



**And Now for Something
Completely Different:
Influencing Threat Behavior**

Notes

Not part of the deck...

- Thousands of hackers, criminals, terrorists, and nation/state actors with malicious intent spend their days finding the gaps in the security of these new technologies. Do we continue to focus on an arbitrary number stating that there is more good code than bad out there today? Do we continue to play whack-a-mole with security patches on systems that can never be 100% secure? Yes, we have to continue to get better at what we are doing, build more secure systems and embed security infrastructure throughout our information infrastructure. However, we have to do more! We have to find new ways to thwart the tide of malicious code and influence the human behavior that is behind of it all.
- To overcome this threat to our national security, culture and livelihood, we have to develop an approach or many approaches focused on the threat and the ability to influence their behavior. This requires rendering hacking a low-payoff pursuit with a high risk. If the cyber security community could expand its efforts toward this, it is quite likely that hacking could be reduced or at least stifle its growth. How to do that? One promising approach involves deciphering the motivations behind malicious cyber attacks, rather than just looking at the activity itself. Here's why: if those tasked with protecting networks can figure out why hackers are hacking, there are ways to deter hackers, narrow the targets we have to defend and change their behavior. An effective defense must be based on understanding the human being behind the keyboard in order to anticipate his actions, as well as to understand what he is after.
- It will not be easy to begin thinking in brand new ways, but the cyber security community must coordinate and collaborate to change the current paradigm. With the exponential growth of new malware, we have to do something different. Our goal should be to make hacking a high risk proposition with minimal pay off and render the probability of occurrence much, much less likely to occur. Focusing on malcode and installing more security products that may quickly become outdated and porous is neither adequate nor robust enough. Studying the hackers, how they operate, and understanding their motivations to disrupt their efforts will support the cyber security community's ability to fend off the threat. This session will offer ways to render malicious cyber activity a low-payoff pursuit with real world, high risk consequences in and outside of cyber space.

2

Clarification...

- What is your definition of the word “threat?”
- What should it be?
- Is it the malware?
- Or is it the person behind the keyboard?

This session's purpose

1. Explain that current cyber security efforts are not enough to stop the flood of new malicious code and actors affecting our nation's critical information, infrastructure and key resources.
2. Establish the culture and motivation behind the individuals who develop malicious code or conduct malicious activity on the Internet.
3. Identify a new approach to taking on the ever-growing sophisticated threat community.
4. Offer ways to influence behavior and reduce malicious activity, not just defend against it.
5. Challenge you all to develop ways and means to focus on the human element to deter or curtail malicious behavior.
6. Take your feedback from today's session and present it to US-CERT leadership in the form of a white paper. I intend to add every name here to the list of contributing authors.

How bad is it?

- ***Over 3 billion malware attacks in 2010***
- ***286M+ types of Malware identified in 2010***
- 93% Increase in Web Attacks in 2010 over the volume observed in 2009.
- Rustock, the largest botnet observed in 2010, had well over 1 million bots under its control.
- 6,253 New Vulnerabilities
- Observed an underground economy advertisement in 2010 promoting 10,000 bots for \$15.

Source: Symantec Internet Security Threat Report dated April 2011

What's the so what?

- Its affects the economy:
 - Average cost per incident of a data breach in the United States was \$7.2 million
 - Largest breach costing one organization \$35.3 million to resolve.
- Its personal:
 - 260,000 average number of identities exposed per Breach
 - \$0.07 to \$100 per Credit Card the range of prices seen advertised in the underground economy
- It has National Security implications...

Source: Symantec Internet Security Threat Report dated April 2011

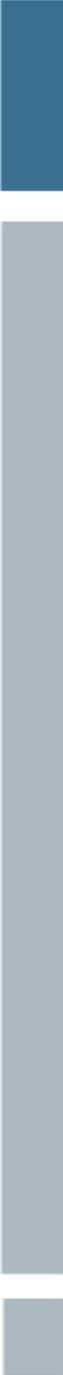


DO YOU AGREE?

7

And Now for Something Completely Different: Influencing Threat Behavior – Matt Stern
GFIRST 2011

GENERAL DYNAMICS
Advanced Information Systems



WHY IS THE PROBLEM GROWING?

THE THREAT IS...

Agile, brilliant and committed

Exploit Technique	Counter-Measure	Threat Response
Malware (virus, worm, Trojan horse)	Anti-virus programs	Fake anti-virus programs
Key stroke loggers (stolen credentials)	Two factor authentication	Exploit the infrastructure supporting the tokens
Use non-standard ports or services for malicious C2 or data exfiltration	Minimize ports and services available	Use legitimate service ports maliciously
Install “root-kits” for remote control	Computer forensics tools and root-kit detection tools	Obfuscate or Booby-trap malware in good code
Attack or negate built in security	Trusted Platform Module (TPM)	Remotely deployed BIOS root- kit
Code Obfuscation	Hashing algorithms	MD5 collision; supply chain evil twin
Social Engineering	User Training and awareness	Social Engineering + Social Networking
Exploit operating system vulnerabilities	Harden the operating system; implement host based security	Exploit applications and web vulnerabilities

Incentivized (motivated by profit)

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card Information	32%	21%	\$0.06-\$30
2	2	Bank account credentials	19%	17%	\$10-\$1000
3	9	Email accounts	5%	4%	\$0.10-\$100
4	3	Email addresses	5%	6%	\$0.33/MB-\$100/MB
5	12	Proxies	4%	3%	\$0.16-\$20
6	4	Full Identities	4%	6%	\$0.70-\$60
7	6	Mallers	3%	5%	\$2-\$40
8	5	Cash out services	3%	5%	8%-50% or flat rate of \$200-\$2000 per item
9	17	Shell scripts	3%	2%	\$2-\$20
10	8	Scams	3%	5%	\$3-\$40/week for hosting, \$2-\$20 design

Table courtesy of Symantec Global Internet Security Threat Report dated April 14, 2009

A Gray Market has fueled an underground industry of vulnerability discovery and exploit code development.

