



1

ToorCon 11

Cyber Criminals Don't Sleep, *So Why Does our Industry?*

Will Gragido | CISSP, CISA, IAM, IEM

John Pirc | CEH, IAM, SANS Thought Leader

Cassandra Security

Analysis of the Security Industry and all that it influences

Agenda

- Profiling the Cyber Criminal Mind
- Evolution of Cyber Criminal Activity
- Next Generation Cyber Threats
 - **Advanced Persistent Threats (APT)**
- Question and Answer

Profiling the Cyber Criminal Mind

- **Forensic Psychology**

- Personality profiles are based on the way in which a crime is committed, *modus operandi*
- *Aides in establishing the identity of the perpetrator*

- **Cyber-Criminal Analysis**

- Profiles utilized to establish localized and global *modus operandi*
- *Based on several determining factors*



Evolution of Cyber Criminal Activity

- **When:**
 - August 2008 Department of Justice announced the largest hacking and identity theft case ever prosecuted in the United States
- **Where:**
 - United States, Estonia, Ukraine, The People's Republic of China, Belarus
- **What:**
 - Charged With The Following:
 - Theft and sale of more than 40 million credit and debit card numbers
- **How:**
 - Obtained via System Compromises using generically available malware
- **Target:**
 - TJX, OfficeMax, Barnes & Noble, Sports Authority...

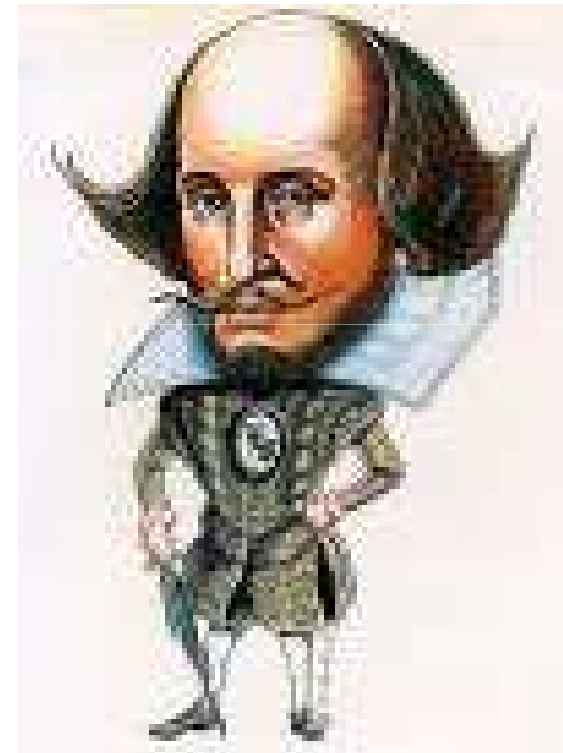
Past...Present...Future

Cassandra Security

Analysis of the Security Industry and all that it influences

Next Generation Cyber Threats (Here Today, Gone Tomorrow)

- What's in a name and MS Tuesday
- Crimeware as a Service
 - Hacking as a Service
 - Polypack
 - Spamming as a Service
 - DDoSing as a Service
 - Botnetting as a Service
 - Soc'ing as a Service
- Designer Malware
 - If you can build it, they will come to you with specific needs...
- Opportunistic Targets (Retail -> Critical Infrastructure)



Cassandra Security

Analysis of the Security Industry and all that it influences

The Cyber Jihad & “Common Cause” Attack Tools

- New social networks take up collective “arms” to target disliked organizations
- Largely bandwidth consumption orientated attacks
- Free tools to enable mass attacks
 - Multi-threaded HTTP GET Flooder
 - Similar to old ICMP PING flooders
- Open-source versions available for DIY authors and new “causes”



Cassandra Security

Analysis of the Security Industry and all that it influences

Evolutionary Tactics for Malware Testing

- KIMS – English/Spanish
 - Requires attacker to install all the AV products themselves
- ScanLix
 - "install & forget" philosophy – just update from time to time.
 - ... see the different signature files being updated.
 - ...disadvantage is the limited number of engines it uses.

The image displays two screenshots related to malware testing. The top screenshot shows the VirusTotal interface, which is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. The interface shows a file named 'test.rtf' received on 2009.10.22 01:42:53 (UTC) and currently in a 'scanning' status. Below this, there is a table listing various antivirus engines and their versions and last update dates.

