



Koobface on Facebook:

How malicious contents sneak into social networking

Mohammad Reza Faghani



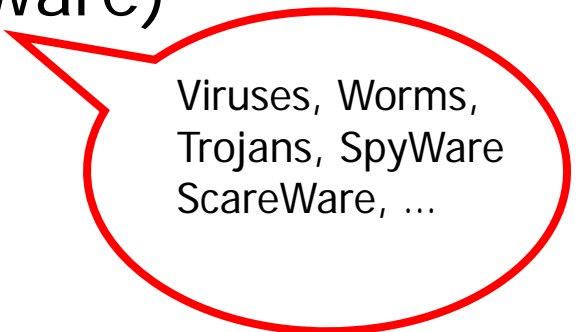
Outline

- Introduction
- Trend of Web malware
- Social networks malware
- What is XSS !?
- Potentials of XSS Worms
- Social Networks
- XSS worm propagation
- ClickJacking malware propagation
- Trojan malware propagation
- Summarizing the results from various studies
- Recent study results
- Our proposed scheme for malware detection
- Conclusion



Introduction

- Four key threats to consider
 - Spam
 - Bugs
 - Denial of Service
 - Malicious Software (malware)
 - Propagate via Spam
 - Exploits bugs
 - Mount DOS



Viruses, Worms,
Trojans, SpyWare
ScareWare, ...

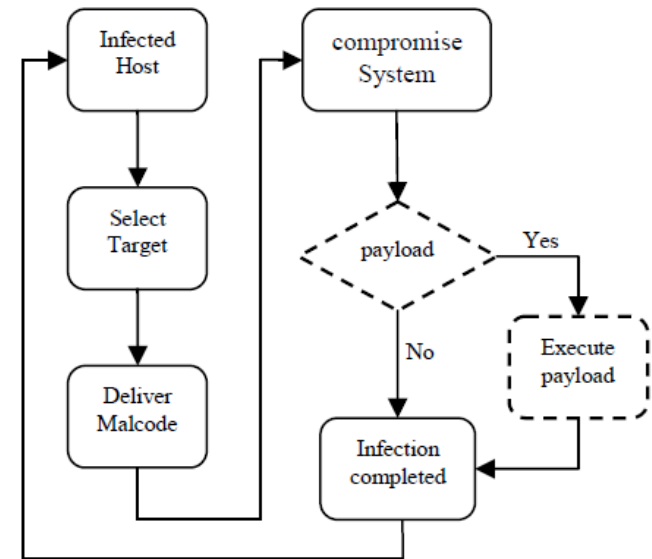


Introduction (cont.)

- Why is malware so important to study?
 - Privacy and security issues
 - Cyber War
 - → Stuxnet, Predator Drone
 - ISPs struggle under virus generated traffic
 - Cyber Criminals make a lot of money
 - Hidden costs
 - Reputation

Introduction (cont.)

- Malware is propagated via
 - Email
 - P2P networks
 - Vulnerable OS services
 - Mobile phones
 - Web
- Can even be Hybrid



Trends of Web malware



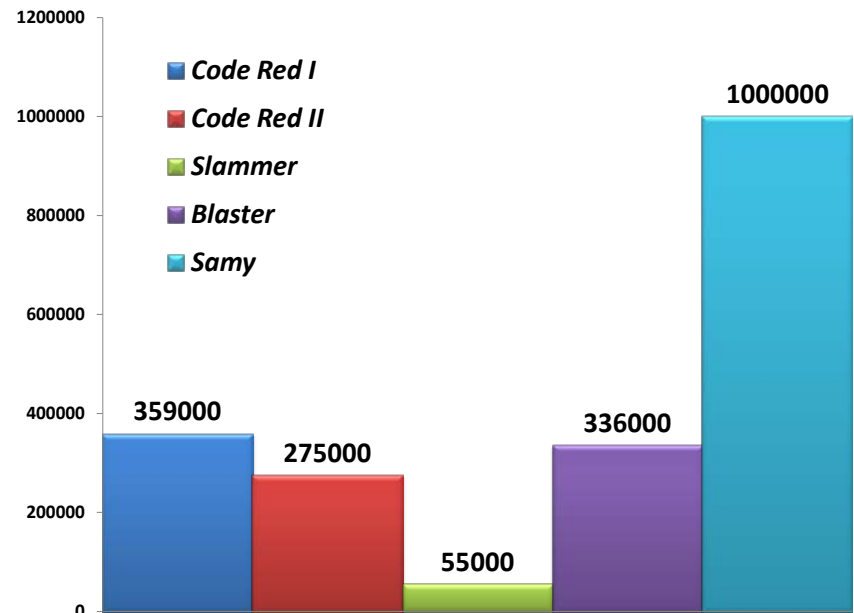
larger than other

- 80% of web security incidents are caused by Web users who prefer to exploit Web users
- Aggregated traffic from such as XSS (vulnerabilities) would be huge

Suppose each active user has on average 128kbps of bandwidth, potential of 10 percent of active users is :
 $80M \times 128\text{kbps} = 10\text{ Tbps}$

Social networks malware

- Samy could affect over 1 million people in less than 20 hours.
- MySpace was the first but :
 - Sina, July 2011
 - FB on March 29, 2011
 - ClickJacking types
 - Almost everyday
 - Twitter on Sep. 2010
 - ...



