



# Corporate Threats

Guillaume Lovet & Sr. Manager EMEA Threat Response Team

**PARTNER CONFERENCE 2009**  
9 - 10 June 2009 Fairmont St Andrews, Scotland

**FORTINET®**

# Agenda

**Risks for Enterprises  
and Infrastructures**

**Vectors of infection**

**Defence**

# Agenda

**Risks for Enterprises  
and Infrastructures**

**Vectors of infection**

**Defense**

# Risks: What you don't want to happen

- Denial of Service (DoS) attack
  - From outside, by a Botnet / Zombie network
  - From inside, on purpose or not (eg: Conficker)
- Data Theft
  - Via **stolen credentials** (Phishing / Social Engineering)
  - Via **Trojan Horses / Bots**
  - Data **Gathering** phase
  - Data **Exfiltration** phase
- Loss of Reputation
  - Top risk identified by UK companies (Aon Ltd, 2005)
  - Eg: Heartland payment system

# Loss of Reputation: Heartland Breach



■ Home ■ News ■ Travel ■ Money ■ Sports ■ Life ■ Tech

## Hackers breach Heartland Payment credit card system

Updated 1/23/2009 12:14 PM | Comments 79 | Recommend 81 | E-mail | Save | Print | Reprints & Permissions

By **Byron Acohido**, USA TODAY

Heartland Payment Systems (HPY) on Tuesday disclosed that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants.

### The Washington Post

TODAY'S NEWSPAPER  
Subscribe | PostPoints

[chives](#) | [Security Fix Live: Web Chats](#) | [E-Mail Brian Krebs](#)

### Payment Processor Breach May Be Largest Ever

A data breach last year at Princeton, N.J., payment processor **Heartland Payment Systems** may have compromised tens of millions of credit and debit card transactions, the company said today.

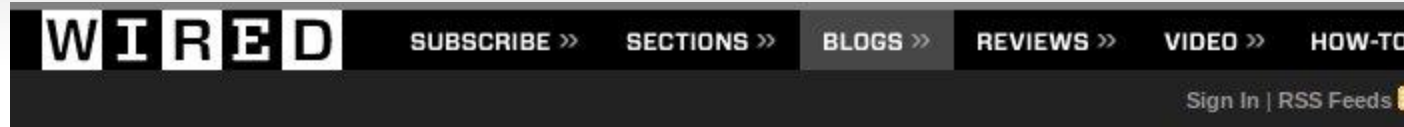
## Heartland Data Breach Could Leave 100 Million Accounts Exposed

By **Stefanie Hoffman**, ChannelWeb  
7:22 PM EST Wed. Jan. 21, 2009

Discuss This

In what could be the biggest security incident in history, Heartland Payment Systems announced on Tuesday that it was the victim of a data breach that possibly compromised more than 100 million accounts after malicious software was found in its payment processing system.

# Loss of Reputation: Heartland Breach



## THREAT LEVEL



PRIVACY, CRIME AND SECURITY ONLINE

### Heartland Breach Cost Company \$12.6 Million So Far

By Kim Zetter  May 7, 2009 | 5:42 pm | Categories: [Breaches](#)

Heartland Payment Systems reported on Thursday that the hack it experienced last year has cost the company \$12.6 million so far. The amount includes legal costs and fines from Visa and MasterCard, who say the company was not compliant with payment card industry rules.



Network World reports that [during the company's financial earnings call](#), Heartland executives acknowledged that the breach was a heavy financial burden that had not reached a final tally yet.

# Risks: Attackers' Motivation

- **Financial:** Blackmail / Ransom
  - Pay or I DdoS you!
  - Holding Intellectual Property
- **Competitive:** Intellectual Property Theft / Industrial Spying
  - Example: the “Israeli Trojan” case
- **Political**
  - Example: GhostNet

# Agenda

Risks for Enterprises  
and Infrastructures

Vectors of infection

Defense




# Multiple Infection Vectors


- **E-Mail & IM**
  - **Attachments: executable, archives AND documents**
  - **Links**
- **Web Sites**
  - The “Drive-By Install” attack strategy
  - “Packs” available for purchase on the underground market
  - 2008: the year of SQL injections
- **Social Networks**
  - Intelligence source for targeted attacks
  - Worms (eg: Koobface)
- **Physical Infection Vectors**
  - Laptops
  - USB Keys
  - CDs

You've received A Hallmark E-Card!

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** postcards@hallmark.com  
**Date:** Friday, March 06, 2009 11:59 AM  
**To:** [REDACTED]  
**Subject:** You've received A Hallmark E-Card!  
**Attach:**  postcard.zip (86.9 KB)

	Shop Online	Hallmark Magazine	Cards & E-Cards	<input checked="" type="checkbox"/> At Gold Crown
--	-------------	-------------------	-----------------	---

**You have received A Hallmark E-Card.**

Hello!

You have received a Hallmark E-Card from your friend.

To see it, check the attachment.

There's something special about that E-Card feeling. We invite you to make a friend's day and send one.

Hope to see you soon,  
Your friends at Hallmark

Your privacy is our priority. Click the "Privacy and Security" link at the bottom of this E-mail to view our policy.


Hallmark.com | Privacy & Security | Customer Service | Store Locator

You've received A Hallmark E-Card!

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** hallmark.com  
**Date:** Friday, March 06, 2009 7:10 AM  
**To:** [REDACTED]  
**Subject:** You've received A Hallmark E-Card!

	Shop Online	Hallmark Magazine	Cards & E-Cards	In Gold Crown Stores
--	-------------	-------------------	-----------------	----------------------

**You have received A Hallmark E-Card.**

Hello!