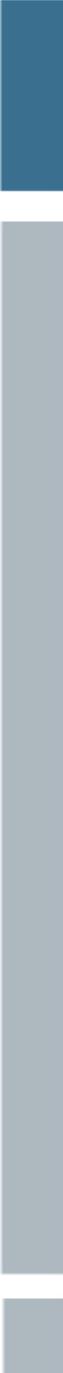
Promoting a cause or themselves

The image is a collage of several 'HACKED!' banners and screenshots. At the top left, a browser window shows 'http://experts.microsoft.fr/'. Below it, a large black banner with 'HACKED!' in white text. To its right, a smaller black banner with 'HACKED' in large, semi-transparent letters. Further right, a red banner with a white crescent and star logo, 'www.turkmilliyetçileri.org', and 'HACKED BY' in red. Below these, a white box contains the text: '@LulzSec The Lulz Boat We aren't hacktivists, whitehats, greyhats or blackhats - categorizing deflates the lulz lizard creativity lasers.' To the right of this box is a screenshot of a website with 'FUCK YOU ADMIN PUTIN MOTHER FUCKER!' and 'OWNED BY WTC.LaGend AND kaAppVp0x'. Below the LulzSec box is a black banner for 'Mafia Hacking Team' with 'HackeD By MazHaR_FasHiS' and 'Our Slogan : Vulnerability Is Possible !!!'. At the bottom right, another screenshot shows two men in suits pointing guns, with 'Powered By Turkish Hacker' and 'YOU UNBAN ME THEN I OR I KEEP HACKING YOUR SITE'.

The threat is also:

- Unencumbered by social norms, pressures, morals or laws
- Undeterred
- Translating virtual reality into real world affects (e.g. money and information theft)
- Not risk averse...

*Low Risk + High Payoff =
High Probability of Occurrence*



**ARE CURRENT
METHODOLOGIES AND
TECHNIQUES EFFECTIVE?**

WHERE'S THE FOCUS?

My theory

- Security of cyberspace cannot be solved with technology alone
- Affect the human element of the equation
- Deter behavior through tangible consequences
- Suppress the growth of development of exploits and discovery of vulnerabilities
- Inflict consequences and suppress threat motivations to create a new risk model for the threat:

High Risk + Low Payoff =

Low Probability of Occurrence

Starve the malware economy

- Focus on identifying money trails and ways to interdict its flow of capital
- Hamper commerce involving the distribution of malicious code, root kits or other exploit tools
- Identify ways to drive up production costs for the development of malicious code, root kits or other exploit tools

Undermine the threat social fabric

- **Redirect:** Some threat actors are like pro athletes without a playing field
- **Engage:** Technical forums to develop respect and understanding
- **Dishonor:** Affect credibility and deflate status
 - Hacker should have the same connotation as thief, spy or vandal
 - Public relations campaign focused on making malicious threat activity socially unacceptable
- **Expose:** Be aggressive and expose the threat
 - Attribution, attribution, attribution
 - Do not treat it like an online game

Use “real world” techniques

- Dye Packs
 - Bank robbers have the initiative and skills to choose the time and place of the robbery
 - Application to cyber security:
 - » Tag critical files
 - » Upon leaving their safe environment, activate an embedded program to delete the file or make unusable
- Self Defense – what are willing to let happen?
- Profiling threat behavior
- Developing plans to focus limited assets on mission essential resources

What else can we do?

Our theory

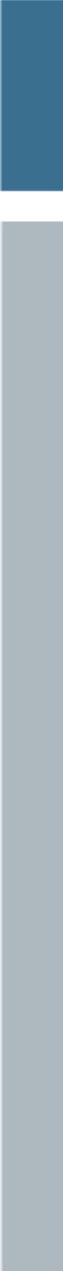
- Security of cyberspace cannot be solved with technology alone
- Affect the human element of the equation
- Deter behavior through tangible consequences
- Suppress the growth of development of exploits and discovery of vulnerabilities
- Inflict consequences and suppress threat motivations to create a new risk model for the threat:

High Risk + Low Payoff =

Low Probability of Occurrence

This session's accomplishments:

1. Gained consensus that current cyber security efforts are not enough to stop the flood of new malicious code and actors affecting our nation's critical information, infrastructure and key resources.
2. Gained understanding of the culture and motivation behind the individuals who develop malicious code or conduct malicious activity on the Internet.
3. Gained acceptance for a new approach to taking on the ever-growing sophisticated threat community.
4. Identified new ways to influence behavior and reduce malicious activity, not just defend against it.
5. Challenge you all to develop ways and means to focus on the human element to deter or curtail malicious behavior.
6. Take your feedback from today's session and present it to US-CERT leadership in the form of a white paper. I intend to add every name here to the list of contributing authors.



***Albert Einstein once said:
“We cannot solve our problems with the
same thinking we used when we created
them.”***

Matthew A Stern
Program Director, NCSD Support
General Dynamics Advanced Information Systems
12450 Fair Lakes Circle, Fairfax, Va. 22033
Cell: 703-232-7294