First Microblog Attack in China

Updated: 01 Jul 2011 | Translations available: [日本語](#)



Livian Ge SYMANTEC EMPLOYEE

Symantec. | Official Blog

The Sina microblog is the biggest microblogging platform

New XSS Facebook Worm Allows Automatic Wall Posts

Posted: 29 Mar 2011 | Translations available: [日本語](#)

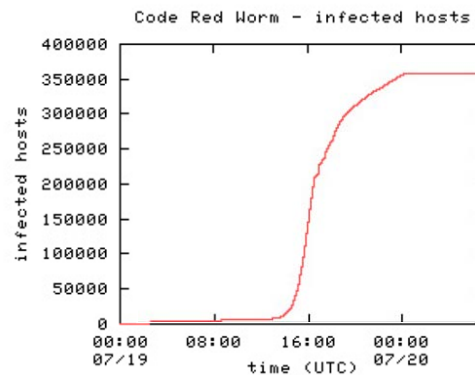
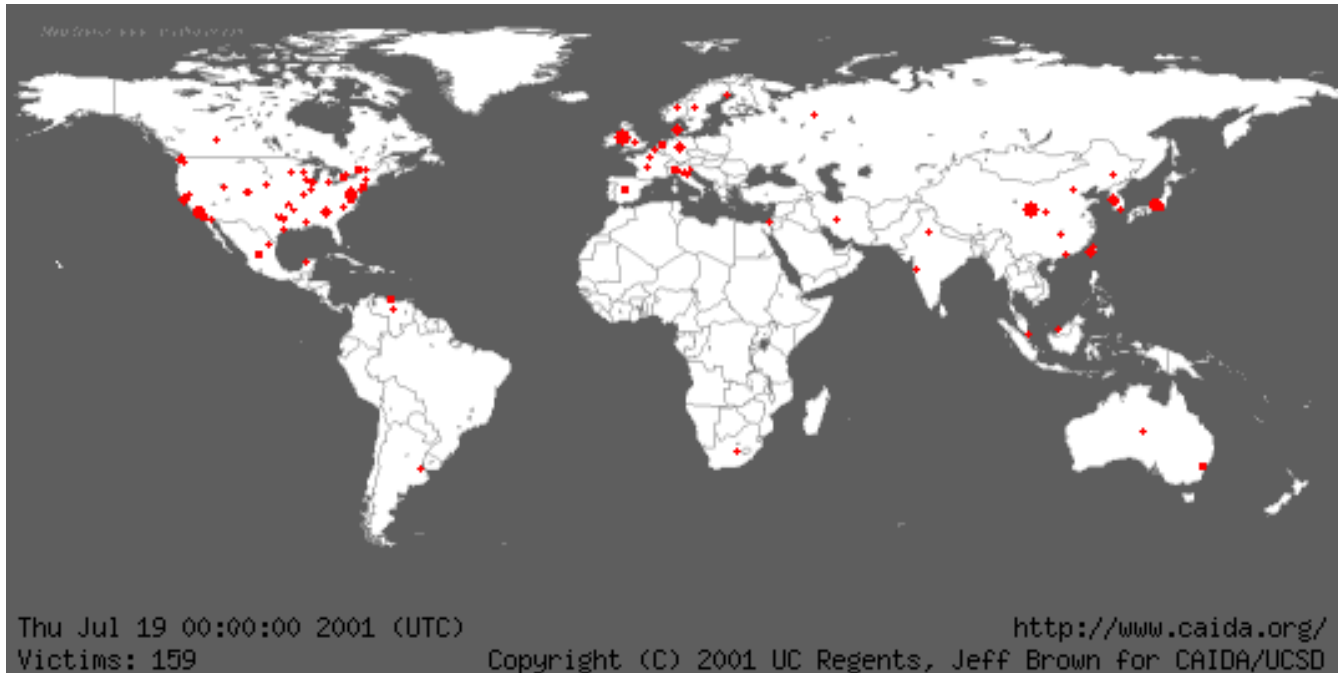


Candid Wueest SYMANTEC EMPLOYEE

Symantec. | Official Blog

+1
1 Vote

Propagation of a Malware





Why studying malware ?

- To have a better understanding of propagation behaviors
- Damage assessment
- Providing enough traffic to avoid Denial of Service
- Detecting the weaknesses of spreading
 - How we can counter-measure in the best way