Antivirus	Version	Last Update	Result
a-squared	4.5.0.41	2009.10.22	-
AhnLab-V3	5.0.0.2	2009.10.21	-
Authentium	5.1.2.4	2009.10.21	-
Avast	4.8.1351.0	2009.10.21	-
AVG	8.5.0.420	2009.10.21	-
BitDefender	7.2	2009.10.22	-
ClamAV	0.94.1	2009.10.22	-
Comodo	2684	2009.10.22	-
DrWeb	5.0.0.12182	2009.10.22	-
eSafe	7.0.17.0	2009.10.21	-
F-Prot	4.5.1.85	2009.10.21	-
F-Secure	9.0.15300.0	2009.10.20	-

The bottom screenshot shows the ScanLix interface, which is a multi-antivirus scanner. It displays a list of AV engines and their status (Fix, UnFix, Do It). The interface also shows a table of scan results for a file named 'C:\beto1.exe'. The results show that the file is infected with several viruses, including Backdoor.Win32.Bifrose.E, Backdoor.Win32.Bifrose.J, and Trojan.Exploit.Win32.DComAD. The scan is completed, and the word 'terminado' (finished) is displayed in green.

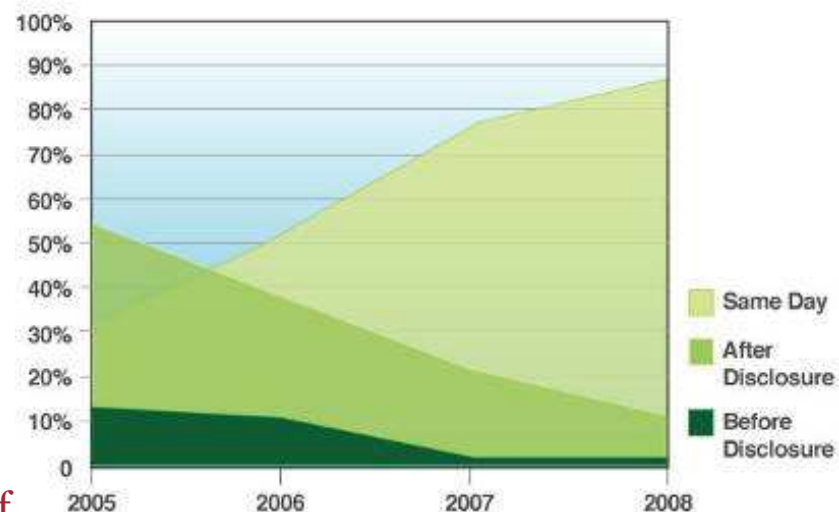
Cassandra Security

Analysis of the Security Industry and all that it influences

Exploit code availability (Time to Protection)

- New browser and plug-in exploits are in high demand
 - o-day exploit for IE/FF = \$25,000-\$75,000
 - Same-day exploit = \$2,000-\$30,000
 - Up to 3-days old exploit = \$5-\$500
- Drive-by-download exploit packs and support services increase spread of new exploits
 - Managed services and C&C distribution
 - New exploits can be propagated to thousands of sites/engines within seconds

Rise in 0-day Exploits



source: IBM X-Force®

Threats Have Advanced

- People
 - Underestimate threat → introduce risk
 - Lack InfoSec knowledge and experience
 - Often not empowered by stake holders due to lack of alignment with business
- Process
 - What Gets Measured Is Supposed To Get Results
 - Horrible IT metrics at best
 - Focus on compliance vs. security
- Technology
 - Deep holes in network visibility that must be addressed



Focus on Compliance Versus Security

The bad & the ugly....

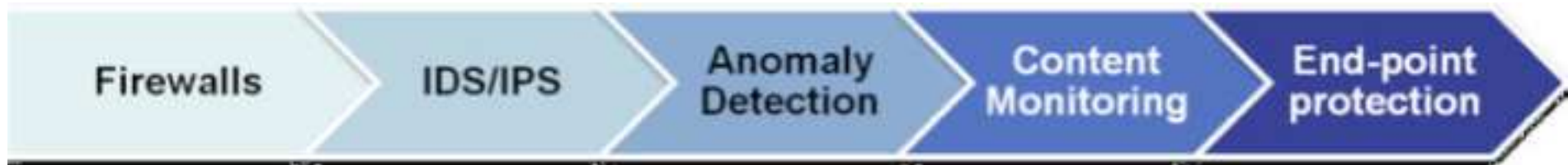
The good....



