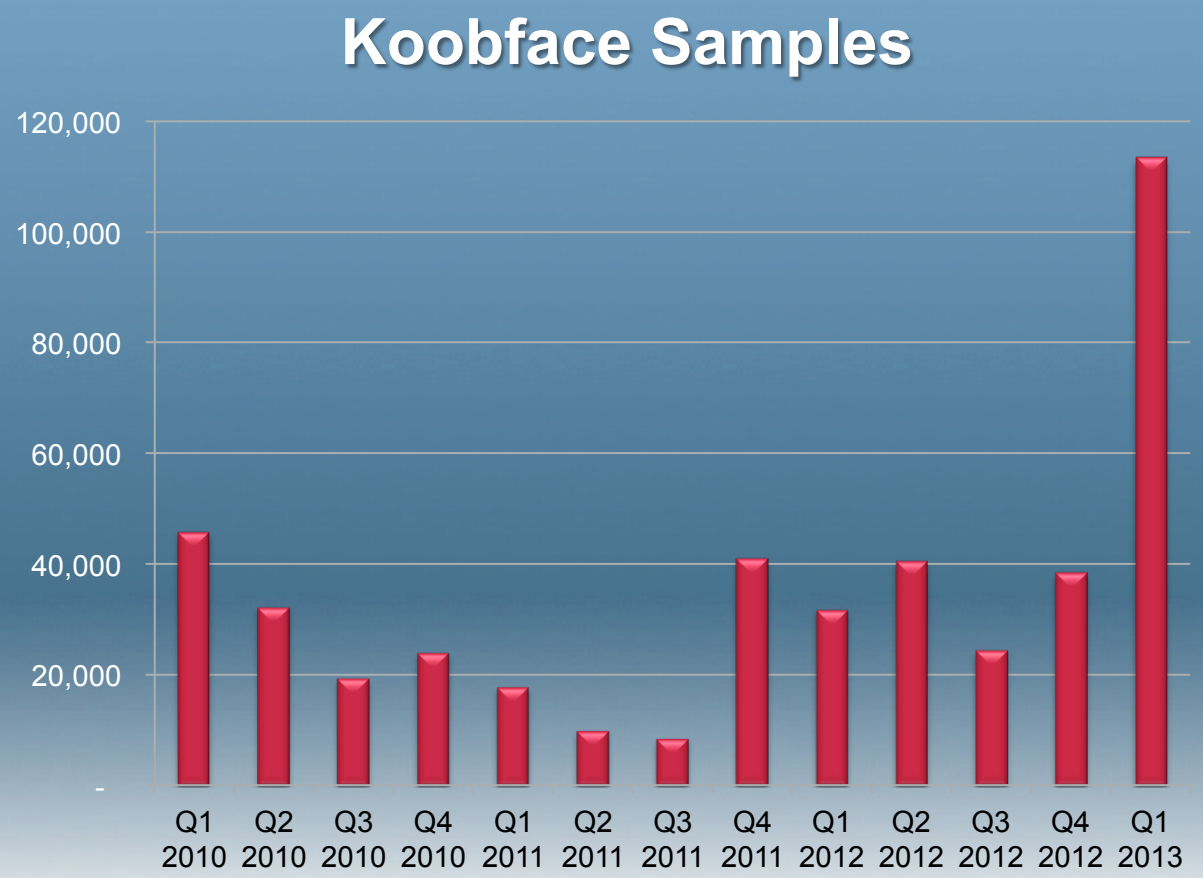
Current Trends

McAfee
An Intel Company

- Increase in targeted attacks using older tools and techniques
- Browser based attacks represent ¾ of ALL attacks
- Global spam volume spikes after years in decline
- AutoRun malware attacks spike likely driven by the popularity of cloud-based file-sharing services
- Increasing use of heavy obfuscation / encryption
- Malicious URLs become the preferred method of malware distribution versus botnets

If It Works, Don't Touch It!

Koobface, a worm first discovered in 2008, had been relatively flat for the last year yet it *tripled* in the first quarter of 2013 to levels never previously seen. The cybercriminal community obviously believes that social media users constitute a very target-rich environment of potential victims.



Source: McAfee Q1 2013 Quarterly Threat Report

Recent Example (June 2013)

- Spearphishing attack targeted Middle East and Caribbean Entities
- Dropped various tools to steal credentials (keylogger, pwd stealers…)
- Techniques used were nothing new
  - Simple XOR encryption
  - Netsh commands to disable local firewall
  - FTP results

```
@netsh firewall set opmode disable
@cls
@netsh advfirewall set currentprofile
state off
```

Source: http://mcaf.ee/7vg2z

“Problem Exists Between Keyboard And Chair...”

McAfee

Exploit Kits

- There are about 30 exploit packs currently known in the wild
  - Does not include multiple variants of the same kit (Blackhole 2.0)
  - Over 69 CVEs are covered
  - CVE-2013-2423 is currently supported by 10 exploit kits (and metasploit)
  - Focus is on add-ons and not Operating Systems
    - PDF, Flash, Java
- Malware is smarter, checking the victim for versions and serving the exploit which will work on the system
- Requests can be obfuscated/redirected

Source: Contagio

How May I Pwn You Today?

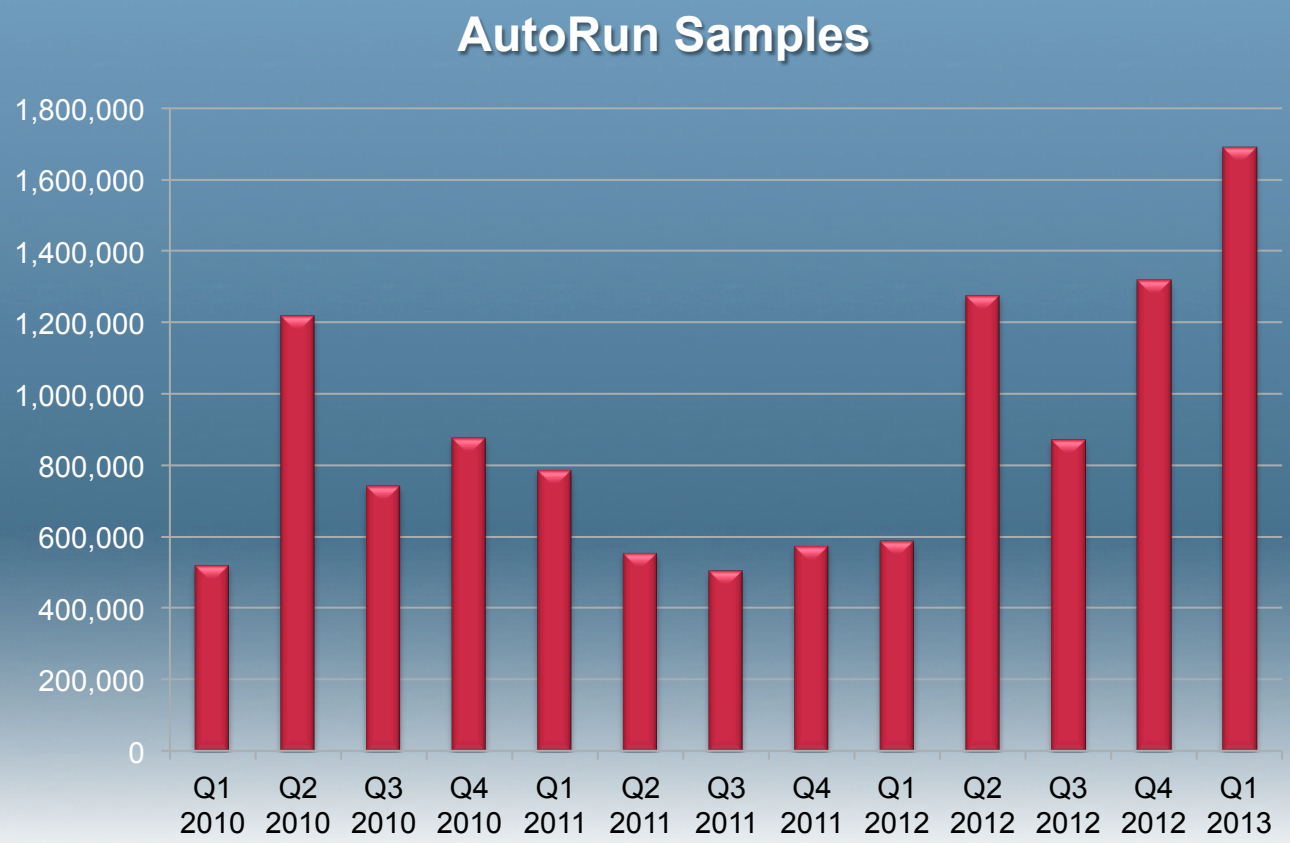
```
document.write('<center><h1>Please wait page is loading...</h1></center><hr>');

function end_redirect() {}

var pdfver = [0, 0, 0, 0], flashver = [0, 0, 0, 0];

try {
    var PluginDetect = {
        version: "0.7.6",
        name: "PluginDetect",


    // removed bulk of PluginDetect library for clarity

    // in recent variants, the PluginDetect library is loaded
    // from a remove site, rather than embedded in the landing
    // page


    PluginDetect.initScript();
    PluginDetect.getVersion(".");
    pdfver = PluginDetect.getVersion("AdobeReader");
    flashver = PluginDetect.getVersion('Flash');
} catch (e) {}

if (typeof pdfver == 'string') {
    pdfver = pdfver.split('.')
} else {
    pdfver = [0, 0, 0, 0]
}
```

Which plugin can I potentially attack?