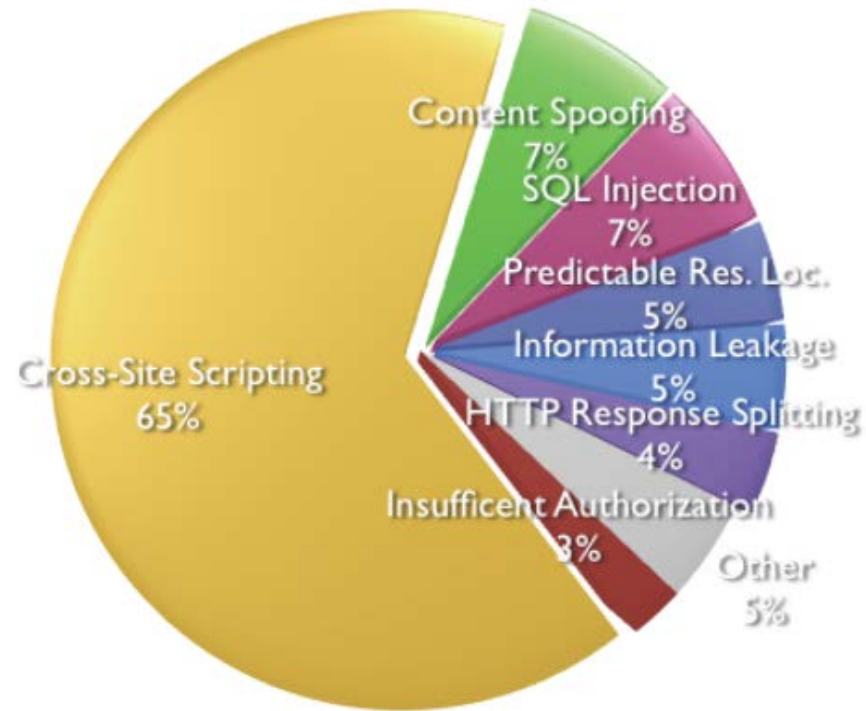


Social networks malware

- We can consider three main types of social networks malware attacks:
 - XSS worms
 - e.g. Samy
 - Trojans
 - e.g. Koobface
 - ClickJacking types
 - Forced like
 - Can lead to DriveByDownloads malware

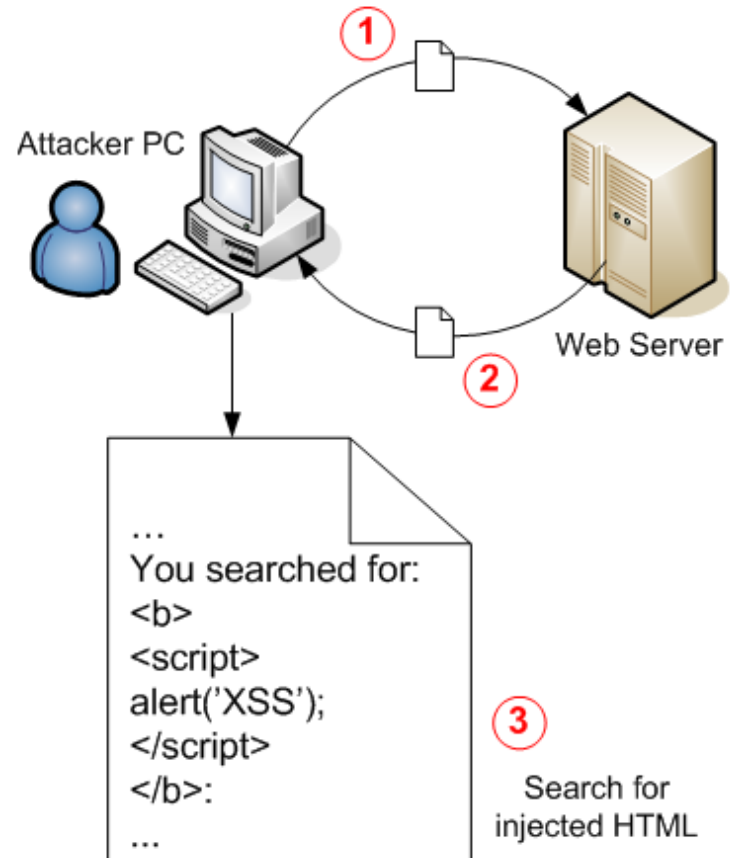
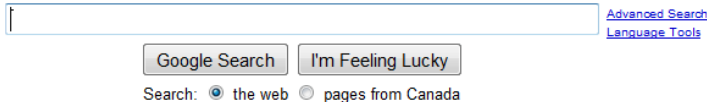
What is XSS !?

- Cross Site Scripting (XSS) is a common vulnerability in web applications.
- Has two types:
 - Reflected
 - Stored



Reflected XSS

- Application reflects exactly what it gets from the user.
 - user may inject a harmful script





Stored XSS

- Attacker stores a harmful script in the application database for further exploitation.
 - Comments
 - Forum talks
 - FB Wall



XSS + AJAX = w0rm

- XSS threat becomes more noticeable due to the combination of HTML and AJAX technology.
- AJAX allows browsers to issue HTTP requests on behalf of the user.
 - No need for the attacker to deceive the victim to click on a special crafted link!



XSS worm propagation

- XSS worm propagation consists of the following two steps:
 - Download
 - A visitor downloads (views) an infected profile and automatically executes the JavaScript payload.
 - Propagation
 - The payload is extracted from the contents of the profile being viewed and then added to the viewer's profile.

ClickJacking Worm Propagation

Unwittingly clicking on a hidden like button

The diagram illustrates a clickjacking worm propagation on Facebook. It shows two posts from Sarah Tav and Mohammad Reza Faghani, both of whom 'like a link' to 'apps.facebook.com'. A video player is shown with a red circle around the play button. Red arrows point from the play button to the 'likes' section of both posts, indicating that clicking the play button triggers a hidden like action.

and more friends get infected...

