# poc 2016

# Effective Patch Analysis for Microsoft Updates

Power of Community | 2016.11

# Agenda

- **Background** – what are we talking about today?
- **Patch Analysis** – let's talk about general approach in analyzing patches
- **Case Study** – case-by-case overview of Microsoft patch analysis
- **PETCH** – everyone loves tools!
- **Conclusion** – wrapping all up, let's go write some 1-days!

# Background

What are we talking today?

# Vulnerabilities

**Exploits**

- 0-days vs. N-days
- State-sponsored
- Malware
- Research

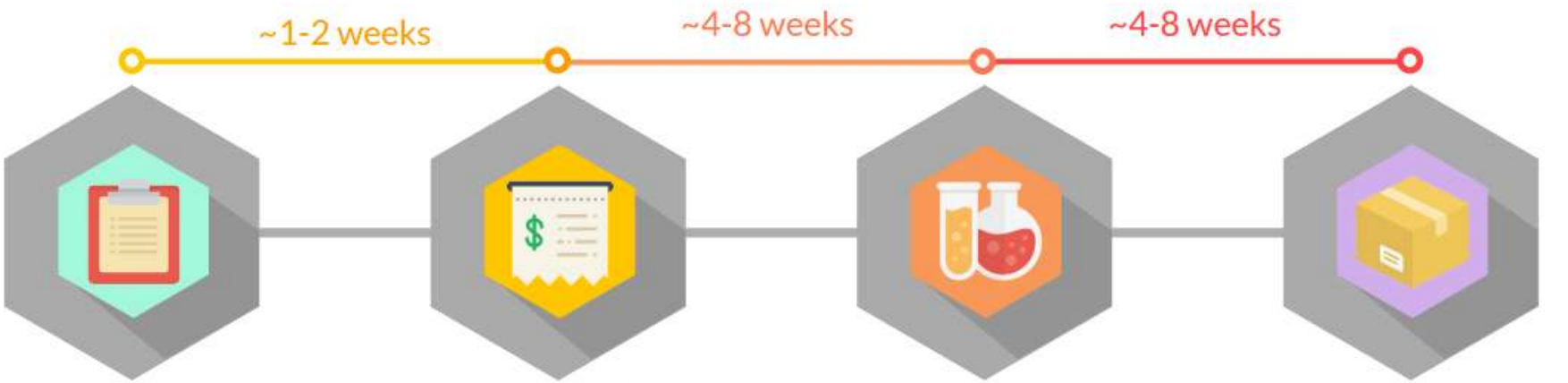
**Bug Bounties**

- Payouts
- Credits
- Competitions

**Market**

- Higher payouts
- No credits

# Security Updates




**Report**

Vendor

Bug bounty platform

**Bargain**

Bug bounty offers

**Review**

Reproduce

Triage

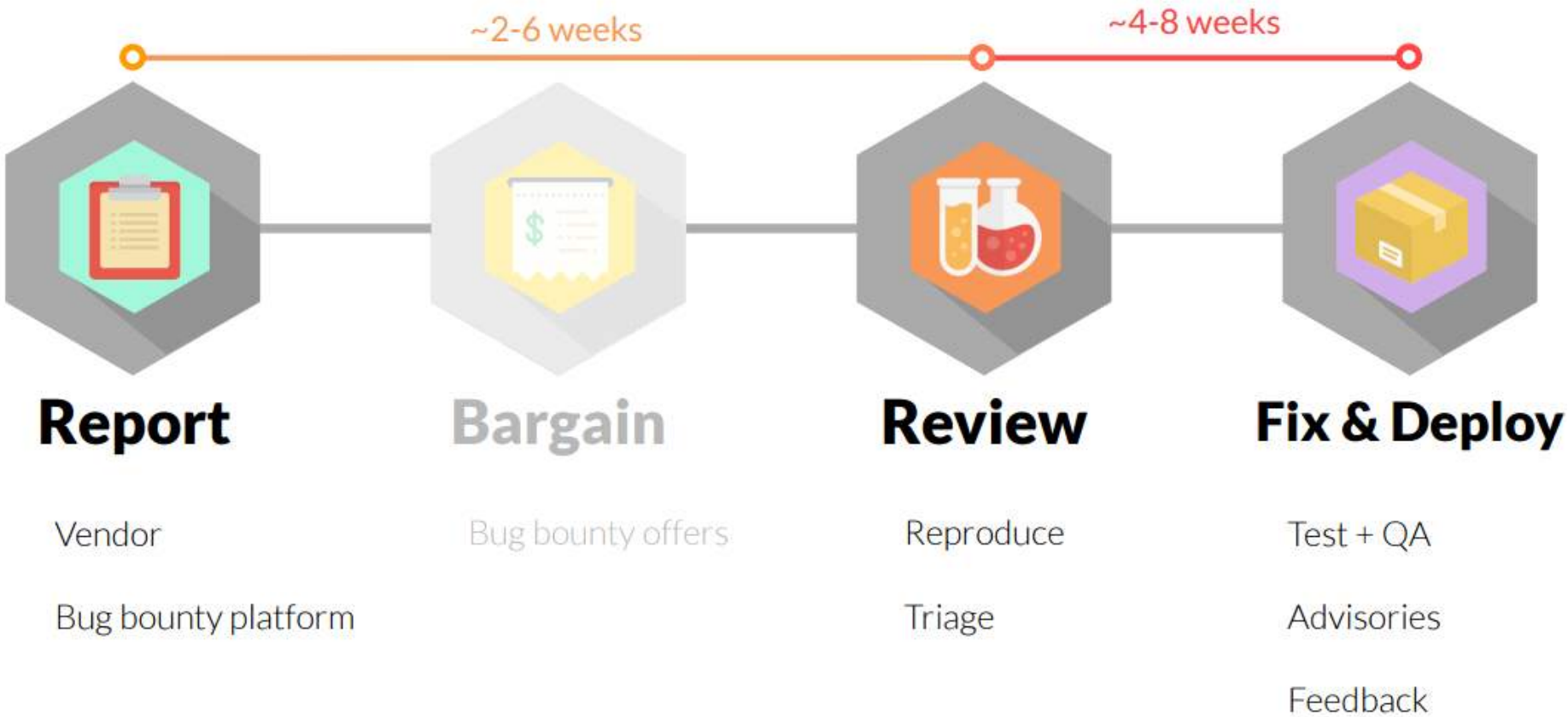
**Fix & Deploy**

Test + QA

Advisories

Feedback

# Security Updates



The worst starts here

# Patch Analysis

It's easy when they tell you the answer!