Source: Malicious Website

AutoRun Malware

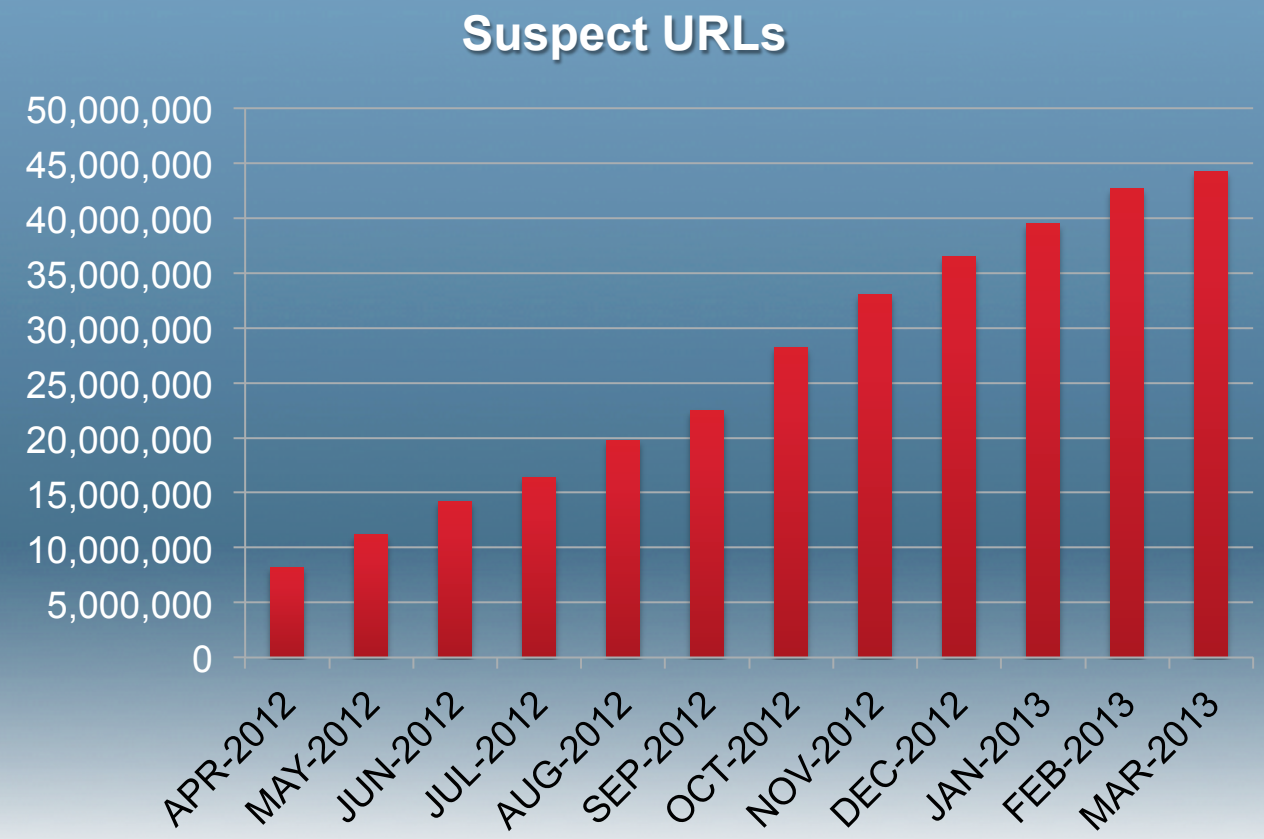
Traditionally, AutoRun worms were distributed via USB thumb drives or CDs. They are particularly useful to cybercriminals as AutoRun worms can be used to install backdoors or password stealers on infected machines. The new spike in AutoRun discoveries is likely being driven by the popularity of cloud-based file-sharing services.



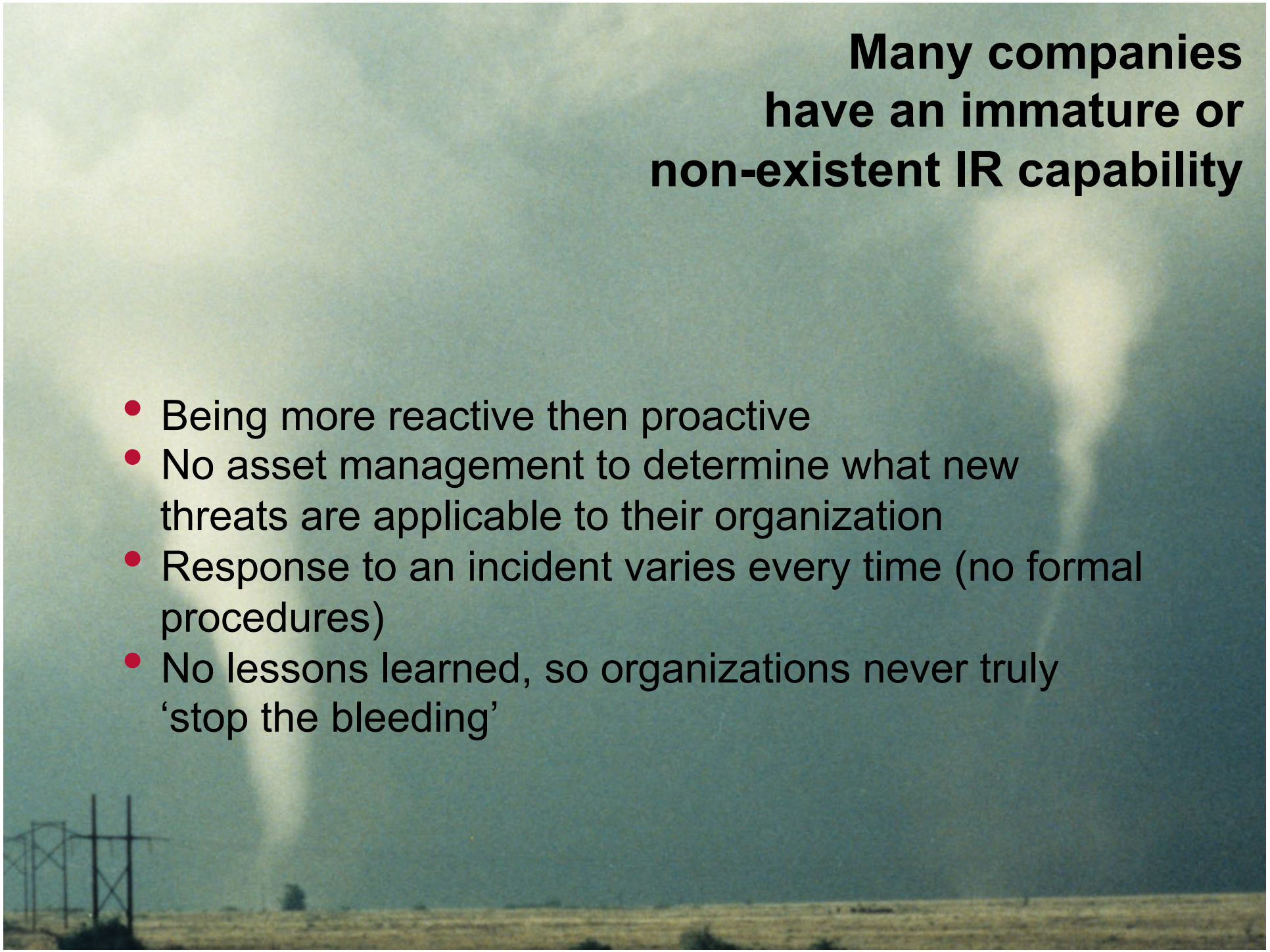
Source: McAfee Q1 2013 Quarterly Threat Report

Suspect URLs

Cybercriminals continued their movement away from botnets as the primary distribution mechanism for malware. They now prefer malicious websites that implement “drive-by downloads.” This approach has the advantage of being more nimble and less susceptible to law enforcement takedowns.