Trojan Propagation

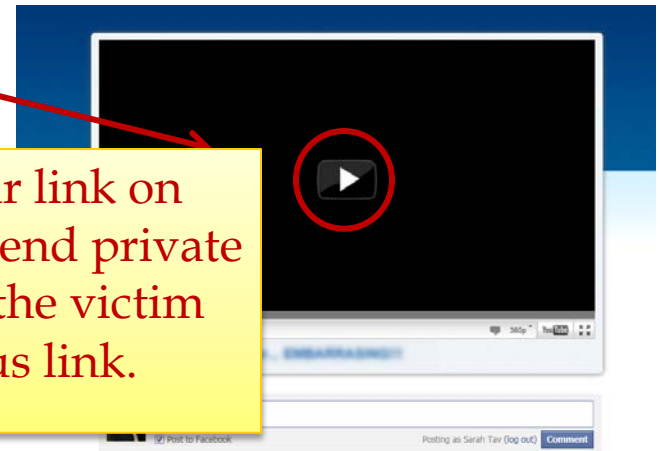


Sarah Tav likes a link.

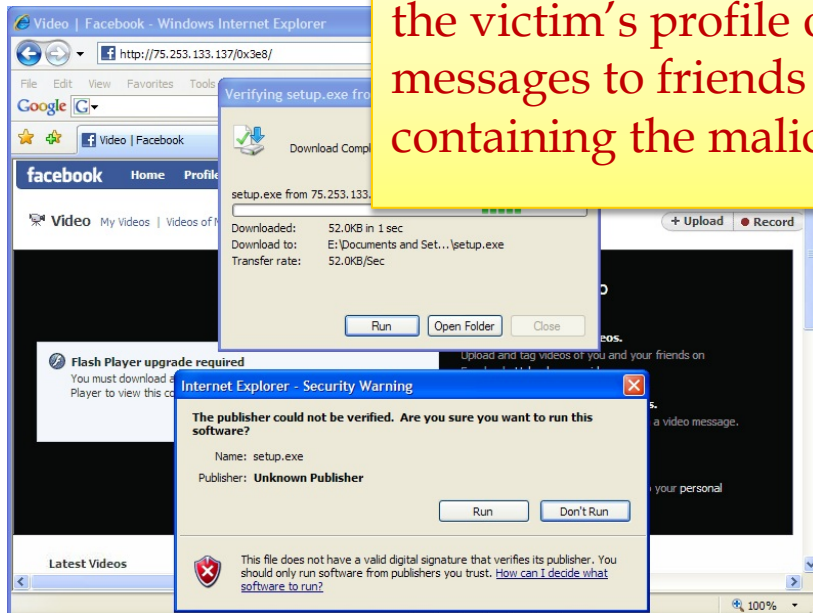


apps.facebook.com
This really has to be an awkward moment.

4 hours ago · Like · Comment



Then they post a similar link on the victim's profile or send private messages to friends of the victim containing the malicious link.



Sometimes, they ask you to download the appropriate decoder to play the movie, which is indeed the Trojan itself.

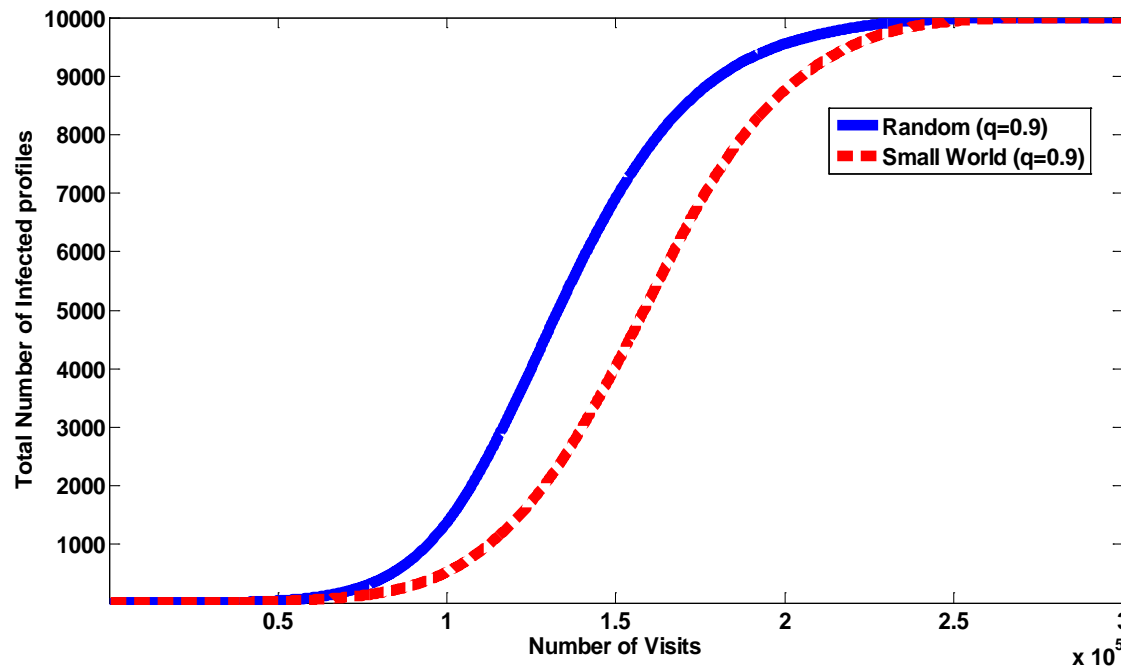


Research on OSN malware

- Three main papers on OSN malware propagation (in chronological order):
 - [1] Faghani M. R., Saidi H., “Malware Propagation in Online Social networks”, Malware09, Montreal, 2009.
 - [2] W. Xu, F. Zhang, and S. Zhu., “Toward worm detection in online social networks”, (ACSAC), 2010.
 - [3] Guanhua Y., Guanling . And et al. , “Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications, (ASIACCS'11), March 2011.