Compliance vs. Security

Source: Netwitness

Network Visibility and Situational Awareness (Gaps Are Critical)



- Unfortunately, “defense-in-depth” has been built upon a series of point solutions offering incomplete capabilities:
 - Signature based detection
 - Zone segmentation
 - Access controls
 - Packet filtering
 - Content monitoring
- This approach leaves many potential gaps in your network visibility, exploited by your top adversaries today:
 - Application attacks
 - Zero-day threats
 - Data loss events
 - Designer malware

Advanced Persistent Threats

Cassandra Security

Analysis of the Security Industry and all that it influences

Advanced Persistent Threat (Selective, Sophisticated and Silent)

HackingTheUniverse

Advanced Persistent Threat

APT or Advanced Persistent Threat describes cyber attacks mounted by organizational teams that have deep resources, advanced penetration skills, specific target profiles and are remarkably persistent in their efforts. They tend to use sophisticated custom malware that can circumvent most defenses, stealthy tactics and demonstrate good situational awareness by evaluating defenders responses and escalating their attack techniques accordingly.

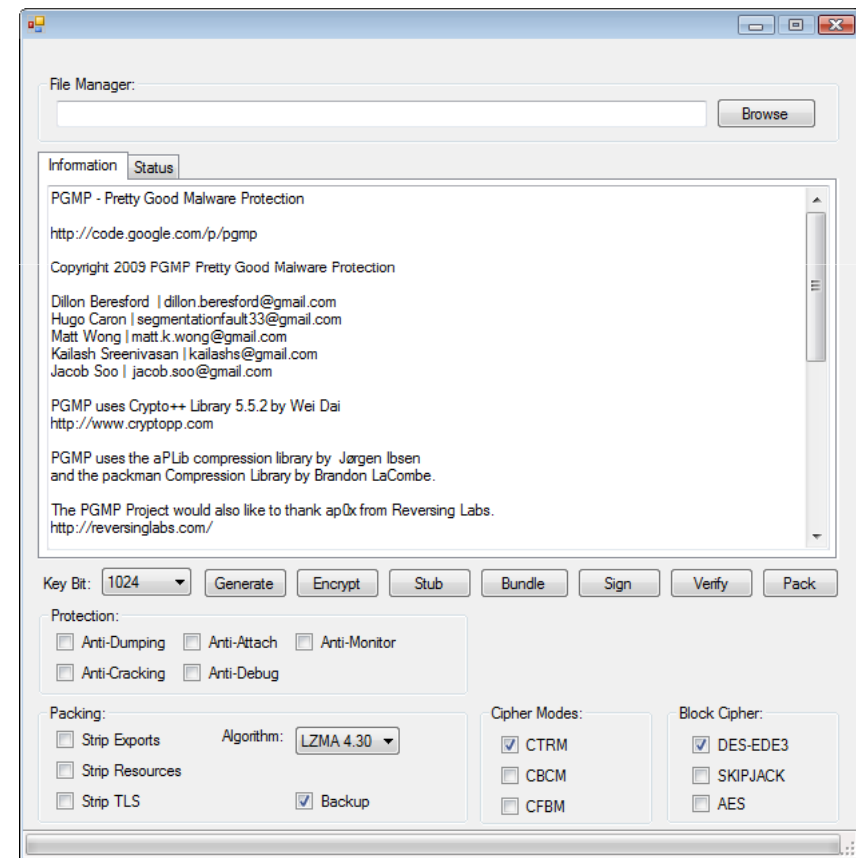
Advanced Persistent Threat (Selective, Sophisticated and Silent)

- Solomon said it best
- Slow, silent and deadly
- What's in not having a name: Encryption, Beacon's, Custom, Blended...
- Recent Examples
- What Are The Recommendations for Addressing it?