Source: McAfee Q1 2013 Quarterly Threat Report



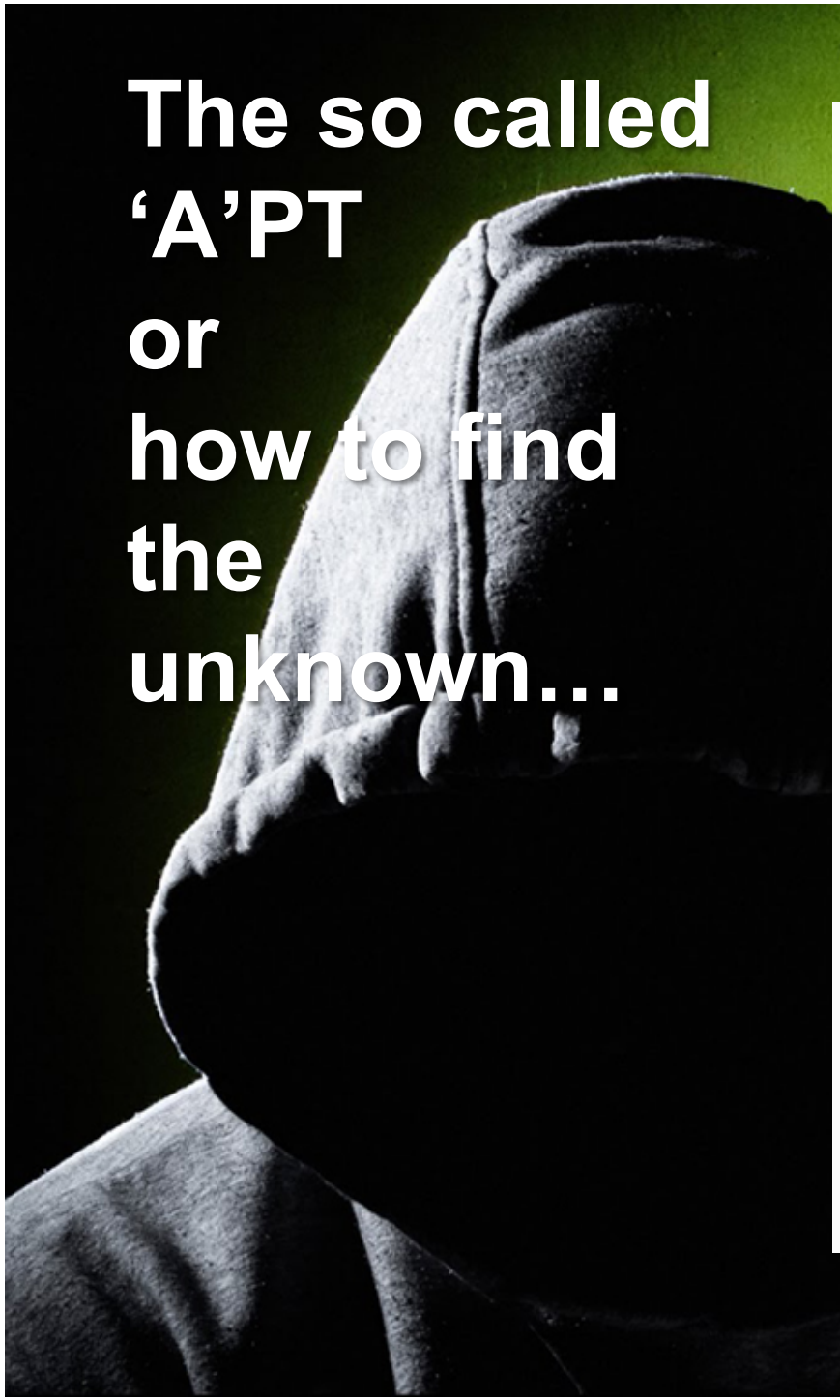
Many companies have an immature or non-existent IR capability

- Being more reactive then proactive
- No asset management to determine what new threats are applicable to their organization
- Response to an incident varies every time (no formal procedures)
- No lessons learned, so organizations never truly ‘stop the bleeding’

“Taking a spoon to a gunfight...”

McAfee

The so called ‘A’PT or how to find the unknown…



- Companies are always worried about the ‘unknown’ malware
  - Nation state sponsored malware
  - Corporate Espionage
- How do you find 0-days?
- Regardless of the malware, they all must follow one rule…

Malware does not exist in a vacuum. It must beacon out, phone home, upload information, download updates…. Therefore, IT CAN BE DETECTED

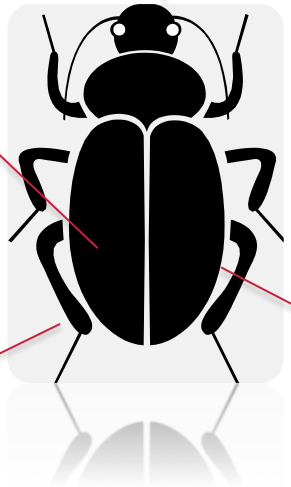
McAfee

Malware Traffic Anatomy

McAfee
An Intel Company

C&C Traffic
- HTTP
- HTTPS
- IRC
- P2P

Obfuscation
- Encryption (use of TLS)
- TLS handshake failures
- Suspicious, Invalid or Weird Certificates
- HTTP traffic on port 443



HTTP traffic
- Suspicious, Invalid or Weird User Agents
- Hidden i-frames
- Malicious Java Code

Reliance on DNS
- FastFlux
- Dynamic DNS
- Multiple samples requesting same hosts

Other Observations

- Adware infections escalating into Malicious Payloads
- Spread using Shares, USB, .exe infections
- Increased use of Cloud Resources
- Upload results to FTP servers


McAfee
An Intel Company
Increasing
your
changes
of
finding
BAYAS
SAFE NEVER SLEEPS.

Practical Kung-Fu

- Quick and dirty tips and tricks to increase your odds at finding malware in network traffic
- Useful to spot abnormal behavior in network streams
- Open Source Tools: good candidates for your IR Toolkit
- Download the tools, get PCAP samples from Contagiodump (or even your own!) and practice, practice, practice:
  - http://contagiodump.blogspot.cz/2013/04/collection-of-pcap-files-from-malware.html