You have received a Hallmark E-Card.

To see it, click [here](#).

There's something special about that E-Card feeling. We invite you to make a friend's day and **send one**.

Hope to see you soon,  
Your friends at Hallmark

Your privacy is our priority. Click the "Privacy and Security" link at the bottom of this E-mail to view our policy.

Hallmark.com | Privacy & Security | Customer Service | Store Locator

[http://\[REDACTED\]sites.com/hallmark/postcards/postcard.gif.exe](http://[REDACTED]sites.com/hallmark/postcards/postcard.gif.exe)



# Targeted attacks against Tibetan communities: Email infection

All,

Attached here is the update Human Rights Report on Tibet issued by Department of State of U.S.A on March 11, 2008.

You may also visit the site:

Tashi Deleg,

Sonam Dagpo

Secretary of International Relations  
Department of Information & International Relations  
Central Tibetan Administration  
Dharamshala -176215  
H.P., INDIA  
Ph.: [obfuscated]  
Fax: [obfuscated]  
E-mail: [obfuscated]@gov.tibet.net or diir-pa@gov.tibet.net  
Website: <http://www.tibet.net/en/diir/>

# Targeted attacks against Tibetan communities: Email infection

- Exploits (source ISC SANS)

**CHM** Help files with embedded objects;

CVE-2008-0655: Acrobat Reader **PDF** exploit

CVE-2006-2492, CVE-2007-3899: **Word**

CVE-2006-3590, CVE-2006-0009: **Powerpoint**

CVE-2008-0081: **Excel**

CVE-2005-0944: **Microsoft Access**

CVE-2006-3845: LHA files exploiting vulnerabilities in **WinRAR**.

# Multiple Infection Vectors

- E-Mail & IM
  - Attachments: executable, archives AND documents
  - Links
- **Web Sites**
  - **The “Drive-By Install” attack strategy**
  - **“Packs” available for purchase on the underground market**
  - **2008: the year of SQL injections**
- Social Networks
  - Intelligence source for targeted attacks
  - Worms (eg: Koobface)
- Physical Infection Vectors
  - Laptops
  - USB Keys
  - CDs

MPack v0.86 stat




Attacked hosts: (total/uniq)

IE XP ALL	87093 - 79152
QuickTime	37 - 34
Win2000	3953 - 3393
Firefox	18028 - 17796
Opera7	25 - 25

Traffic: (total/uniq)

Total traff:	112525 - 102044
Exploited:	13765 - 10705
Loads count:	14103 - 5224
Loader's response:	102.46% - 48.8%
User blocking:	ON
Country blocking:	OFF

Efficiency: 12.53% - 5.12%

Country	Traff	Loads	Efficiency
 IT - Italy	76625	11539	15.06
 ES - Spain	8042	466	5.79
 US - United states	3877	133	3.43

# Multiple Infection Vectors

- E-Mail & IM
  - Attachments: executable, archives AND documents
  - Links
- Web Sites
  - The “Drive-By Install” attack strategy
  - “Packs” available for purchase on the underground market
  - 2008: the year of SQL injections
- **Social Networks**
  - **Intelligence source for targeted attacks**
  - **Worms (eg: Koobface)**
- Physical Infection Vectors
  - Laptops
  - USB Keys
  - CDs





Leo > **Youtube**

▶ Slideshow

✉ Share

Download ▾

Prints ▾

Photo 1 of 1 [«View album](#)



[http://\[redacted\].info/go/fb.php?\\_ENTER\\_&\\_SEE\\_VIDEO](http://[redacted].info/go/fb.php?_ENTER_&_SEE_VIDEO)



Leo

COOL!

Oct 29, 2008 6



Jan

Why cant I open the flippen video. Ive got Flash player 10

Oct 29, 2008 7

Video ActiveX Object Error.



**Video ActiveX Object Error:**

Your browser cannot display this video file.

You need to download new version of Video ActiveX Object to play this video file.

Click Continue to download and install ActiveX Object.

Continue

Cancel

Details...

# Multiple Infection Vectors

- E-Mail & IM
  - Attachments: executable, archives AND documents
  - Links
- Web Sites
  - The “Drive-By Install” attack strategy
  - “Packs” available for purchase on the underground market
  - 2008: the year of SQL injections
- Social Networks
  - Intelligence source for targeted attacks
  - Worms (eg: Koobface)
- **Physical Infection Vectors**
  - **Laptops**
  - **USB Keys**
  - **CDs**

# Agenda

Risks for Enterprises  
and Infrastructures

Vectors of infection

Defense

# Key Elements to Modern Defense



You need AV, IPS, AS, WCF

Above all, you need them **altogether**

And most importantly, you need them **working altogether**

Goal: when facing a threat, be able to tackle it from **different angles**

=> **Intelligent Redundancy**

# Two Examples of Enhanced Security by Intelligent Redundancy



## Phishing

- Phish Letter blocked by **AS**
- If not, blocked by **AV**
- If not, Phish Site blocked by **WCF**

## Backdoor / Bot

- Binary blocked by **AV**
  - If not, access to C & C blocked by **IPS**
  - If not, by **WCF**
- => The bot cannot “phone home”

# Example of IPS antibackdoor signature (simplified)

```
F-SBID( --vuln_id 17280; --attack_id 20488; --name "Backdoor.EvilFTP";  
--group backdoor; --protocol tcp; --default_action pass; --revision  
2602; --severity medium; --app Other; --os Windows; --status disable;  
--flow from_server; --service FTP; --pattern "220- Welcome To EvilFTP  
:)|0d 0a|"; --data_size >100; --seq =,1,relative; )
```



**Thank you**