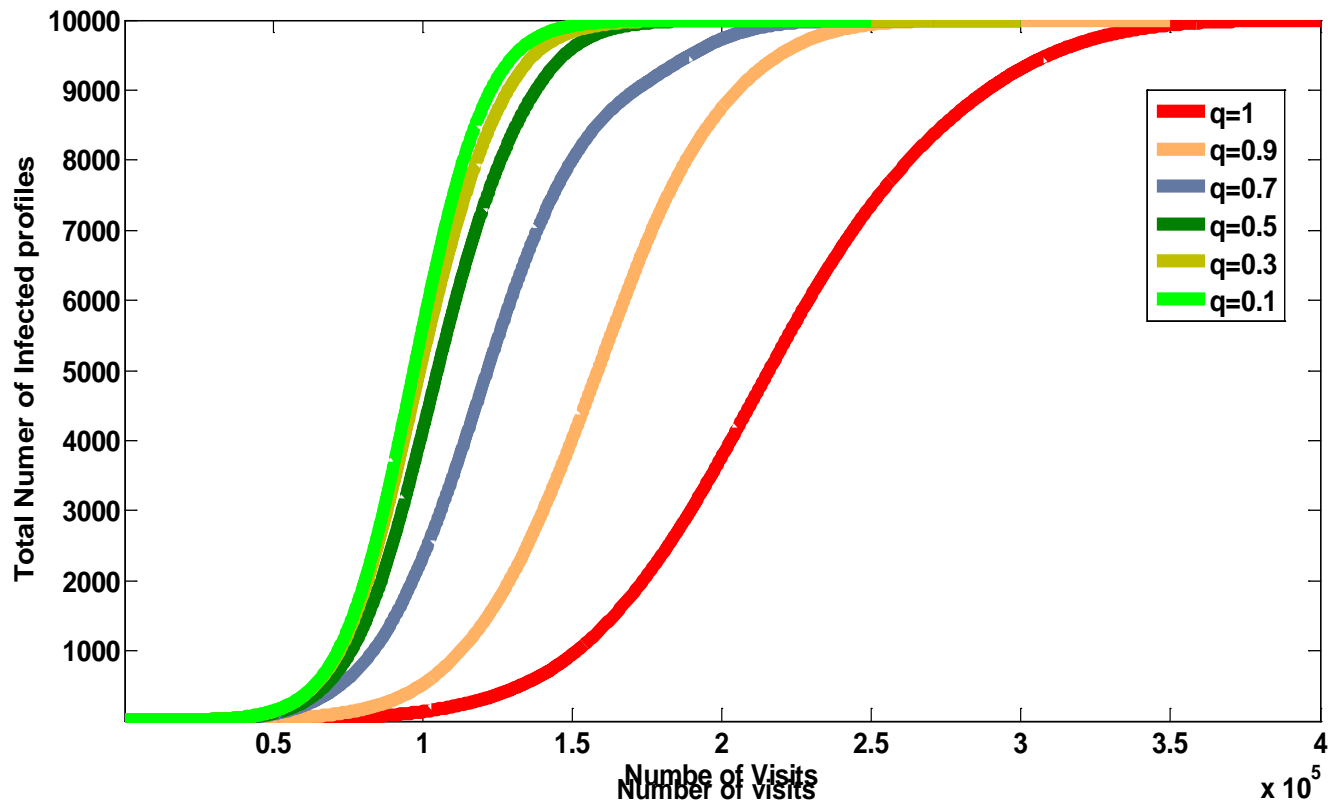
Result Summary (from simulations)

- Social network structure itself slows down the worm propagation.