# Patch Analysis

Analyzing patches released by vendors to better understand what code changes were made

## Patch analysis *isn't* new

**APEG (Automatic Patch-based Exploit Generation)** – Brumley et al.

**Towards Generating High Coverage Vulnerability-Based Signatures with Protocol-Level Constraint-Guided Exploration** – Caballero et al.

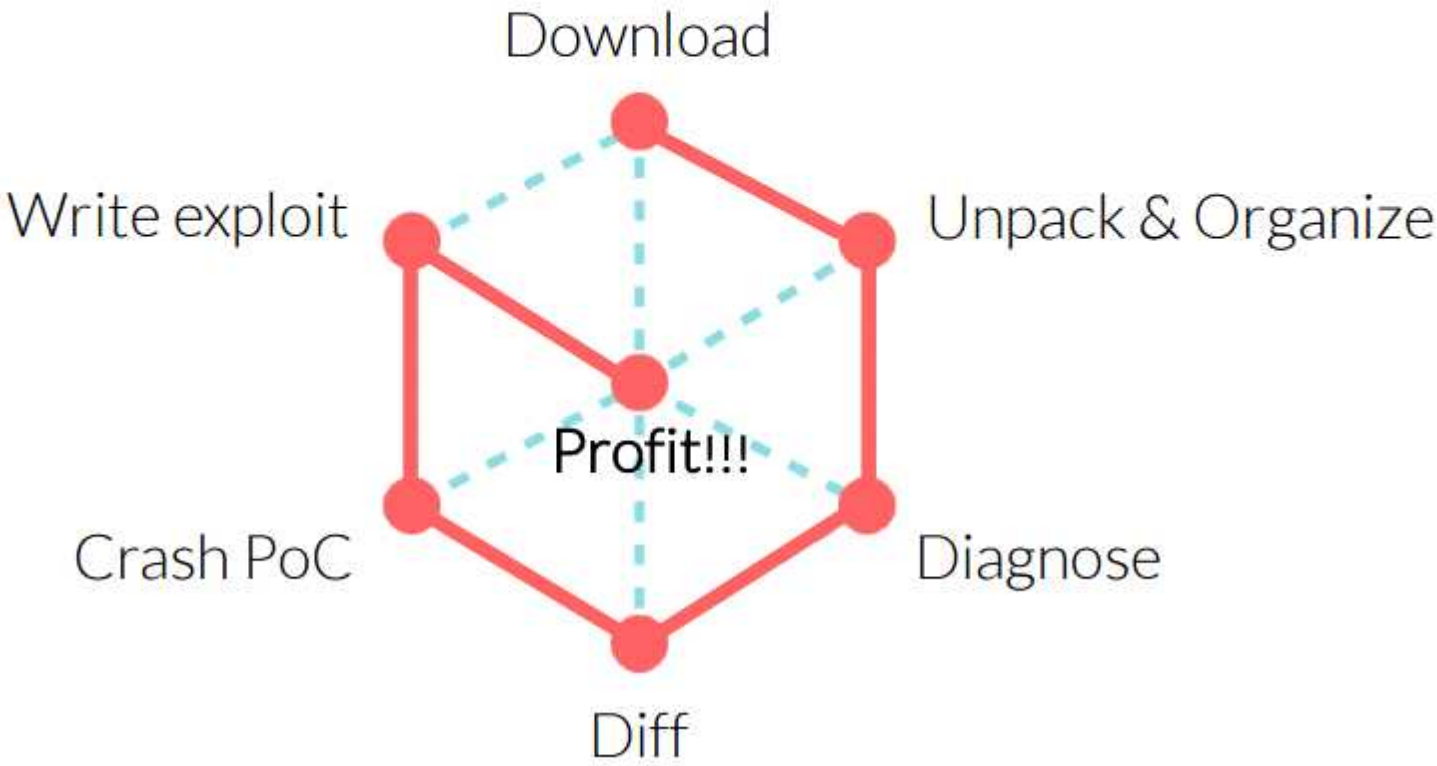
**Reverse Engineering and Computer Security** – Alex Sotirov

**Fight against 1-day exploits: Diffing Binaries vs Anti-diffing Binaries** – Jeongwook Oh

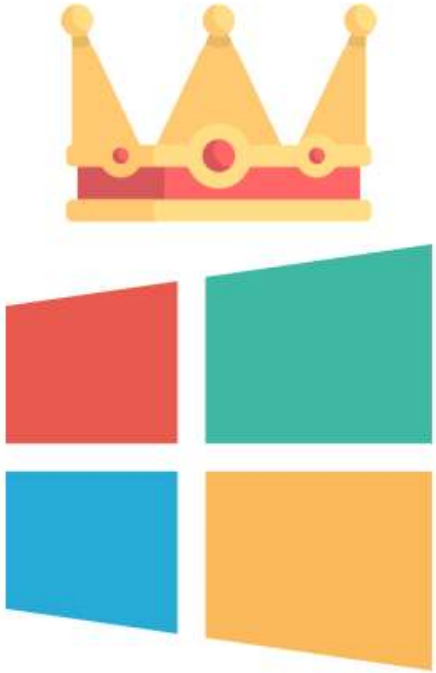
# Why?