Advanced Persistent Threat (Methodology)



- Information Acquisition
 - Data Collection Types
 - Social Engineering
- Credential Acquisition
 - Beyond Spear Phishing
- Cyber Trade Craft
 - Communication Channels
 - Clear Text to Crypto



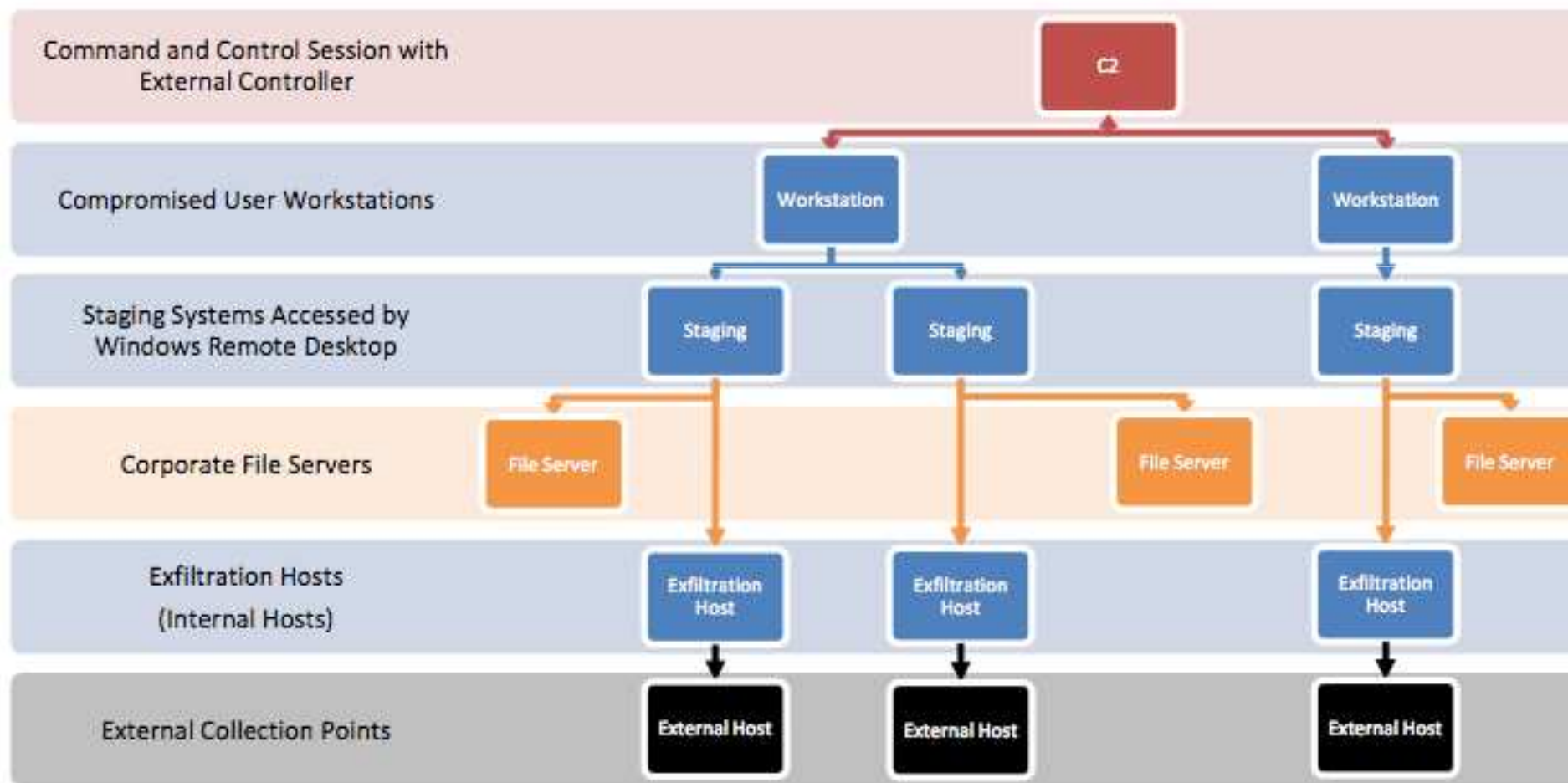
Source: Northup Grumman, Netwitness, Komodo KPMG

Cassandra Security

17

Analysis of the Security Industry and all that it influences

Advanced Persistent Threat (Framework)



