

# Classification of Malicious Tools in Underground Markets for Vulnerabilities

Jaziar Radianti & Nils Ulltveit-Moe  
NISK  
Kristiansand, 17 November 2008

# Contents

- Background
- The Purposes
- Definition
- Categorisation Approach
- Tools or Items Advertised in Black Markets (BMs)
- Malicious Tool's Objectives in BMs
- Supply Chain for BMs
- Sector and Size of BMs
- Mitigating the Impacts

## Background

- Recently, undisclosed exploits do not only circulate among underground insiders but are also traded in black markets.
- Huge financial losses occur from computer security incidents due to malicious actors' activity in underground markets.
- Law enforcement initiatives targeting underground markets for financial fraud were already initiated (e.g. *Operation Firewall*, *Operation Bot Roast II*)

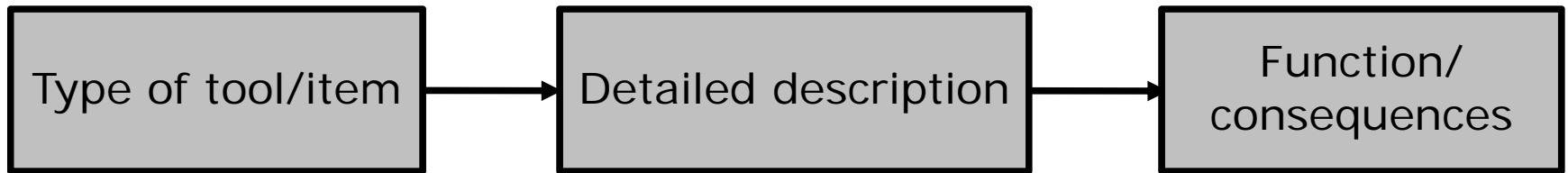
## The Purposes

- To identify, classify and analyse the type and function of malicious tools advertised in BMs.
- To discuss black market's characteristics, and the black market supply-chain.
- To discuss possible preventive actions from the exposure of the black market's threats.

## Definition

- BM for vulnerabilities is: *"an arena for illegal selling and buying activities, to trade vulnerability exploits and malware or any products or services taking malicious advantage of the weaknesses in software and computer networks"*.
- Vulnerabilities are: *"bugs and flaws (caused by programming errors) that give rise to exploitation techniques or particular attack patterns. The vulnerability term here is also extended to cover social vulnerabilities, which with some degree of success are exploitable by social engineering based techniques"*.

## Categorisation Approach



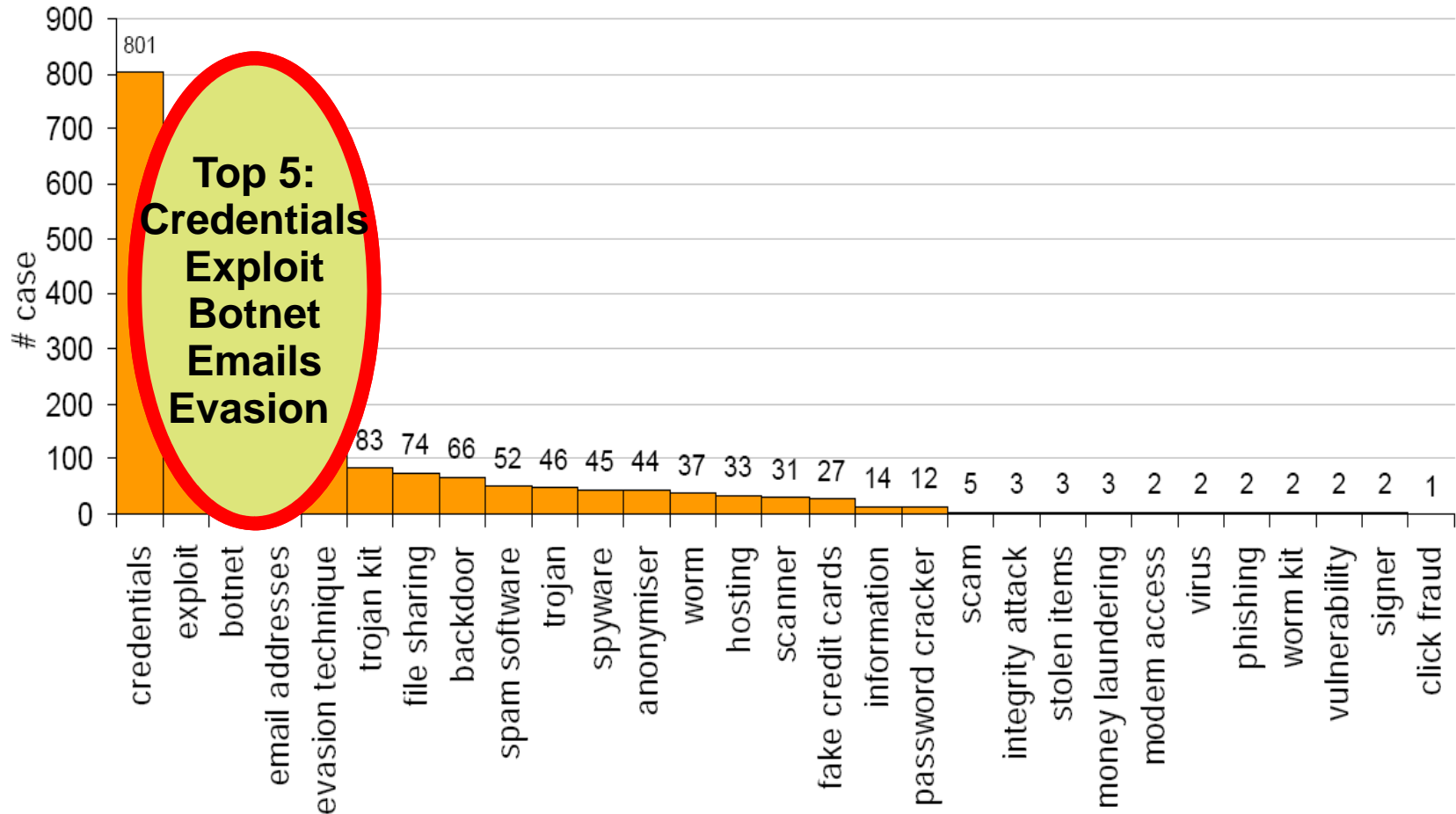
- *Type of tool or item*: a similar group of various tools or items traded underground.
- *Detailed description*: more specific attributes of the advertised underground goods and facilitates the identification of consequences.
- *Function/ Consequences* capture the possible impact from identified malicious tools in the black markets.
- A malicious tool sometimes supports multiple functionalities like a “swiss-army knife”.
  - One tool may fall into several functions or consequences.