Slow updates
Real threat
Metasploit module
Pentesting & Auditing
Insight from fixed bugs
New bug class
Find similar bugs
Vulnerability Research
Network filters (IDS, IPS)
Anti-virus
Mitigation solutions
Defense Research
Real-world CTF
1-day Market
Fun & Profit

# Patch Analysis in 6 easy steps!



We are going to be
Microsoft-specific today,



Microsoft makes patch analysis
extremely convenient, though!

but the same process applies
to any patch analysis.

# Step 1: Download

2 Versions
- $(n-1)^{th}$ month
- $n^{th}$ month

Minimal changes, focusing on security updates

VM with $(n-1)^{th}$ month cumulative updates

For Microsoft patches,

- Security Bulletin
- Knowledge Base (KB)

Oh, man. Patches came out today!

Security Advisories and Bulletins > Security Bulletin Summaries > 2016

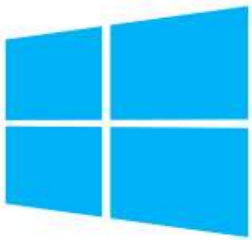
Find the latest updates

MS16-OCT

MS16-SEP

# Microsoft Security Bulletin Summary for October 2016

Published: October 11, 2016 | Updated: October 12, 2016



Windows 10

MS releases cumulative updates that contain all of component updates

For older Windows, you can download each component update separately

# Step 2: Extract files

Figure out how to get files out from update package, installer, etc.

Preferably, in an automated way

Organize the output

# Update file structure

- .msu
  - pkgProperties.txt
    - Contains string properties used for Wusa.exe
  - xml
    - Describes the update package installation information
  - cab
    - Each .cab file represents one update

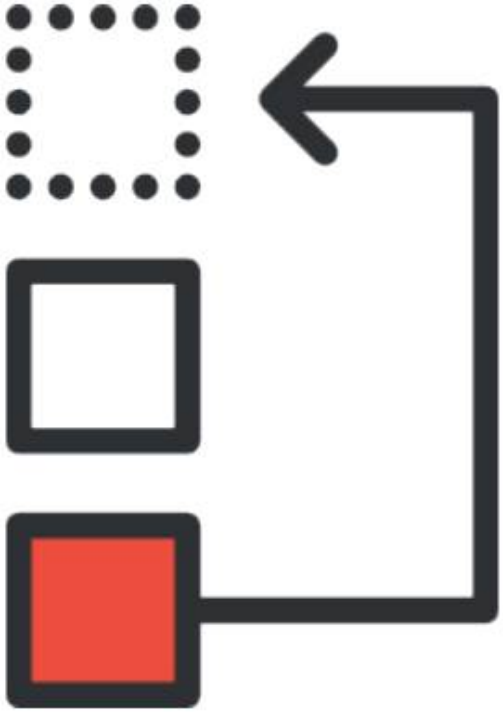
# Step 3: Diagnose

Narrow the target vulnerabilities
⇒ CVEs, Bulletins, Patch notes

Collect changed/updated files

Collect other useful files for analysis

# Changed files



- Sort by modified time
- Useful to narrow down the target
- Microsoft updates only contain modified/updated files ☺

# Step 4: Diff

Use various tools to compare patched vs. original

Find the patched code
$\Rightarrow$ added, removed, changed

Perform root cause analysis for better understanding of the bugs

# Step 5: Write a crashing PoC

Prove that we understand the bug

Give us something to start with for developing a full exploit

Determine the exploitability of the bug

# Step 6: Write an exploit

Debugging environment

Exploitation primitives

Mitigation bypass

# Case Study #1

Internet Explorer 11 (vbscript.dll)
May, 2016 (MS16-051, CVE-2016-0189)

```
20  v22 = a2;
21  v7 = VAR::PvarCutAll(a1);
22  if ( 8204 == *(_WORD *)v7 )
23  {
24    v8 = (SAFEARRAY *)*((_DWORD *)v7 + 2);
25  }
26  else
27  {
28    if ( 24588 != *(_WORD *)v7 )
29      return 0x80020005;
30    v8 = (SAFEARRAY *)**((_DWORD **)v7 + 2);
31  }
32  if ( !v8 )
33    return 0x8002000B;
34  v9 = (struct VAR **)v8->cDims;
35  if ( !(_WORD)v9 )
36    return 0x8002000B;
37  v10 = a3;
38  if ( v9 != a3 )
39    return 0x8002000B;
40  v11 = 0;
41  v23 = v8->rgsabound;
42  v12 = a4;
43  while ( 1 )
44  {
45    v13 = VAR::PvarCutAll(v12);
46    if ( 2 == *(_WORD *)v13 )
47    {
48      v14 = *((signed __int16 *)v13 + 4);
49    }
50    else if ( 3 == *(_WORD *)v13 )
51    {
52      v14 = *((_DWORD *)v13 + 2);
53    }
54    else
55    {
56      if ( rtVariantChangeTypeEx(
57             (struct tagVARIANT *)0x400,
58             (struct tagVARIANT *)2,
59             3u,
60             (unsigned __int16)v19,
61             (unsigned __int16)v20) < 0 )
62        return CScriptRuntime::RecordHr(v18, v19, v20);
63      v14 = v21;
64    }
65    v15 = v14 - v23->lLbound;
```