Source: Northrup Grumman

Cassandra Security

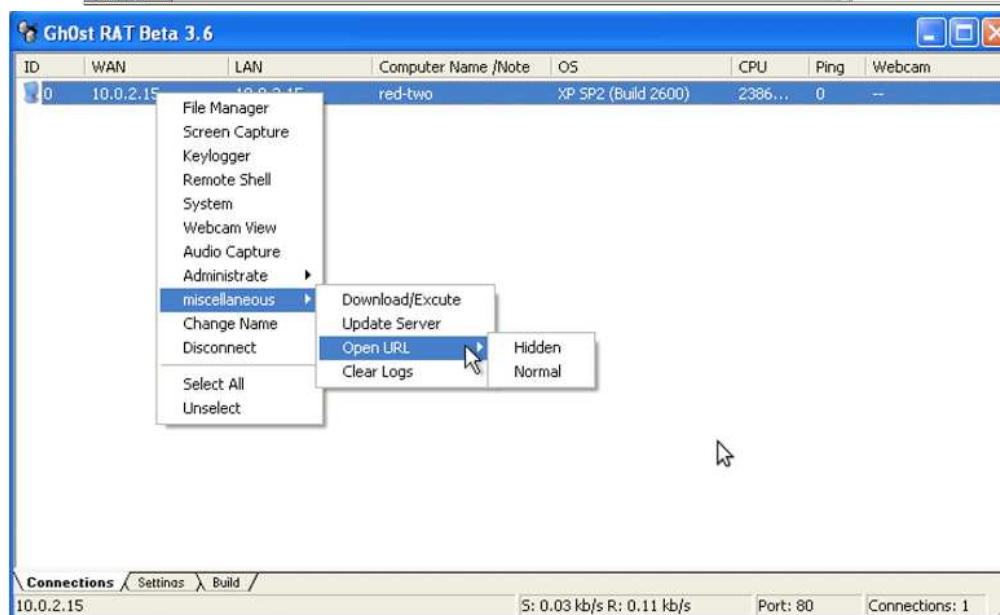
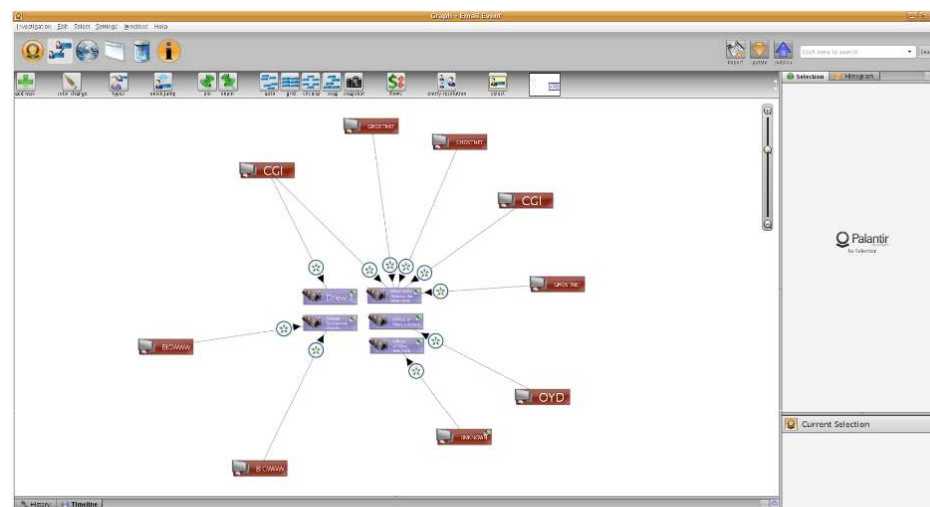
Analysis of the Security Industry and all that it influences

Public APT Activity

(Ghost Net) aka Byzantine Foothold

What Happened?

- **Verified in 103 countries**
 - Over 1,295 infected hosts identified
 - Impacts + / - a dozen computers on a weekly basis
- **Commonly Used Tools (Not Too Sophisticated):**
 - Remote access tool called ghost RAT (Remote Access Tool)
 - Data harvest
 - Email siphoning
 - Listening / Recording of Conversations via microphone and / or webcams



Source: Information Warfare Monitor

Uncovering the Unknown (Separating the Boys from the Men)