## Data and BM Characteristics

- *Data acquisition method*: Disguised observation of online underground websites that possess BM feature during April 2006-May 2008.
- *Black market characteristics*:
  - Trading is either for money or by exchanging items or services.
  - *Disguised-pseudonymous* communities
  - *Meritocratic* communities
  - Illicit e-Business
  - Regular alteration of underground servers' geographical location--convenience-based.
  - Internal rules and ethics e.g. a verification system, permissible traded items, no flaming, no rip-off...
  - Requires some level of credence and integrity among malicious actors to keep black markets working.

# Number of Tools or Items Advertised in Black Market

Tools or items advertised in underground market



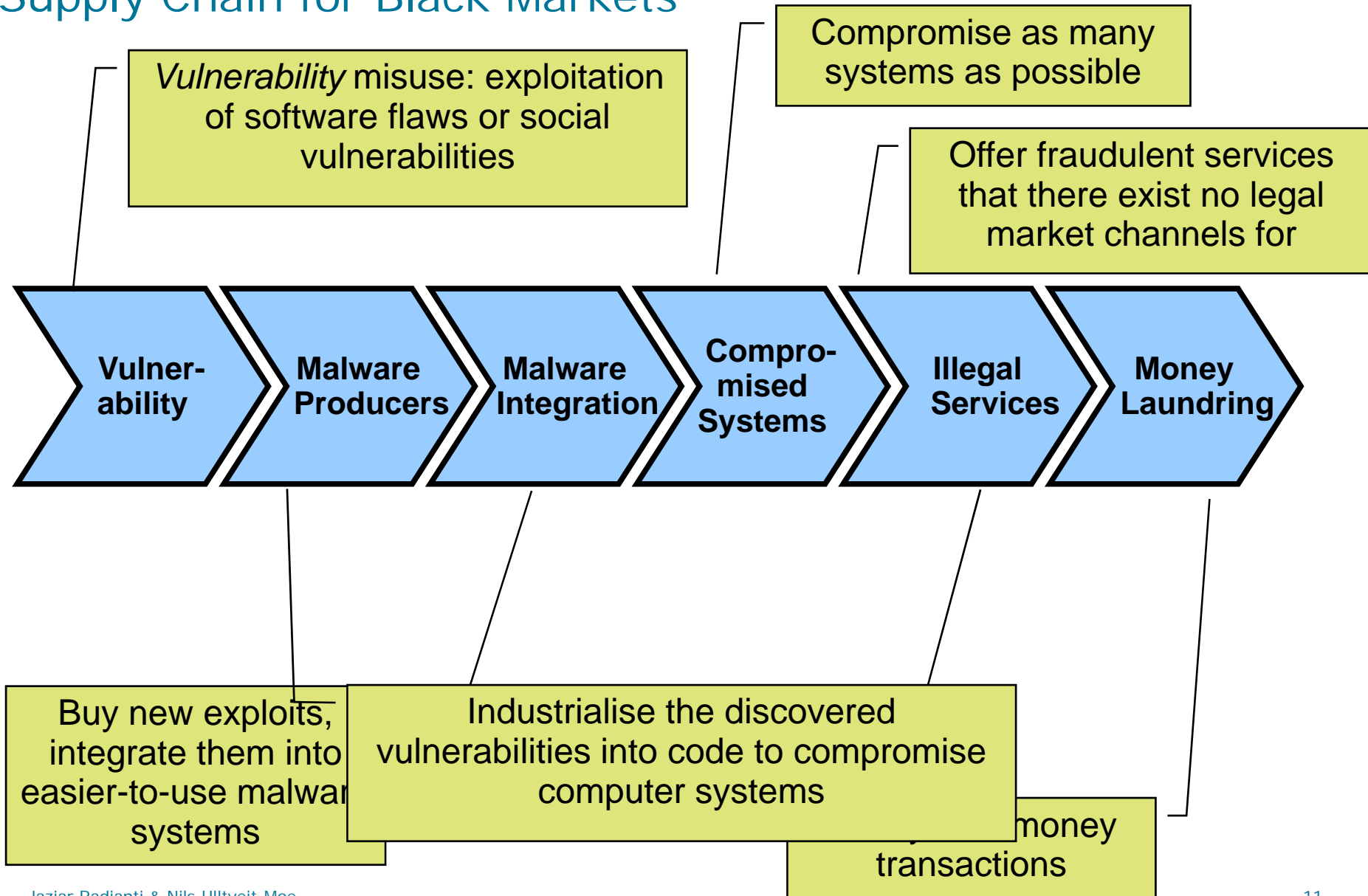
## Breakdown of Malicious Tool's Objectives in Black Markets