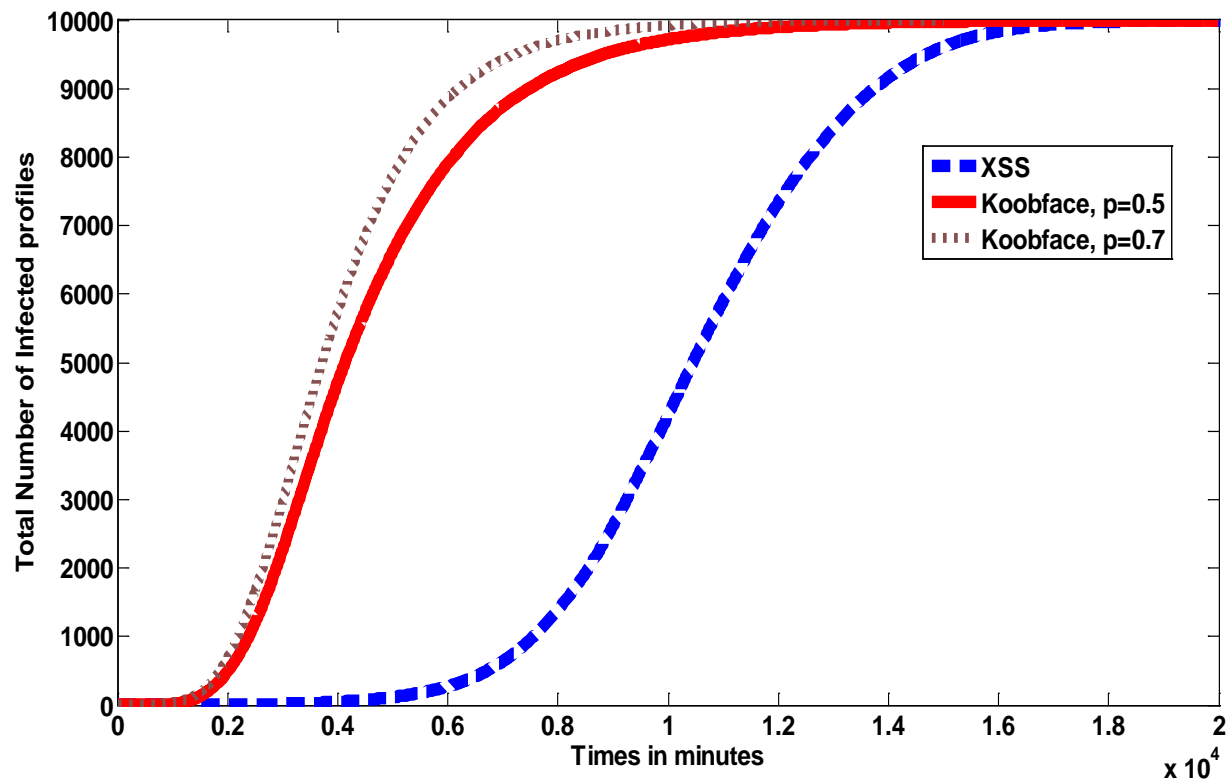
Result summary (cont.)

- User activities play an important role.



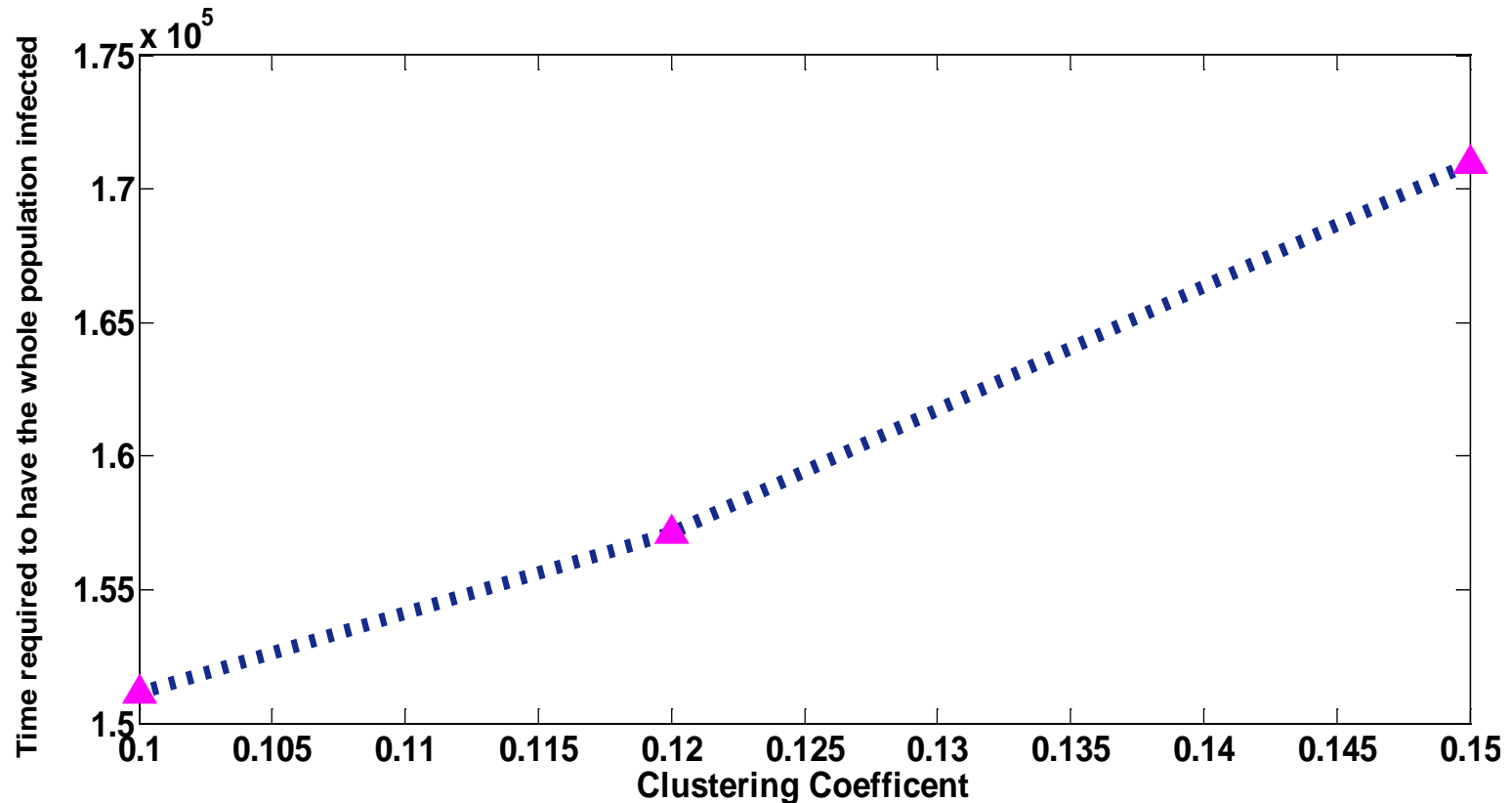
Result summary (cont.)