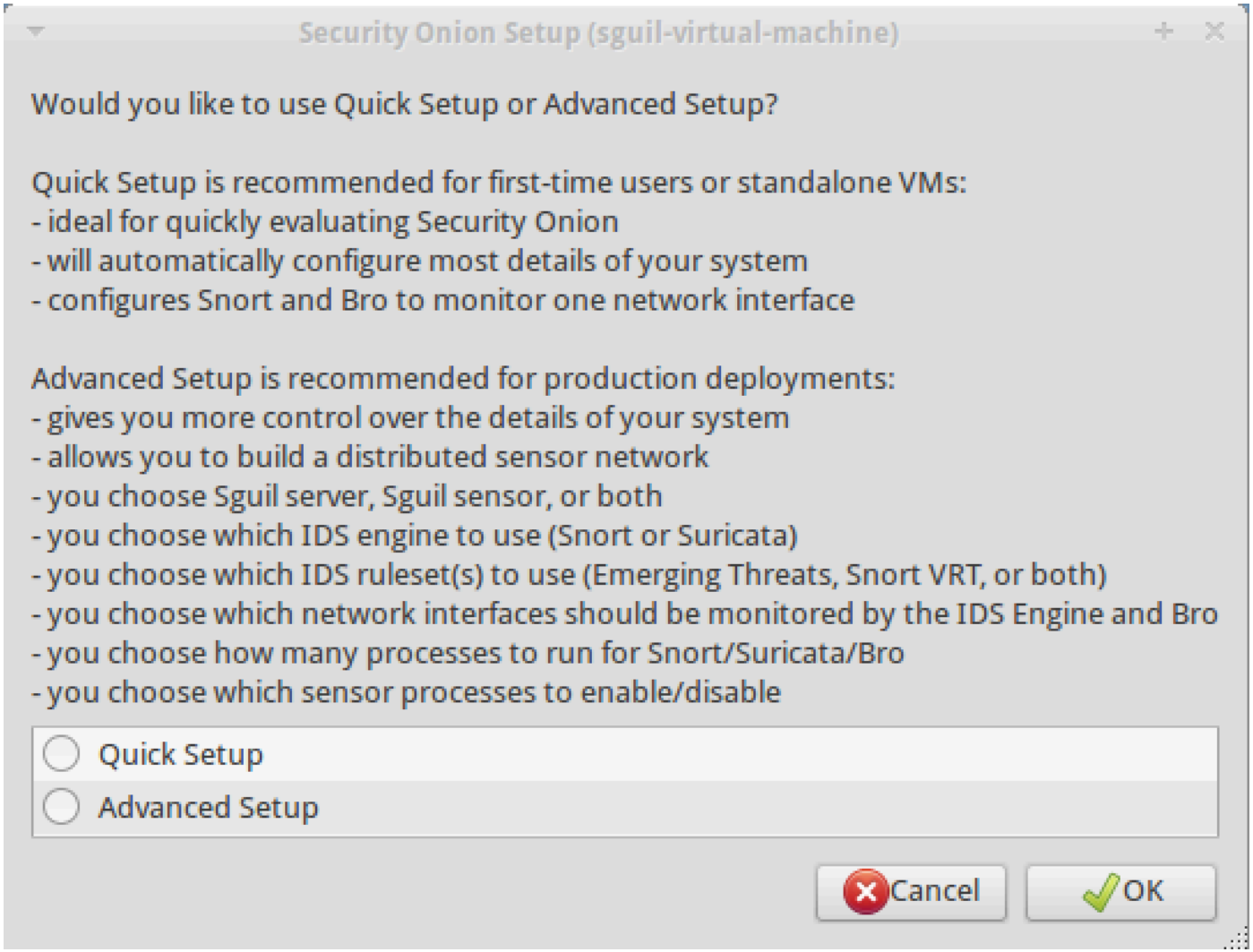
May the Onion Be With You

- An awesome FREE linux distribution that implements the concept of Network Security Monitoring
  - Packed with tons of Network Forensics Tools

- NIDS alerts from Snort, Suricata and HIDS alerts coming from OSSEC
- Asset Data (Bro and PRADS)
- Session Data (Argus, Bro and PRADS)
- Transaction Data (Bro protocol logs: http, ftp, dns, etc.)
- Full Content Data (netsniff-ng)

http://securityonion.blogspot.com

5 minutes to setup, guaranteed!



Snort Rules from Malware Threat Center

McAfee An Intel Company

- http://mtc.sri.com/live_data/signatures/

Download the most effective malware infection detection Snort signatures as experienced by our Malware Honeynet.

Most Effective Malware-Related Snort Signatures

Fri Oct 4 23:16:26 2013

160 Day Rule Set

Phase = BotHunter infection phase: (scan, infection, egg download, C&C, outbound attack)
Malcode = Number of unique malware binaries that this rule fired on during the analysis window
Infects = Number of malware infections that this rule detected during the analysis window
Detects = 30-day signature detection rates based on exposure to **593** malware infections

Detects	SID	First	Last	Infects	Author	Phase	Description
89%	2001683:3	04/27	10/03	530 of 593	emerging threats	egg download	bleeding-edge malware windows executabl...
89%	5001684:99	04/27	10/03	530 of 593	bothunter	egg download	bothunter malware windows executable (p...
88%	22466:7	04/27	10/03	524 of 593	snort	inbound exploit	netbios smb-ds ipc$ unicode share access
40%	2002750:10	04/27	10/03	241 of 593	snort	inbound	policy reserved ip space traffic - bogon nets 2
31%	299913:1	04/28	09/29	188 of 593	snort	inbound exploit	shellcode x86 0x90 unicode noop
31%	3000003:99	04/28	09/29	184 of 593	bothunter	egg download	bothunter http-based .exe upload on bac...
25%	3000000:99	04/28	09/29	153 of 593	bothunter	egg download	bothunter http-based .exe upload on bac...
25%	22000032:6	04/28	09/29	153 of 593	emerging threats	inbound exploit	bleeding-edge exploit lsa exploit
25%	292000032:99	04/28	09/29	153 of 593	bothunter	inbound exploit	bothunter exploit lsa exploit
09%	2002749:4	04/27	09/29	54 of 593	snort	inbound	policy reserved ip space traffic - bogon nets 1
07%	2003070:4	04/28	09/27	42 of 593	emerging threats	c&c channel	worm korgo.u reporting
05%	52123:3	04/30	09/15	35 of 593	snort	outbound scan	registered free attack-responses micros...
03%	2008120:1	04/30	08/25	20 of 593	emerging threats	egg download	policy outbound tftp read request
03%	3001441:1	04/30	08/25	20 of 593	snort	egg download	tftp get .exe from external source
03%	1444:3	04/30	08/25	20 of 593	snort	egg download	tftp get from external source
02%	31000004:99	05/09	09/15	14 of 593	bothunter	egg download	bothunter scrip-based windows egg downl...
01%	2000352:6	07/28	07/28	6 of 593	emerging threats	local attack prep	attack response irc - dns request on...
01%	2400003:1146	05/27	07/12	6 of 593	snort	inbound	drop spamhaus drop listed traffic inbound
01%	2000346:7	07/28	07/28	5 of 593	emerging threats	c&c channel	attack response irc - name response ...
01%	2538:15	05/08	09/30	2 of 593	snort	inbound exploit	netbios smb ipc$ unicode share access
01%	2002751:3	05/30	05/30	1 of 593	snort	inbound	policy reserved ip space traffic - bogon nets 3
01%	22001056:5	09/15	09/15	1 of 593	emerging threats	inbound exploit	bleeding-edge virus w32/sasser.worm.b -...
01%	2000047:4	09/15	09/15	1 of 593	emerging threats	egg download	worm sasser transfer _up.exe

Other Good Signature Based Resources

- Running YARA against Network Streams
  - **Yaraprocessor**, a Python library that allows for scanning TCP streams
  - **Yarashop**, a plugin for Chopshop that leverages Yaraprocessor to
  - **Chopshop**, a modular, Python based, protocol analysis and decoding Framework

  - https://github.com/MITRECND

- Or running “your favorite AV” against files extracted from Pcaps:
  - Foremost
  - Scalpel
  - NFEX (Network File EXtraction tool) – based off defunct tcpxtract tool
  - NetworkMiner, etc…

Wireshark Kung-Fu

McAfee
An Intel Company

- Christiaan Beek at BlackHat
  - https://media.blackhat.com/bh-ad-11/Beek/bh-ad-11-Beek-Taming_Worms_RATS_Dragons-Slides.pdf

- DNS queries:
  - **dns contains “ru” or dns contains “cn” or dns contains “biz” or dns contains “dyndns.org or dns contains cc”**

- Incoming file share access attempts (over SMB)
  - **((smb.cmd && ip.dst > internal network address) || (smb.cmd && ip.dst < internal network broadcast address))**

- SMB worm creating .exe on share:
  - **smb.create.action == 2 and smb.file contains "exe”**

Even some Tshark Kung-Fu

McAfee
An Intel Company

- Dump all domains visited via HTTP to a text file to compare with domain blacklists
  - **tshark -R http.request -T fields -e http.host -r traffic.pcap| sort -u > domains**
- List the hosts that visited malware.cn
  - **tshark -o column.format:'"Source","%s"' -r traffic.pcap -R "http.host == malware.cn" | sort –u**
- Set up a passive DNS service to keep a history of authoritative DNS responses (useful in IR!)
  - **tshark -i eth0 -f "src port 53" -R "dns.flags.authoritative == 1" -n -T fields -e dns.qry.name -e dns.resp.addr -E occurrence=f**

Even some Tshark Kung-Fu II

McAfee
An Intel Company

- Finding hosts that bypass the internal DNS server to resolve names. Malware can:
  - Use DNS_QUERY_NO_HOSTS_FILE in DnsQuery API
  - Open a UDP socket and send and craft UDP packets to use a specific resolver (i.e. Festi Botnet)