0000BEBD ?AccessArray@@YGJPAPAVVAR@@PAV1@H1PAPAUtagSAFEARRAY@@@Z:38

April vs. May

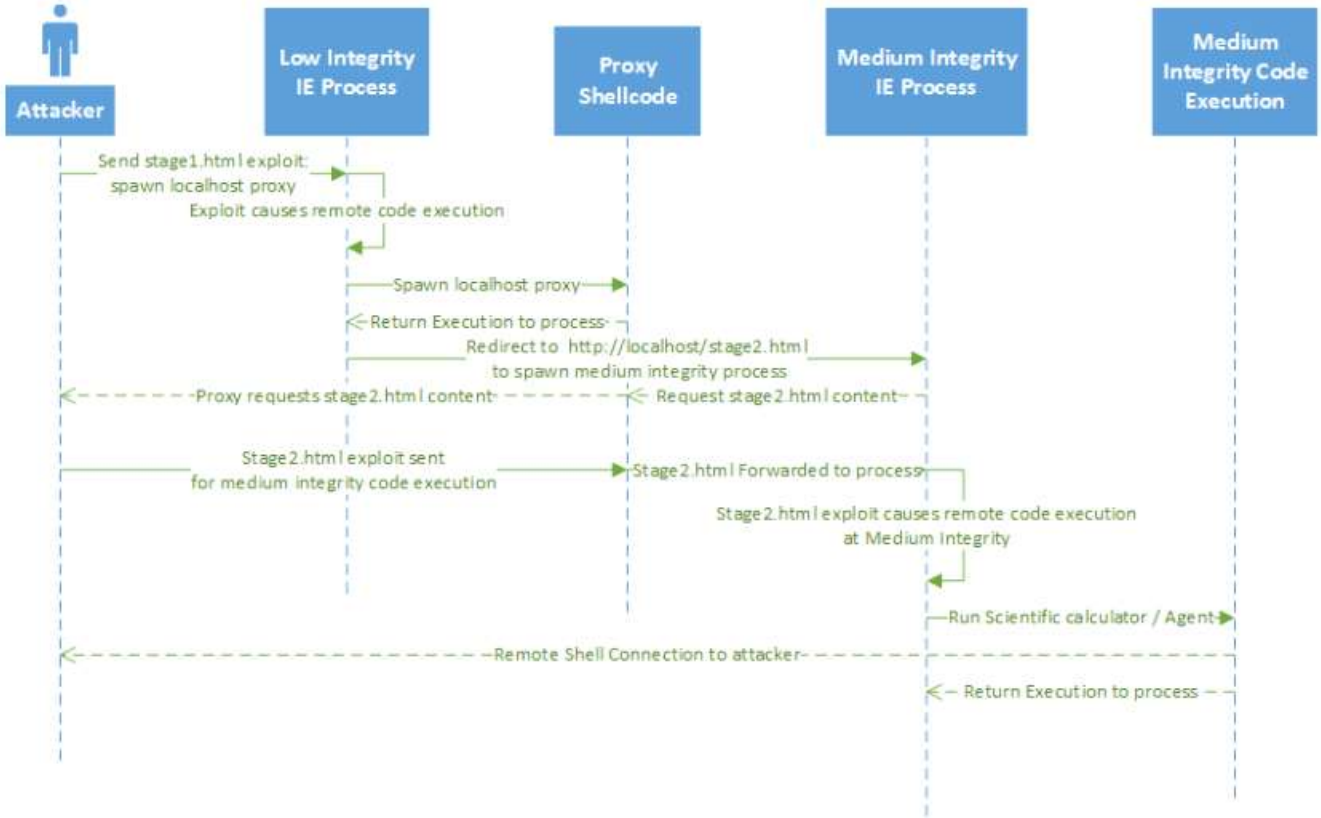
```
23  v25 = a2;
24  v7 = VAR::PvarCutAll(a1);
25  if ( 8204 == *(_WORD *)v7 )
26  {
27    v8 = (SAFEARRAY *)*((_DWORD *)v7 + 2);
28  }
29  else
30  {
31    if ( 24588 != *(_WORD *)v7 )
32      return 0x80020005;
33    v8 = (SAFEARRAY *)**((_DWORD **)v7 + 2);
34  }
35  if ( !v8 )
36    return 0x8002000B;
37  v10 = (struct VAR **)v8->cDims;
38  if ( !(_WORD)v10 || v10 != a3 )
39    return 0x8002000B;
40  result = SafeArrayLock(v8);
41  if ( result >= 0 )
42  {
43    v11 = a4;
44    v12 = v8->rgsabound;
45    v13 = 0;
46    while ( 1 )
47    {
48      v14 = (const VARIANTARG *)VAR::PvarCutAll(v11);
49      if ( 2 == v14->vt )
50      {
51        v15 = v14->iVal;
52      }
53      else if ( 3 == v14->vt )
54      {
55        v15 = v14->lVal;
56      }
57      else
58      {
59        v22 = 0;
60        v24 = rtVariantChangeTypeEx(
61                v14,
62                (VARIANTARG *)&v22,
63                (struct tagVARIANT *)0x400,
64                (struct tagVARIANT *)2,
65                3u,
66                (unsigned __int16)v20,
67                (unsigned __int16)v21);
68        if ( v24 < 0 )
```

0000BF1C ?AccessArray@@YGJPAPAVVAR@@PAV1@H1PAPAUtagSAFEARRAY@@@Z:57

# The Plan

- Create a (dummy) ***VBScriptClass*** instance
- Get the address of the class instance
- Leak ***CSession*** address from the class instance
- Leak ***COleScript*** address from the ***CSession*** instance
- Overwrite ***SafetyOption*** in ***COleScript***

# Sandbox Escape




ZDI-14-270

#won't_fix

Stager hosted on local host (Low)

Intranet is trusted

Medium Integrity for trusted hosts

# PETCH

Making your life little bit easier

# PETCH

- Patch fetcher
- Microsoft update management tool
- Reduce repetitive tasks
  - **Search, download, extract, get symbols**, diff, analyze, exploit
  - ⇒ ***PETCH***, diff, analyze, exploit
- Queue up multiple updates
  - Automatically populated, downloaded and extracted