Malicious Tool's Objectives	Frequency	%
Spread information	199	9.5
Gain privilege	195	9.3
Financial fraud	167	8.0
Keylogging, DDoS, proxy, exploit, backdoor	143	6.8
Obfuscator	138	6.6
Game fraud	72	3.4
Credentials- file sharing warez	68	3.2
Information theft	67	3.2
Backdoor trojan, staged downloader	48	2.3
Forward traffic, anonymise traffic	44	2.1
DDoS, keylogging, backdoor, exploits, proxies, spamming	38	1.8
Bind infector to software make trojan	36	1.7
Compromise systems	30	1.4

## An Example of Vulnerabilities Exploited in Black Markets (BMs)

MD ID/ CVE ID	Discovery	Announced	Patch status	Exploit in BM	Severity	Note
MS07-009/ CVE-2006- 5559	2006-10-24	2007-02-13	Unknown	2008-05-14 (W6)	High, Remote Attack	Vulnerability in MSDA Component
MS06-014/ CVE-2006- 0003	Unknown	2006-04-11	Unknown	2008-05-14 (W6)	Critical, Remote Attack	Vulnerability in MSDA Component
MS07-004/ CVE-2007- 0024	2006-10-03	2007-01-09	Unknown	2008-05-14 (W6)	Critical, Remote Attack	Vulnerability in Vector Markup Language
MS07-005/ CVE-2007- 2217	Unknown	2007-10-09	Unknown	2008-05-14 (W6) 2007-04-12 (W1)	Critical Remote Attack	Vulnerability in Kodak Image Viewer in MS Windows 2000 SP4

# Supply Chain for Black Markets



## Sector and Size of BMs

Supply chain sector	Items	%	Original category
Vulnerabilities	2	0.1	Vulnerabilities
Malware producers	596	28.6	Exploit, evasion techniques, backdoor, trojan, spyware, worm, scanner, password cracker, integrity attack, virus, signer
Malware Integration	329	15.8	botnet, trojan kit, spam software, worm kit
Compromised Systems	801	38.5	Credentials
Illegal goods and services	349	16.8	email addresses, file sharing, anonymiser, hosting, fake credit cards, information, scam, modem access, phishing, click fraud
Money laundering	3	0.1	money laundering
(Other)	3	0.1	stolen items

## Mitigating the Impacts

- **Strengthen the authorities' role**
- **Minimise social vulnerabilities**
- **Minimise supply of vulnerabilities**

## Strengthen the authorities' role:

- Audit and certify on-line financial actors.
- Enforce transparency and traceability.
- Increase the risk of being detected.
- Make it harder to operate anonymously in the Internet.
  - Using both technical and legal remedies.

## Minimise social vulnerabilities:

- Increase security awareness among users.
- Enlighten computer users to be more aware of various malicious motives in cyber space.
- Computer systems should provide a “safety net” and inform about risky behaviour.

## Minimise supply of vulnerabilities:

- Better software engineering methods and tools.
- Better authentication models, strong cryptographic methods.
- Remunerate vulnerability findings through an open market.

Thank you!

Q & A?