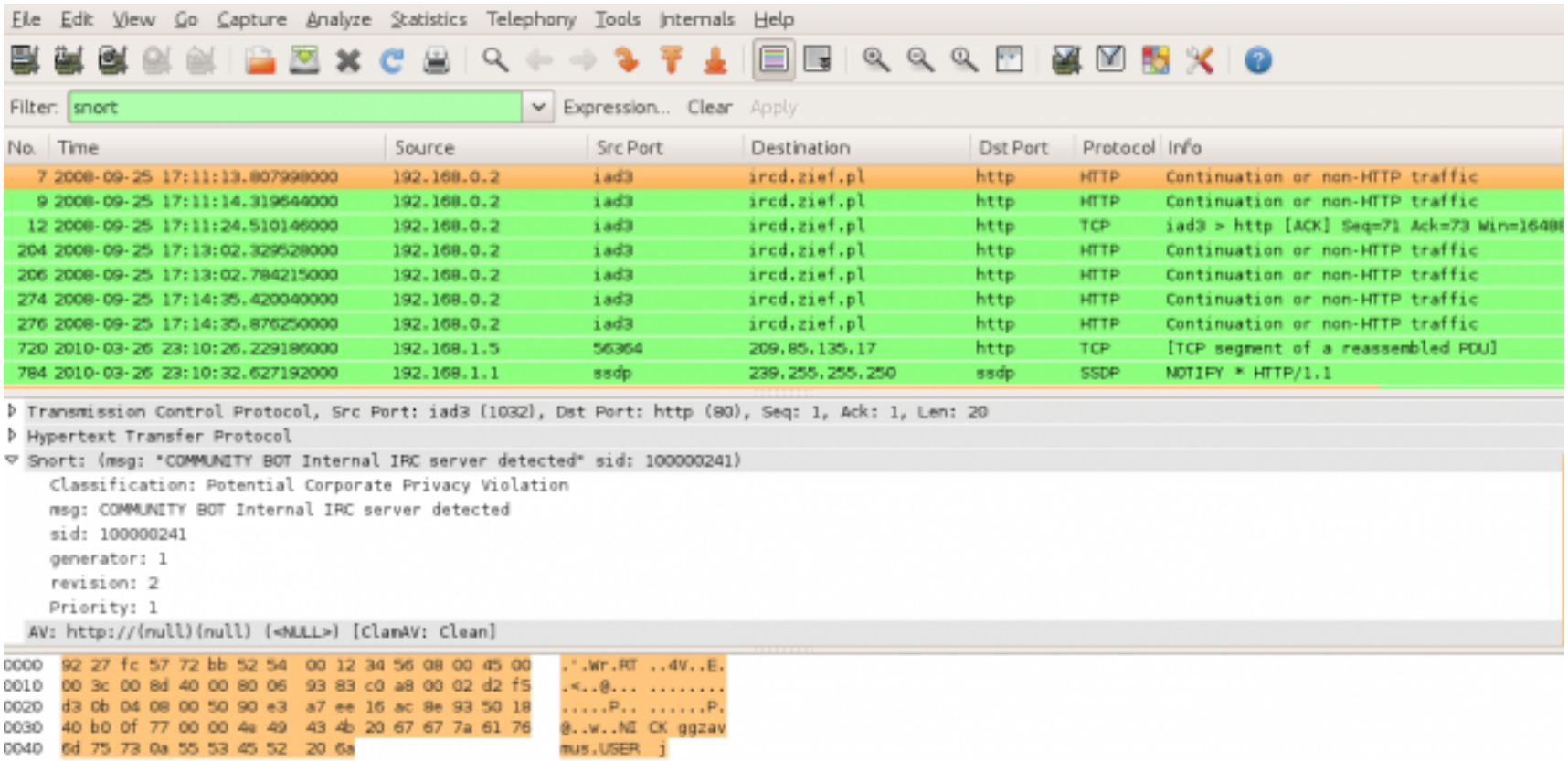
  - **tshark -r ismael.pcap "udp dst port 53 and not src host 192.168.1.100”**

- Search for non-existent domains in DNS responses (C&C is shutdown)
  - **tshark –r ismael.pcap -T fields -e dns.qry.name -e ip.dst -R "dns.flags.rcode==3" | sort |uniq –c**

Extending Wireshark Analysis

McAfee
An Intel Company

- Wireshnork & WireshAV
  - http://www.honeynet.org/node/716



User Agents (RFC2616, section 14.43)

McAfee
An Intel Company

- Sometimes malware use unusual, alien to your organization, unique or just plain evil HTTP header request user agents.

- Great whitepaper in SANS Reading Room:
  - The User Agent Field: Analyzing and Detecting the Abnormal or Malicious in your Organization

- List HTTP Requests that contain a blank User Agent
  - **tshark –r traffic.pcap –R “http.request == 1 and not http.user_agent” –T fields – e ip.addr | sort –u > outempty.txt**

- Extracting User Agent of the browser of an IP address found to visit malware.cn
  - **tshark -R http.request -T fields -e http.user_agent -r traffic.pcap -R "http.host == malware.cn" | sort –u**