# Lessons Learned


# THE GREAT TRAIN CYBER ROBBERY

Sergey Gordeychik
Gleb Gritsai

*All pictures are taken from Dr Strangelove movie and other Internets

# Railways

9260 km
6 day 1:59

| Rank | Country | Railway length (km) |
|---|---|---|
| 1 | United States | 224,792 |
| 2 | China | 112,000 |
| 4 | Russia | 86,000 |
| 3 | India | 65,000 |
| 5 | Canada | 46,552 |
| 6 | Germany | 43,468 |
| 7 | Australia | 38,445 |
| 8 | Argentina | 36,966 |
| 9 | South Africa | 31,000 |
| 10 | France | 29,640 |

# INDUSTRIAL CYBERSECURITY


The secrets of cybersecurity, Valentin Gpanovich, Efim Rozenberg, Sergey Gordeychik . Railway Strategies, Issue 130

https://issuu.com/schofieldpublishingltd/docs/railway_strategies_issue_130_june_2

# Cyber Grand Shellphish


POC 2016

SECLAB

THE COMPUTER SECURITY GROUP AT UC SANTA BARBARA

CYBER

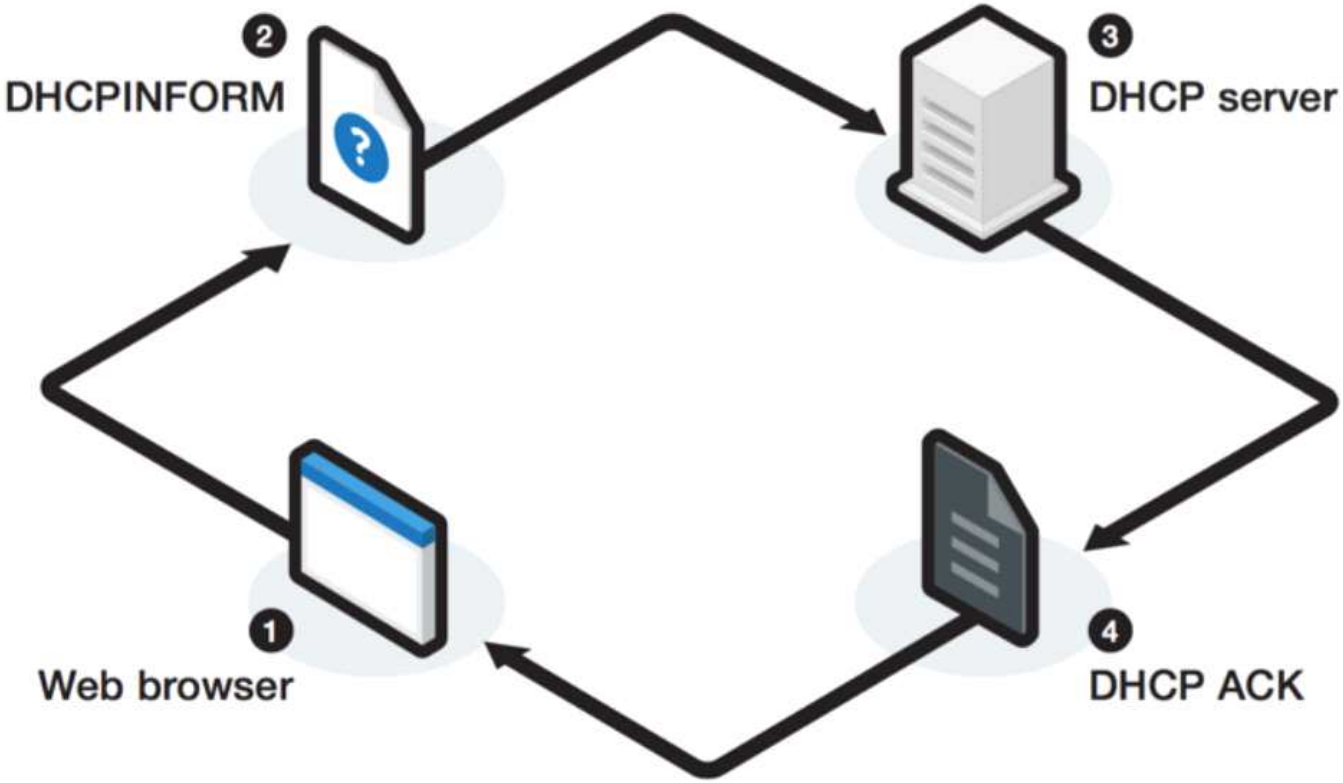
GRAND_CHALLENGE


SHELLPHISH

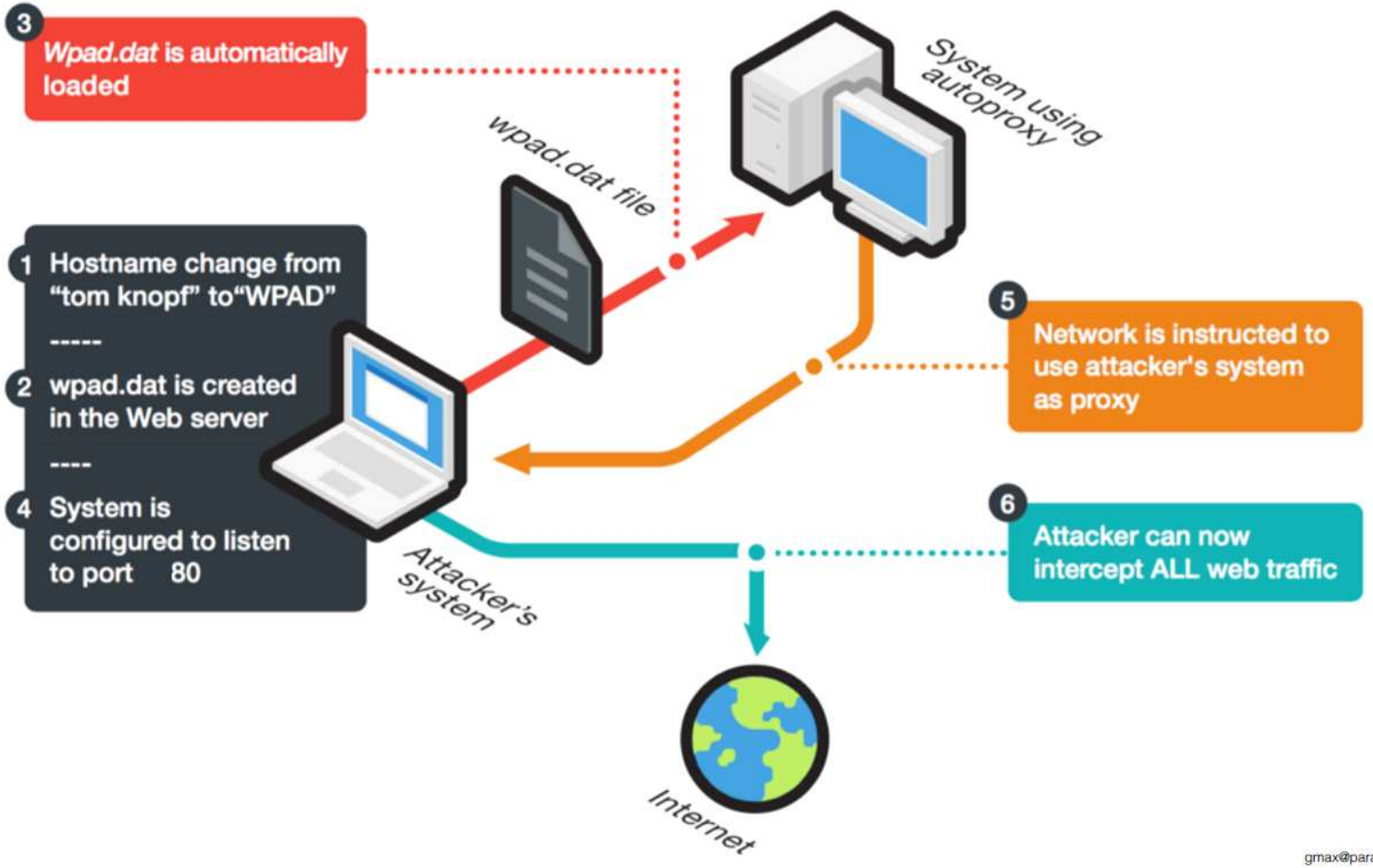

CRISPY
YELLR
disekt
CYBER

# what is WPAD

DHCP Discovery Method



# WPAD experiment #1




# 1


Lufthansa
Senator Lounge
Business Lounge
STAR ALLIANCE
GOLD
2


3
HotSpot


# 4


# 5

# Analysis of iOS 9.3.3 Jailbreak & Security Enhancements of iOS 10

Team Pangu

# Agenda

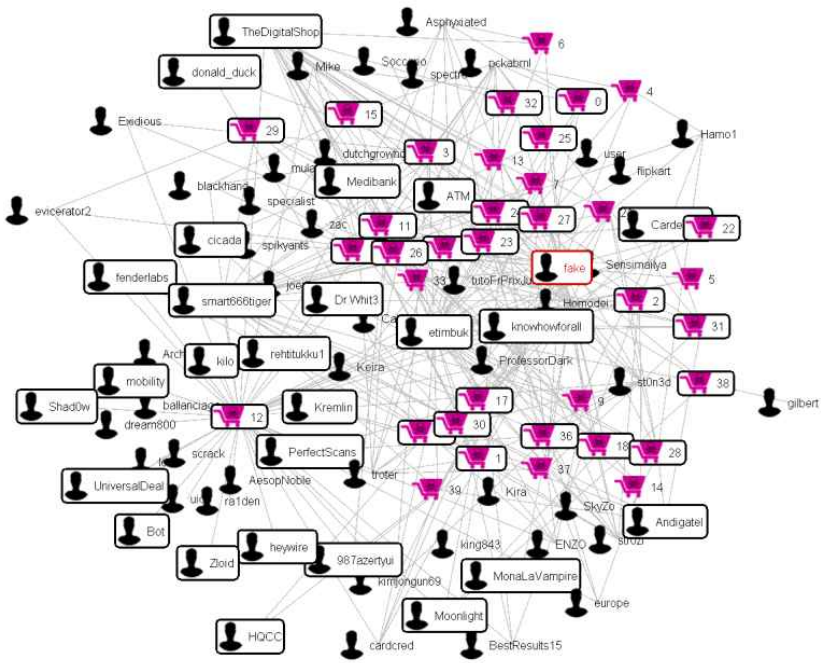
- CVE-2016-4654
- Exploit Strategy
- iOS 10 Security Enhancements
- iPhone 7 New Protection
- Conclusion

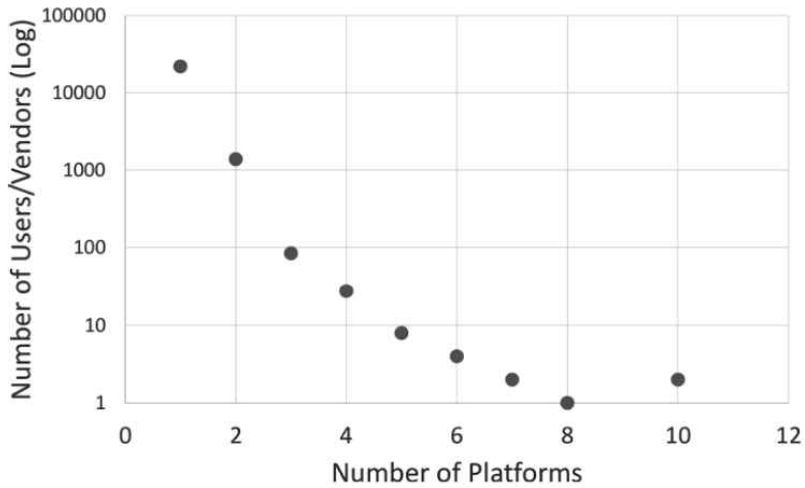
# Agenda

- CVE-2016-4654
- Exploit Strategy
- iOS 10 Security Enhancements
- iPhone 7 New Protection
- Conclusion