- Trojan type spreads faster than XSS



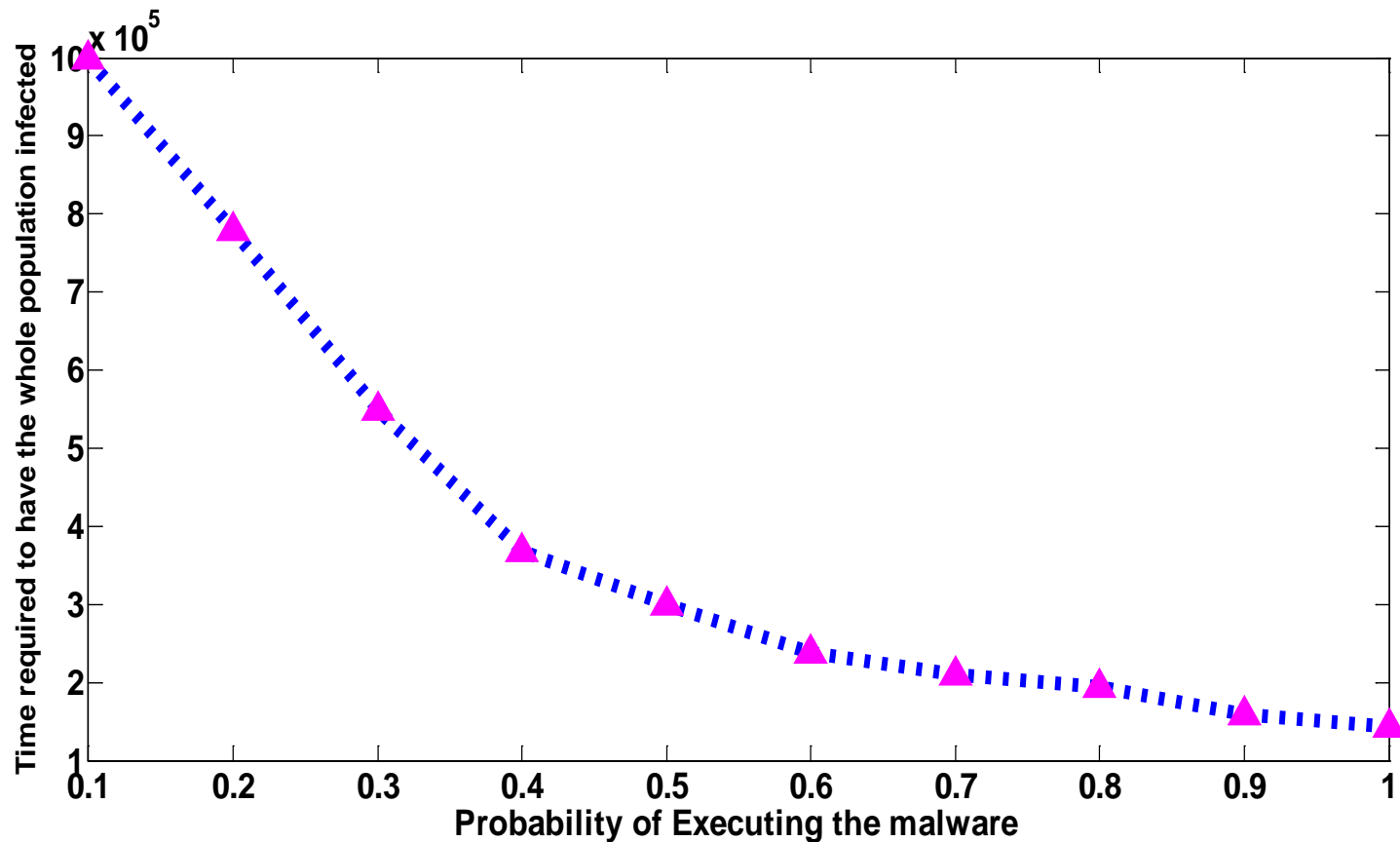
Result summary (cont.)