Reputational Analysis & Threat Intelligence

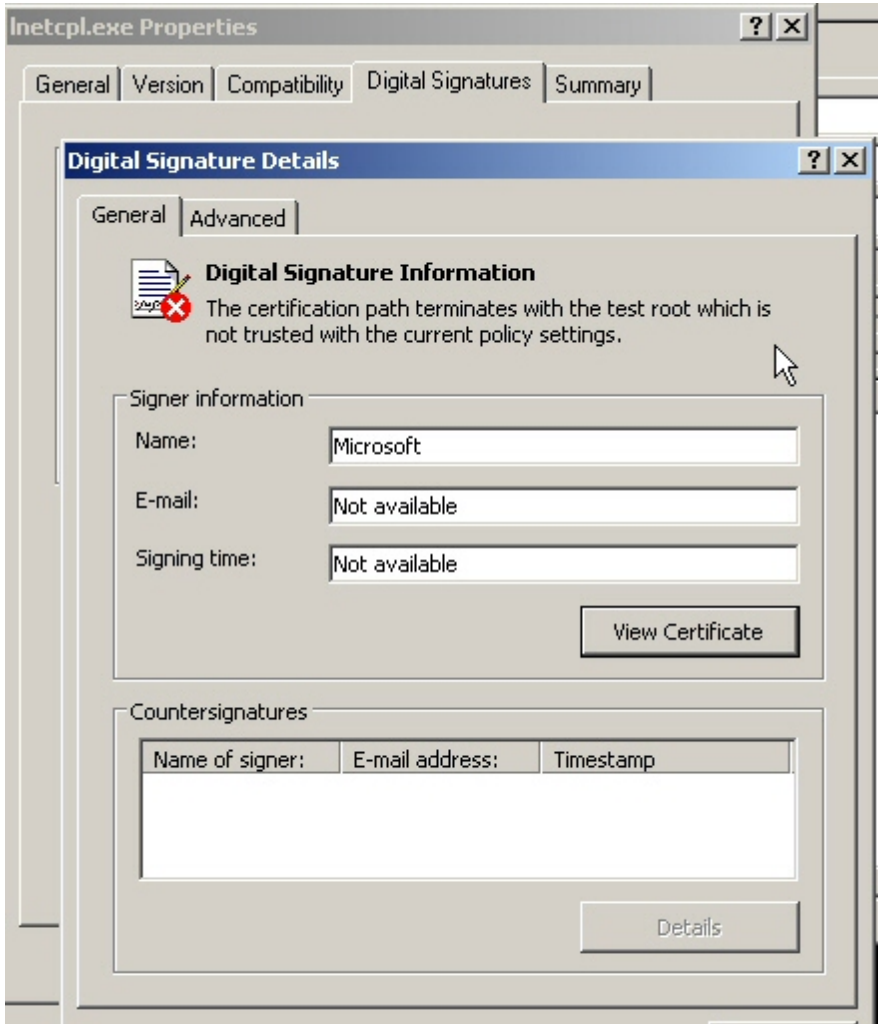
McAfee
An Intel Company

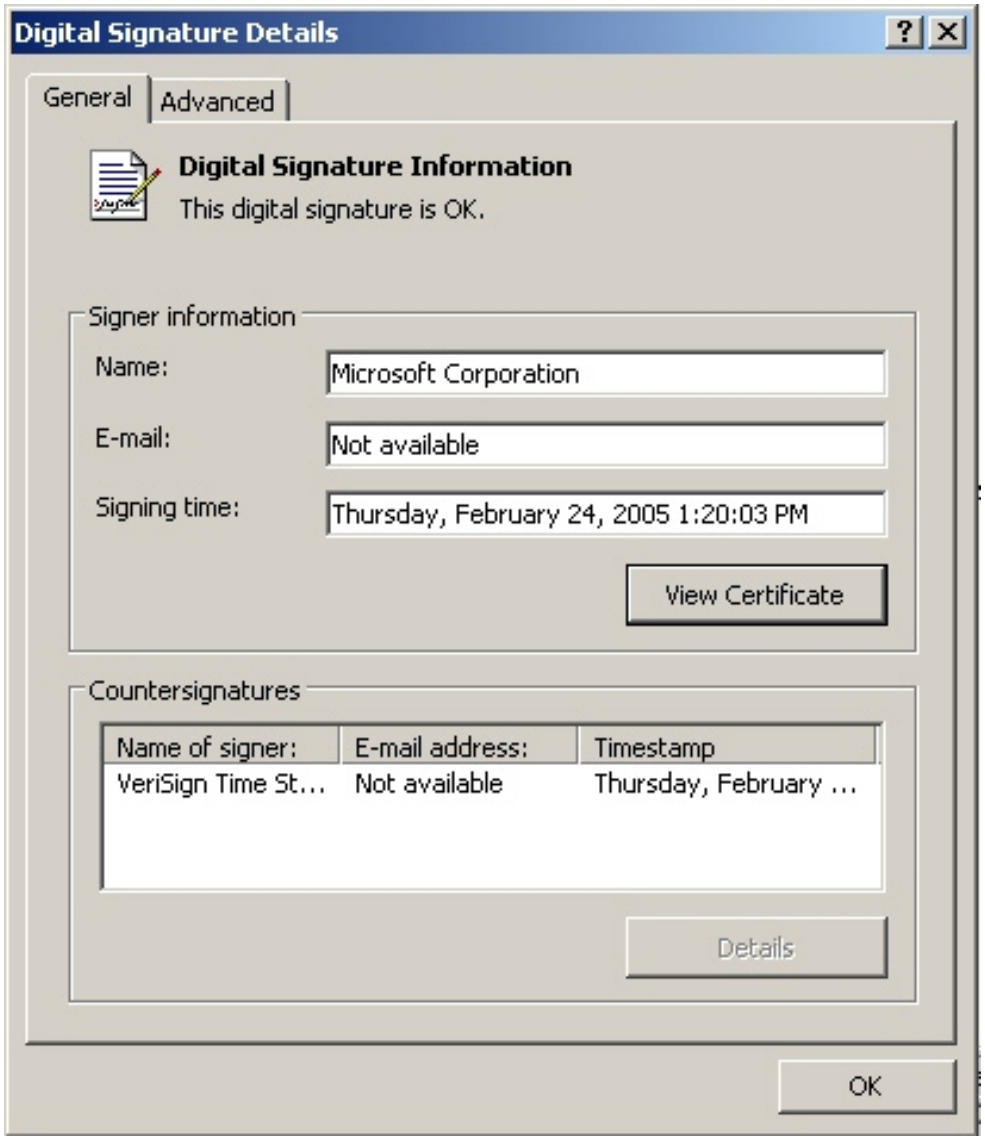
- Organize, collect and aggregate Intel for better insight
  - IPs, Domains, URLs, Geolocation, File Hashes, User Agents…
- Top 5 data feeds recommended by ENISA:
  - **Shadowserver Foundation**
  - **Zeus/SpyEye Tracker**
  - **Google Safe Browsing Alerts**
  - **Malware Domain List**
  - **Team Cymru's CSIRT Assistance Program**
- Collective Intelligence Framework (CIF)
  - Allows you to combine known malicious threat information from many sources and use that information for IR, detection and mitigation.
- Library of Malware Traffic Patterns by deependresearch.org

Valid Certificate?

Source: http://www.businesscomputingworld.co.uk/zero-day-malware-drops-payloads-signed-with-a-forged-microsoft-certificate/

Valid Certificate?





Source: http://www.businesscomputingworld.co.uk/zero-day-malware-drops-payloads-signed-with-a-forged-microsoft-certificate/

Detecting Malware in TLS/SSL

McAfee
An Intel Company

- Malware can use TLS to communicate with C&C servers to evade IDS

- Don’t panic! There are still things you can look at:
  - TLS handshake failures (initial part of communication is not encrypted)
  - Invalid, weird certificates:
    - Strange, suspicious looking CNAMES
    - Blank fields (country, state, etc…)

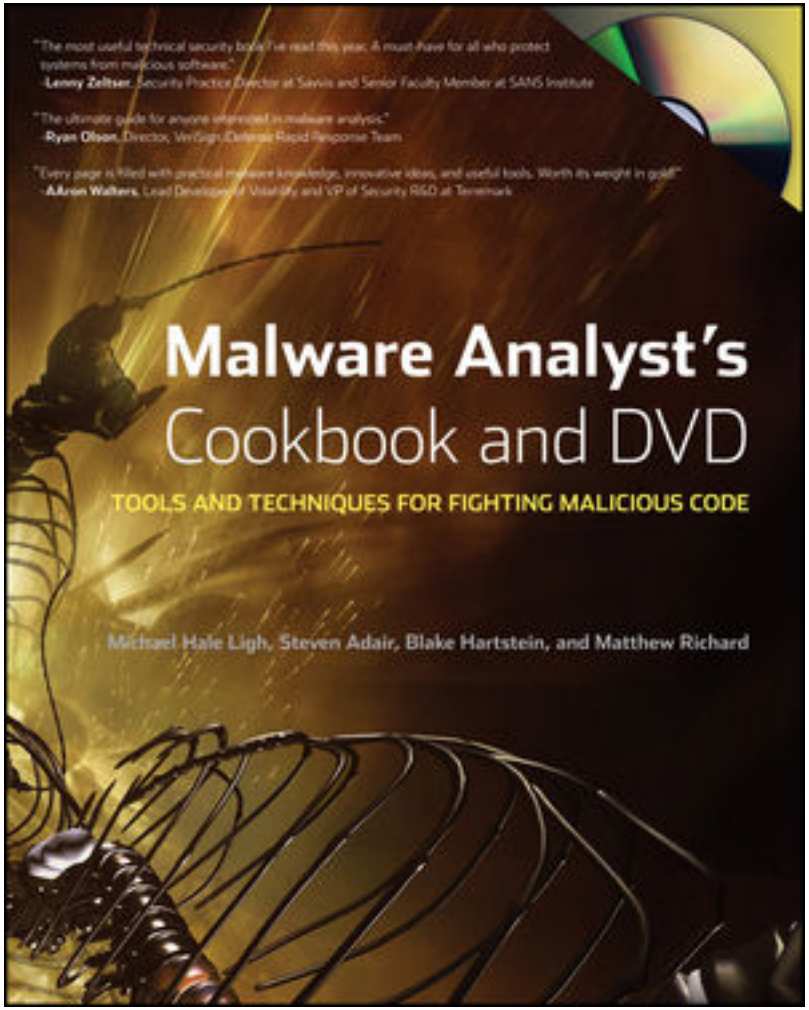
- Suricata records tls.log with this info, BRO does it too!