Cassandra Security

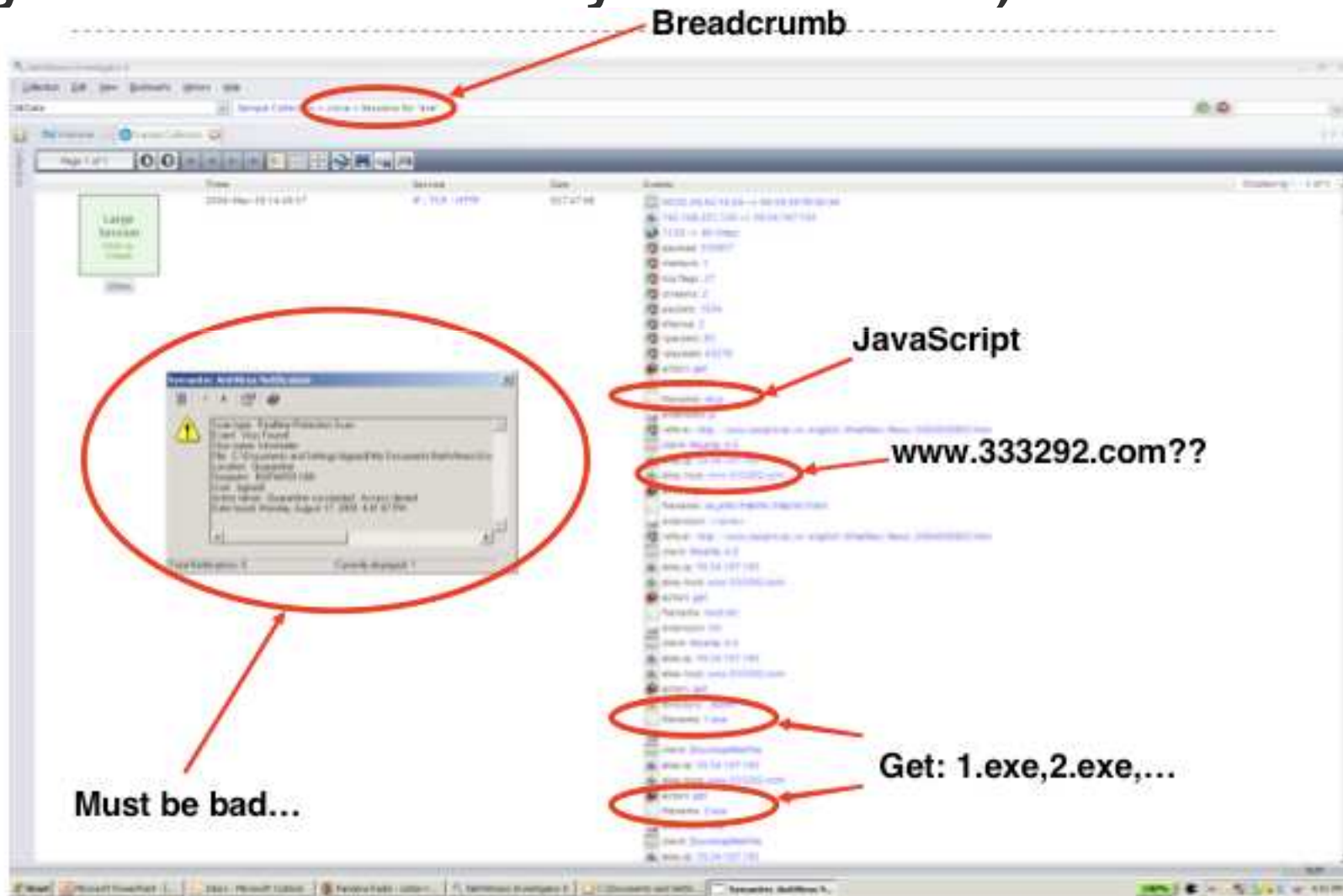
Analysis of the Security Industry and all that it influences

Cassandra Security

Analysis of the Security Industry and all that it influences

Analysis from Netwitness

(why session based analysis is needed)



Source: Netwitness

Summary

Cassandra Security

Analysis of the Security Industry and all that it influences

Key Points

- The Importance of Cyber Criminal Analysis
- Known Current Solutions Not Good Enough
- Regulatory Compliance != Security
- Advanced Persistent Threat Will Become Pervasive
- What are you doing to tackle the problem?

Thank You!

Contact Information:

will@cassandrasedecurity.com

john@cassandrasedecurity.com

www.cassandrasedecurity.com

Cassandra Security

Analysis of the Security Industry and all that it influences