# Q&A

# Use Case: Social Network Analysis




**We identify malware vendors who have a presence in multiple marketplaces**

# Use Case: Social Network Analysis

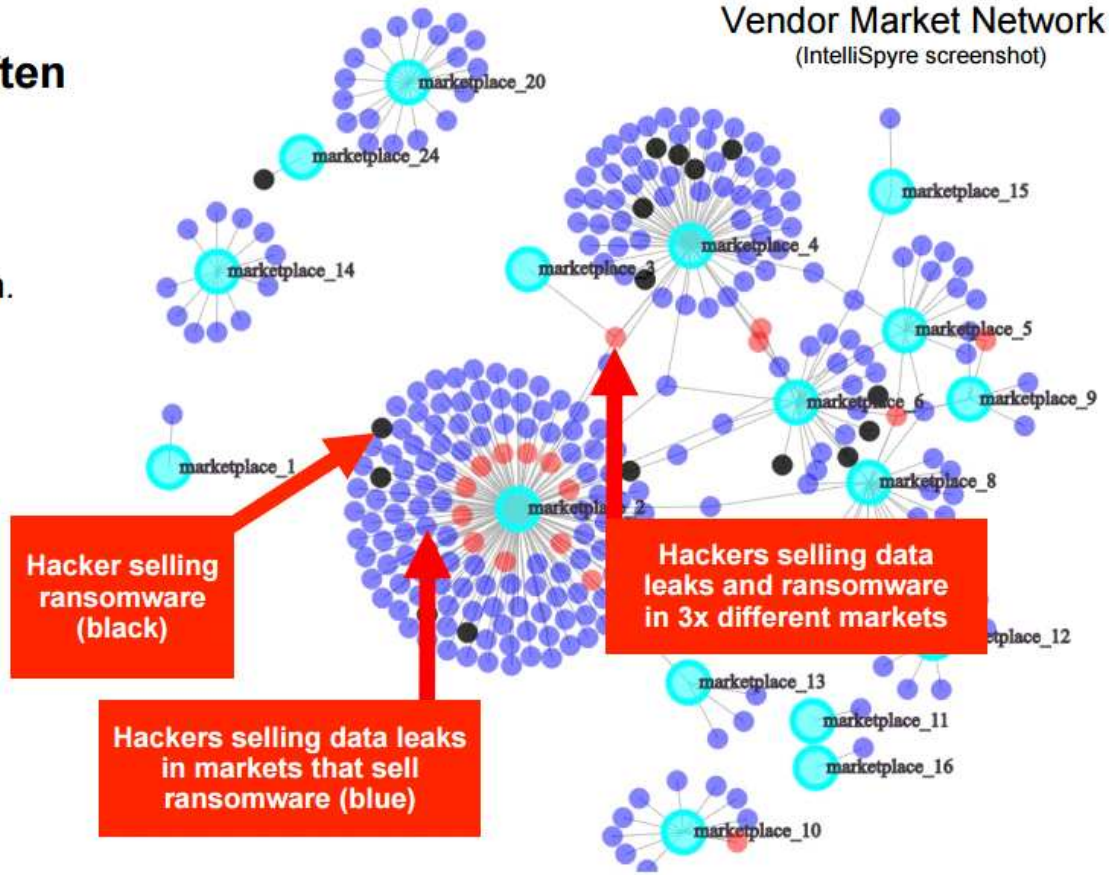
**Ransomware victims are also often data-leakage victims.**

Ransomware vendors and markets also sell the results of data-leakage information.

IntelliSpyre can identify where data leaks are sold from the vendors of ransomware through link analysis.

Quick location of dataleaks after ransomware incidents.

Vendor Market Network
(IntelliSpyre screenshot)




***IntelliSpyre made the semi-finals***

**15 semi-finalists**
7x from U.S.
2x cybersecurity
1x from Arizona


info@intellispyre.com
intellispyre.com

# Thank You!

@PauloShakASU @intellispyre

# The Million-Key Question: Investigating the Origins of RSA Public Keys

**Based on paper "The Million-Key Question: Investigating the Origins of RSA Public Keys"**
**25th Usenix Security Symposium, 2016. Received Best Paper Award**

Petr Švenda, Matúš Nemec, Peter Sekan, Rudolf Kvašňovský, David Formánek, David Komárek and Vashek Matyáš
*svenda@fi.muni.cz* *@rngsec*
Faculty of Informatics, Masaryk University, Czech Republic

CROCS
Centre for Research on Cryptography and Security

How to defend against possibility of classification?

# MITIGATION

# Conclusions

- RSA keypair generation observably bias public keys
  - Different libraries use different implementation choices
- Source library can be probabilistically estimated from RSA public key
  - Accuracy more than 85 % with 10 keys (>99 % within top three matches)
  - For some sources, even a single key is enough
- Information disclosure vulnerability
  - Forensics, de-anonymization, vulnerability scans, compliancy testing…

Questions ?

*Get tech. report and datasets at http://crcs.cz/rsa, try classification at http://crcs.cz/rsapp*

## How Smartphones Set Clock?

- Smartphones have multiple clock sources such as:

Cellular Network: NITZ

Internet: NTP

Satellite Navigation: GPS

- We cover NITZ and NTP as user interaction not required
- GPS spoofing, NTP attack is well known but NITZ attack is not
- How clock sources interact on smartphones?

POC2016

# LTE Redirection

## Forcing Targeted LTE Cellphone into Unsafe Network

Lin Huang @360 UnicornTeam
Wanqiao Zhang @360 UnicornTeam



360UNICORNTEAM

# Thank you !

# Countermeasures (1/2)

- Cellphone manufacture – smart response
  - Scheme 1: Don't follow the redirection command, but auto-search other available base station.
  - Scheme 2: Follow the redirection command, but raise an alert to cellphone user: Warning! You are downgraded to low security network.