- Effect of Clustering coefficient is linear



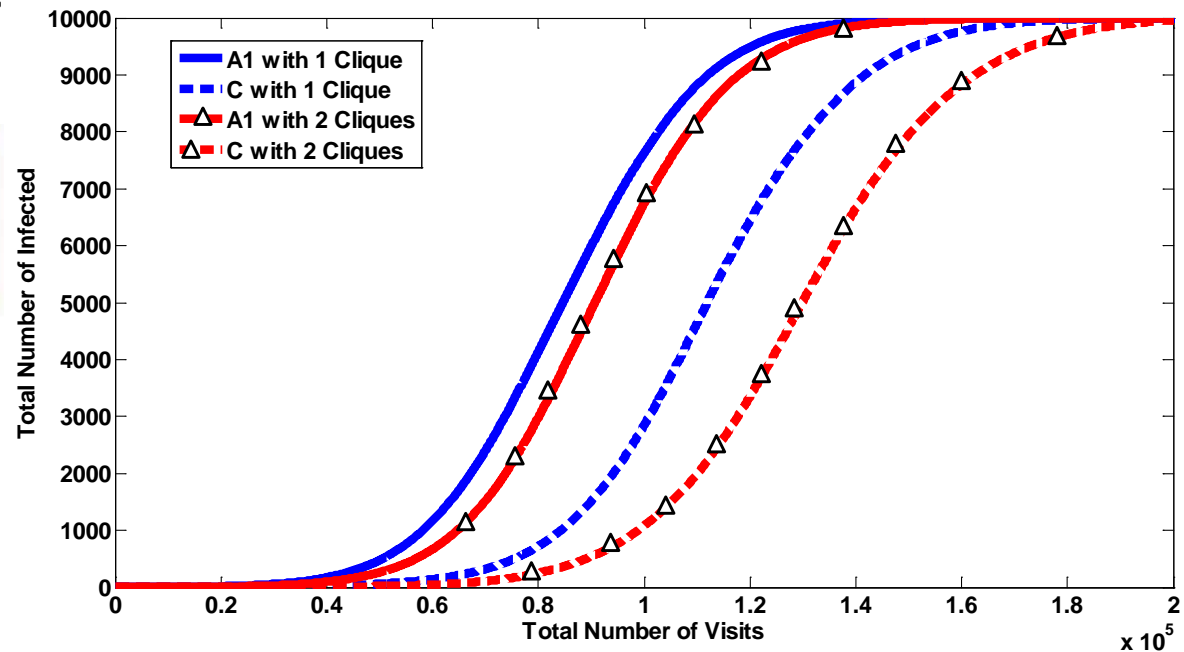
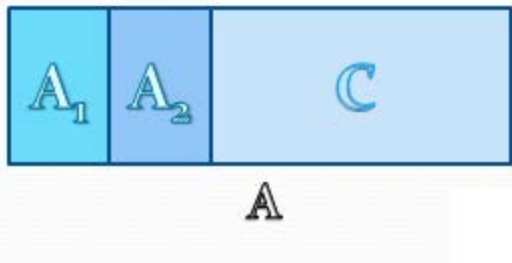
Result summary (cont.)

- Effect of Infection Probability is exponential



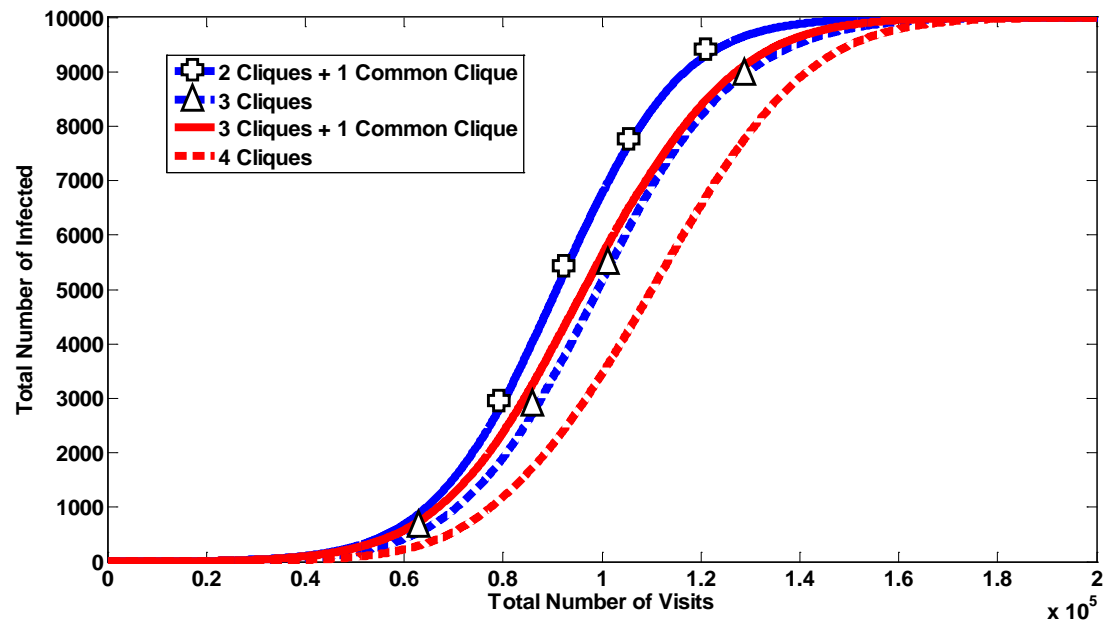
Recent Results (1)

- Considering cliques
 - Those who have common interests create a group.



Recent Results (2)

- Considering overlapping cliques:





Proposed Defense System

- Identify big cliques
 - Among them distinguish those users who are connected to different cliques.
 - Implement decoy friends or other detection mechanisms to detect malicious behaviors.
- It is more efficient than current Facebook classifier system.



Conclusion

- User relationship structure plays an important role in malware propagation.
- User activities affect speed of propagation.
- Propagation of XSS types is slower than that of Trojan types.
- A new defense mechanism can be built using OSN graph topology.



Acknowledgement

- Thank you
- Any Question ?