- More tshark Kung-Fu:
  - **tshark -r traffic.pcap -R "ssl.handshake.certificates" -T pdml > certificates**
  - **cat certificates | grep -i commonname**

Python Scripting

McAfee
An Intel Company

- The GLUE that ties all together
- Endless possibilities:
  - SCAPY library
  - APIs to interface with VirusTotal, Threat Expert, Team Cymru, and many more!
- Extracting files from network streams and run them against hash libraries, Virustotal, Cuckoo sandbox, etc…

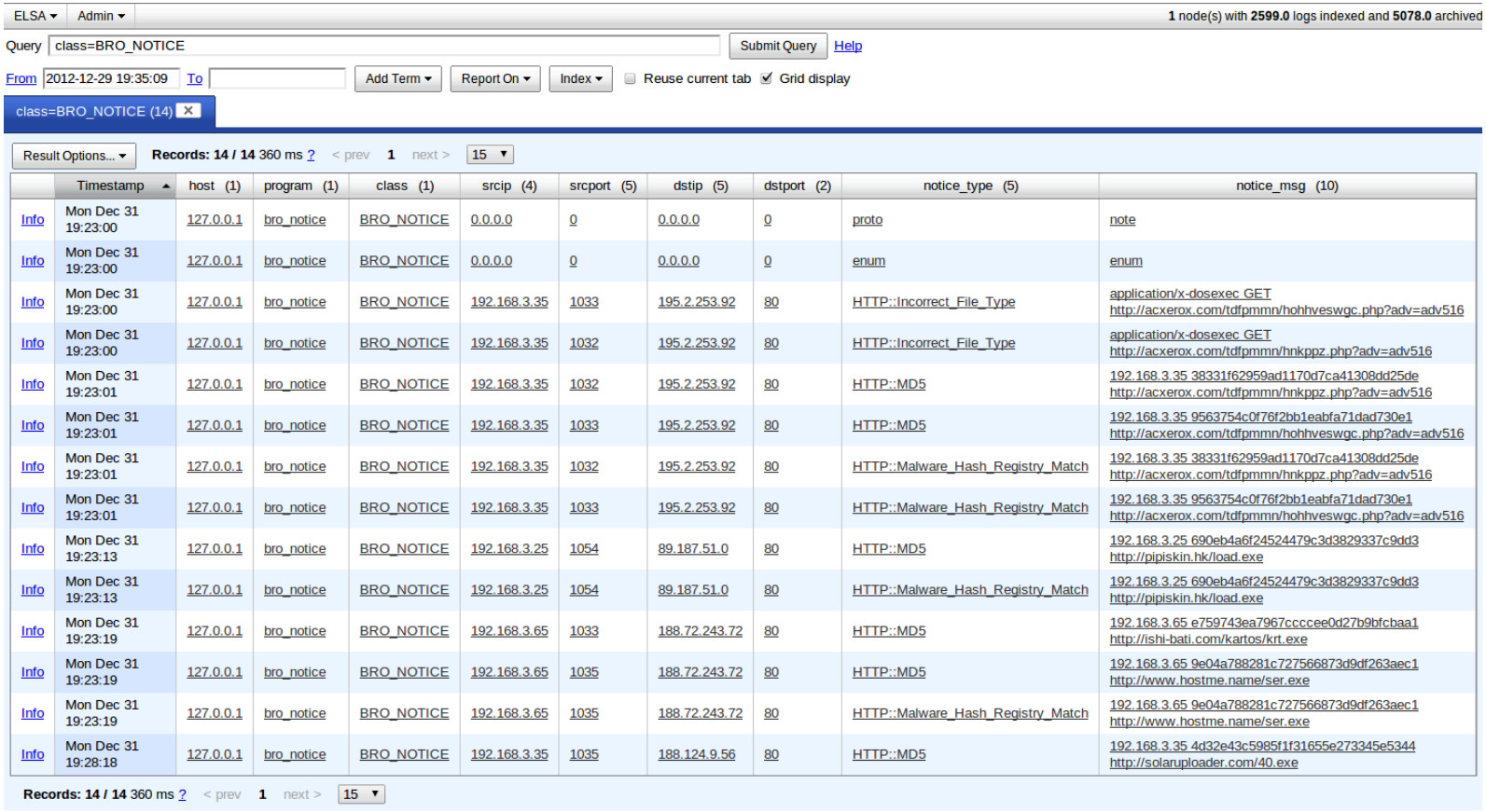


http://www.malwarecookbook.com

Seeing the Bigger Picture

McAfee
An Intel Company

- ELSA provides a Splunk-like interface to the vast wealth of log data Security Onion will harvest from Bro, Snort, OSSEC and more.



ELSA ▾ Admin ▾ **1** node(s) with **2599.0** logs indexed and **5078.0** archived

Query class=BRO_NOTICE Submit Query Help

From 2012-12-29 19:35:09 To Add Term ▾ Report On ▾ Index ▾ Reuse current tab Grid display

class=BRO_NOTICE (14)

Result Options... ▾ **Records: 14 / 14** 360 ms ? < prev **1** next > 15 ▾

	Timestamp ▲	host (1)	program (1)	class (1)	srcip (4)	srcport (5)	dstip (5)	dstport (2)	notice_type (5)	notice_msg (10)
Info	Mon Dec 31 19:23:00	127.0.0.1	bro_notice	BRO_NOTICE	0.0.0.0	0	0.0.0.0	0	proto	note
Info	Mon Dec 31 19:23:00	127.0.0.1	bro_notice	BRO_NOTICE	0.0.0.0	0	0.0.0.0	0	enum	enum
Info	Mon Dec 31 19:23:00	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.35	1033	195.2.253.92	80	HTTP::Incorrect_File_Type	application/x-dosexec GET http://acxerox.com/tdfpmmn/hohhveswgc.php?adv=adv516
Info	Mon Dec 31 19:23:00	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.35	1032	195.2.253.92	80	HTTP::Incorrect_File_Type	application/x-dosexec GET http://acxerox.com/tdfpmmn/hnkppz.php?adv=adv516
Info	Mon Dec 31 19:23:01	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.35	1032	195.2.253.92	80	HTTP::MD5	192.168.3.35 38331f62959ad1170d7ca41308dd25de http://acxerox.com/tdfpmmn/hnkppz.php?adv=adv516
Info	Mon Dec 31 19:23:01	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.35	1033	195.2.253.92	80	HTTP::MD5	192.168.3.35 9563754c0f76f2bb1eabfa71dad730e1 http://acxerox.com/tdfpmmn/hohhveswgc.php?adv=adv516
Info	Mon Dec 31 19:23:01	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.35	1032	195.2.253.92	80	HTTP::Malware_Hash_Registry_Match	192.168.3.35 38331f62959ad1170d7ca41308dd25de http://acxerox.com/tdfpmmn/hnkppz.php?adv=adv516
Info	Mon Dec 31 19:23:01	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.35	1033	195.2.253.92	80	HTTP::Malware_Hash_Registry_Match	192.168.3.35 9563754c0f76f2bb1eabfa71dad730e1 http://acxerox.com/tdfpmmn/hohhveswgc.php?adv=adv516
Info	Mon Dec 31 19:23:13	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.25	1054	89.187.51.0	80	HTTP::MD5	192.168.3.25 690eb4a6f24524479c3d3829337c9dd3 http://pipiskin.hk/load.exe
Info	Mon Dec 31 19:23:13	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.25	1054	89.187.51.0	80	HTTP::Malware_Hash_Registry_Match	192.168.3.25 690eb4a6f24524479c3d3829337c9dd3 http://pipiskin.hk/load.exe
Info	Mon Dec 31 19:23:19	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.65	1033	188.72.243.72	80	HTTP::MD5	192.168.3.65 e759743ea7967ccccee0d27b9bfcbaa1 http://ishi-bati.com/kartos/krt.exe
Info	Mon Dec 31 19:23:19	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.65	1035	188.72.243.72	80	HTTP::MD5	192.168.3.65 9e04a788281c727566873d9df263aec1 http://www.hostme.name/ser.exe
Info	Mon Dec 31 19:23:19	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.65	1035	188.72.243.72	80	HTTP::Malware_Hash_Registry_Match	192.168.3.65 9e04a788281c727566873d9df263aec1 http://www.hostme.name/ser.exe
Info	Mon Dec 31 19:28:18	127.0.0.1	bro_notice	BRO_NOTICE	192.168.3.35	1035	188.124.9.56	80	HTTP::MD5	192.168.3.35 4d32e43c5985f1f31655e273345e5344 http://solaruploader.com/40.exe