# QEMU+KVM & XEN Pwn: virtual machine escape from “Dark Portal”

Wei Xiao & Qinghao Tang

360 Marvel Team

# About 360 Marvel Team

- 360 Marvel Team focus on cloud and virtualization security.
- 360 Marvel Team has found 35 vulnerabilities in cloud and virtualization product in last year.
- 360 Marvel Team is able to finish virtual machine escape attacks in VMWARE workstation virtual machine , docker container , XEN virtual machine , QEMU+KVM virtual machine by utilizing vulnerabilities .

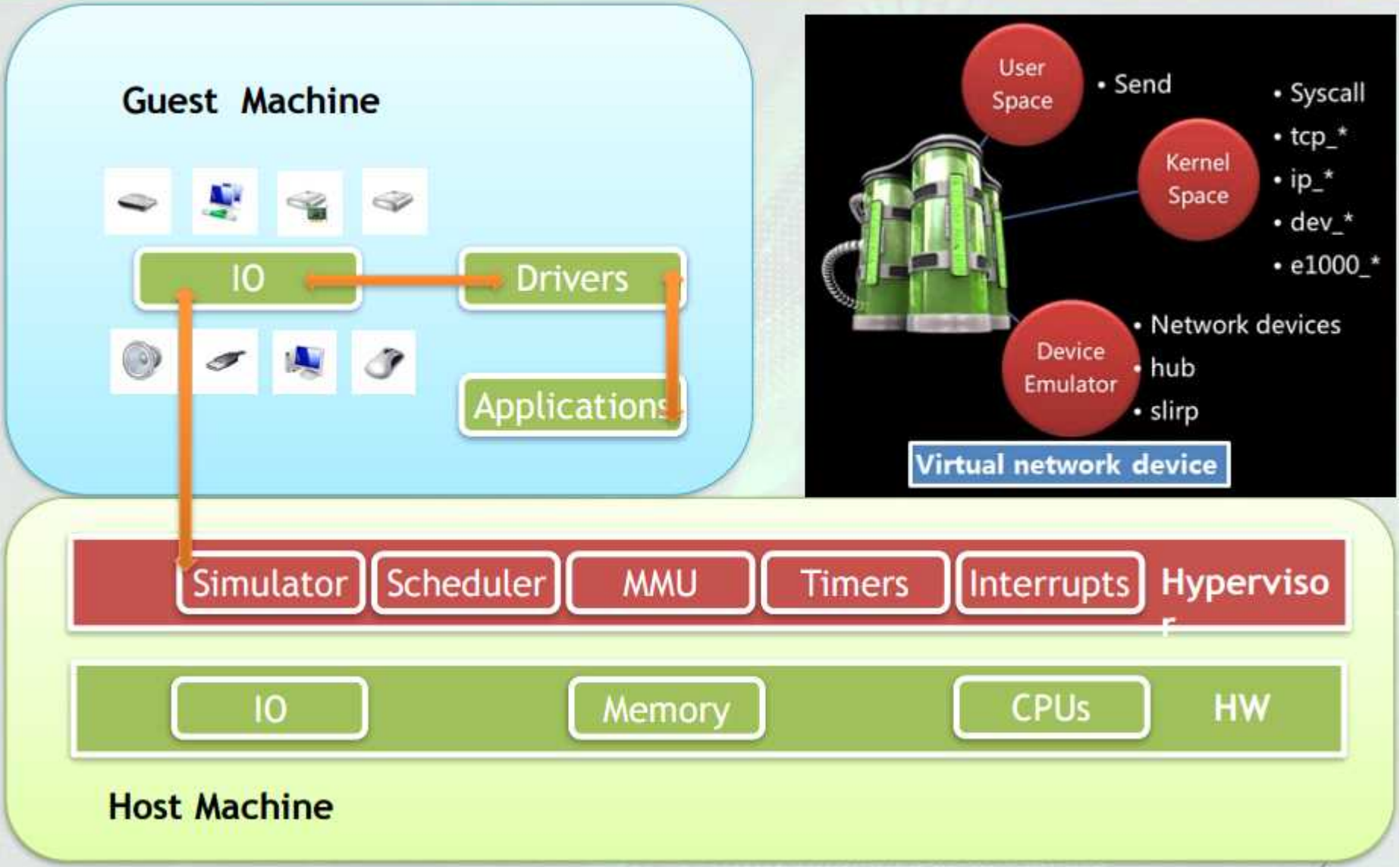
Marvel Team

# Agenda

- Vulnerabilities in QEMU
- Dark Portal Vulnerability
- Dark Portal Exploitation
- QEMU Vulnerability Limitation and Solutions

# VULNERABILITIES IN QEMU

# Device Simulator Data Flaw



# Q&A

# New Reliable Android Kernel Root Exploitation Techniques

INetCop Security
dong-hoon you (x82)

2016-11-11

## - Outline

1. **Introduction**
2. Technical background of kernel attack
3. Proposing new kernel attack technique
4. Demonstration
5. Conclusion

# 1-1. About me

- Co-founder / CTO / Head of INetCop Security smart platform lab
  - Ph.D. Chonnam National University Graduate School of Information Security
  - Speaker and operator of many seminars, conferences
  - Operating hacking & security contests/conferences
    - SECUINSIDE CTF/CTB organizer
  - Various project advisors
  - Published several security advisories and POC codes
  - Working on machine learning based android malware analysis and search for vulnerabilities in android apps and kernel



TOTAL SECURITY SOLUTION

NETCOP

**Smart Platform Security**

tel. 02 575 3339 / fax. 02 575 3340
www.inetcop.net
㈜아이넷캅

Check Point
SOFTWARE TECHNOLOGIES LTD.

# TEACHING THE NEW DOG OLD TRICKS

## PHP7 Memory Internals for Security Researchers

Yannay Livneh | Security Researcher