Records: 14 / 14 360 ms ? < prev **1** next > 15 ▾

Moloch

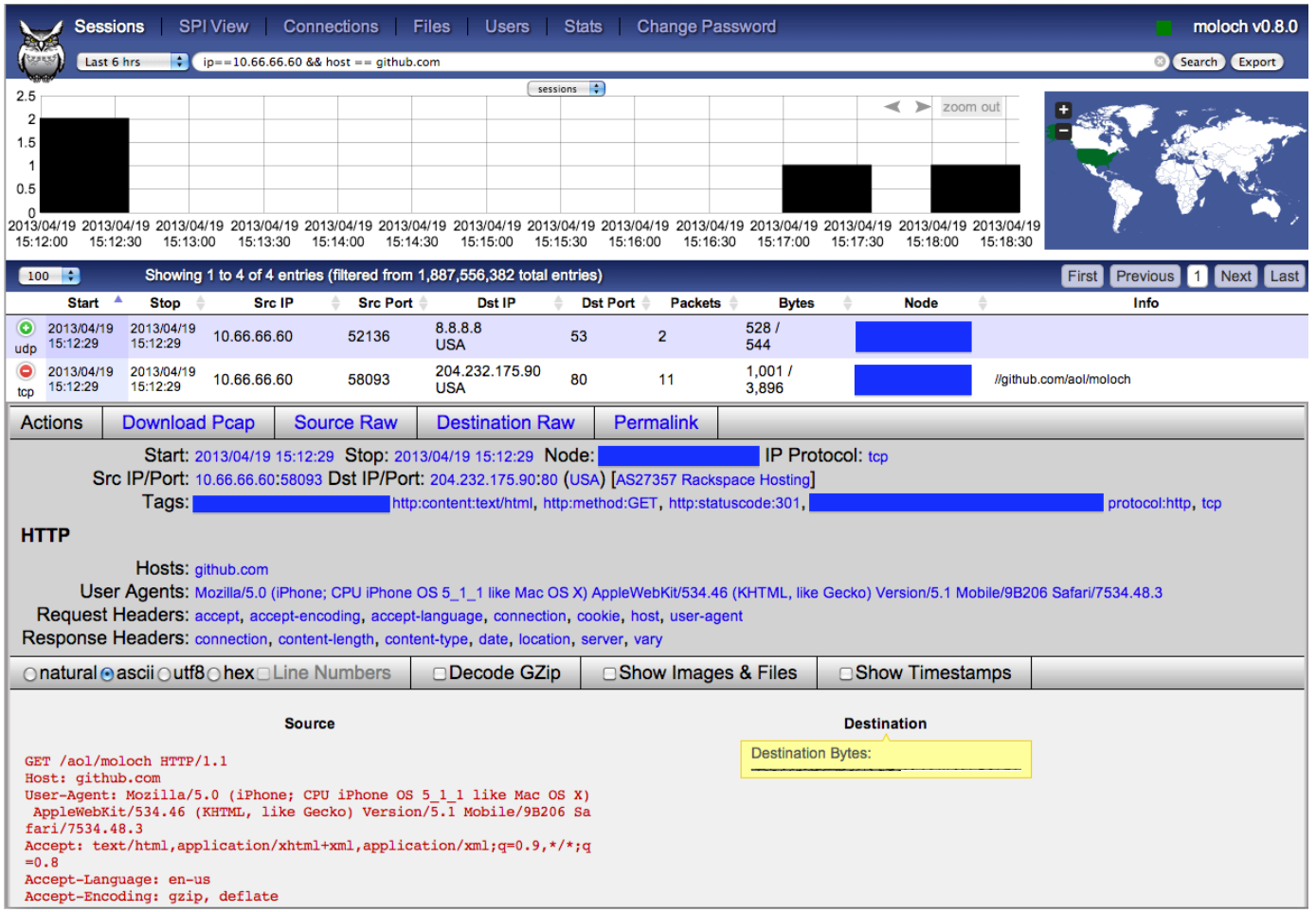
- ***"Moloch is an open source, large scale IPv4 packet capturing (PCAP), indexing and database system. A simple web interface is provided for PCAP browsing, searching, and exporting. APIs are exposed that allow PCAP data and JSON-formatted session data to be downloaded directly."***
  - from https://github.com/aol/moloch

- Allows to run almost real-time searches among dozens or hundreds of captured GB network traffic and apply several filtering options on the way, including filtering by country or AS

- Cons:
  - Requires beefy HW
  - Filtering system is no as complete as Wireshark yet

Moloch

- Sessions tab




McAfee
An Intel Company
Catching
BAYAS
with
BRO
SAFE NEVER SLEEPS.TM


“Sometimes you can’t see the forest for the trees...”
McAfee

Bro: Much more than an IDS

McAfee
An Intel Company

- Bro (created in 1994) provides visibility into the forest, while signature-based detection targets the tree. Strong support from the community!
  - More than an IDS: a **Network Programming Language**
  - Tcpdump, Wireshark, Argus, Snort and Python ALL IN ONE!

- Now you can know not only what signature-based events occurred, but you can have full context of all activity detected from the host involved
  - What domains a host queries
  - What SSL certificates are used
  - What files are downloaded
  - Any FTP/SMTP/IRC activity, etc

- All contextual questions that can help determine whether a signature-based alert is an event or an incident

Bro Structured Output

McAfee
An Intel Company

- Three classes of Output
  - Protocol Logs
    - CONN, HTTP, DNS, FTP, SSL/TLS…
  - Actions – allows active network management
    - Act on the Data, react on the data, protocol specific. In example:
      - Read a file
      - Call program
      - Output data
  - Alerts
    - Notice, Weird -> ACTIONS

- Highly structured logs (sed/grep/awk/sort/unique friendly!)

New File Analysis Framework

McAfee
An Intel Company

- Plenty of new functionalities in Bro 2.2

- One of the most powerful features is the ability to Extract Files:
  - Multiple Extraction Criteria
    - Geo Spacial -> per country of origin
    - Signature based
    - Destination Based

  - FTP, HTTP, SMTP, IRC and others coming (Bittorrent, SMB, etc..)

- Combine it with ACTIONS to do powerful file analysis:
  - Look up in Malware Hash Registry, other Intel resources
  - Upload to Virustotal, Cuckoo sandbox, even tweet the results!!

Learn More about Bro

- Awesome training resources (videos, presentations, exercises, scripts, sample pcaps, workshops, etc.)

- Bro community:
  - http://www.bro.org/community/index.html

- Youtube channel:
  - http://www.youtube.com/user/MrSlageII

- Lliam Randall's github repository:
  - https://github.com/LiamRandall

Malware Analysis with Bro - Showcase

McAfee
An Intel Company

BAYA Tool

- Work in progress…

- Set of scripts to automate much of the analysis seen during this presentation
- A wrapper for many of the tools included in Security Onion
- Leverages different APIs to gather Intel from different sources (inc. CIF)
- Created by Incident Responders for Incident Responders
- Available from my Github account in the coming weeks:
  - https://github.com/aboutsecurity

Conclusions

- Malware tries to blend in normal user traffic, but there are still certain odd, out of place or wrong behavior indicators that can help identifying
- Don’t come to the fight with a spoon: learn the tools, the techniques and the motivations of the bad guys to protect yourself
- Analyze the context, collect & aggregate good Intel for insight, and build mature processes around your whole IR program

> **Know thyself and the enemy. - Sun Tzu**

McAfee

References

- When Prevention Fails, Extending IR and Digital Forensics Capabilities to the Corporate Network: http://blog.ismaelvalenzuela.com/wp-content/uploads/2011/09/SANS-boston-night_120811.pdf
- http://www.sans.org/reading-room/whitepapers/detection/60-seconds-wire-malicious-traffic-34307?show=60-seconds-wire-malicious-traffic-34307&cat=detection
- http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/scanning-streaming-data-with-yarashop
- http://blog.alejandronolla.com/2013/04/06/moloch-capturing-and-indexing-network-traffic-in-realtime/
- http://liamrandall.com/effective-intelligence-analysis-in-bro-ids/
- http://www.deependresearch.org/2013/02/yara-resources.html
- http://www.sans.org/reading-room/whitepapers/hackers/user-agent-field-analyzing-detecting-abnormal-malicious-organization-33874?show=user-agent-field-analyzing-detecting-abnormal-malicious-organization-33874&cat=hacker
- Instant Traffic Analysis with Tshark How-to, by Borja Merino, ISBN-13: 978-1-78216-538-5
- https://media.blackhat.com/bh-ad-11/Beek/bh-ad-11-Beek-Taming_Worms_RATS_Dragons-Slides.pdf

Thanks! Q&A?

Personal

@aboutsecurity

http://blog.ismaelvalenzuela.com

ismael.valenzuela@foundstone.com

Foundstone Team

@foundstone / @fsemea

http://www.youtube.com/
OpenSecurityResearch

http://blog.opensecurityresearch.com

Free tools & whitepapers:

http://www.foundstone.com

McAfee
An Intel Company


McAfee®
An Intel Company