

рос 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

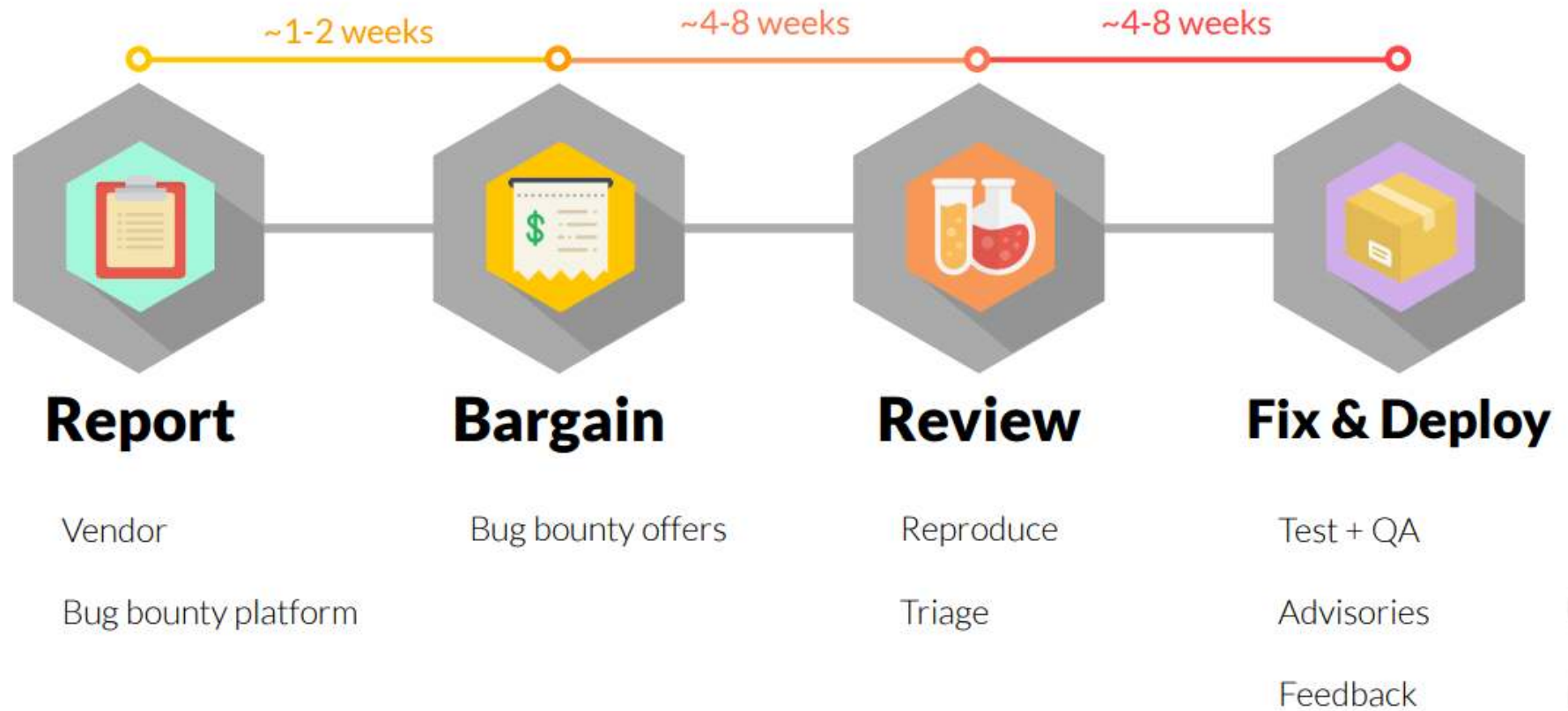
- Payouts
- Credits
- Competitions



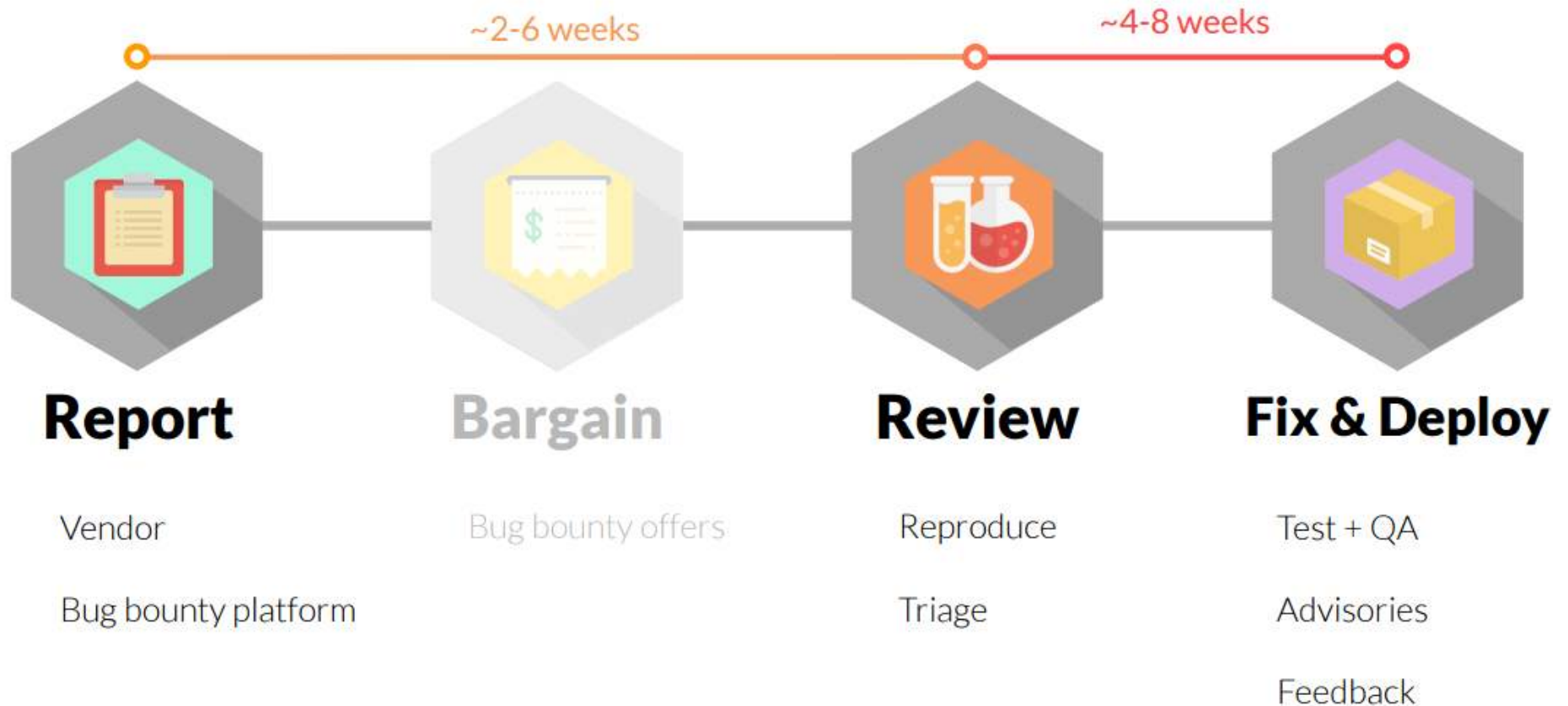
Market

- Higher payouts
- No credits

Security Updates



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.

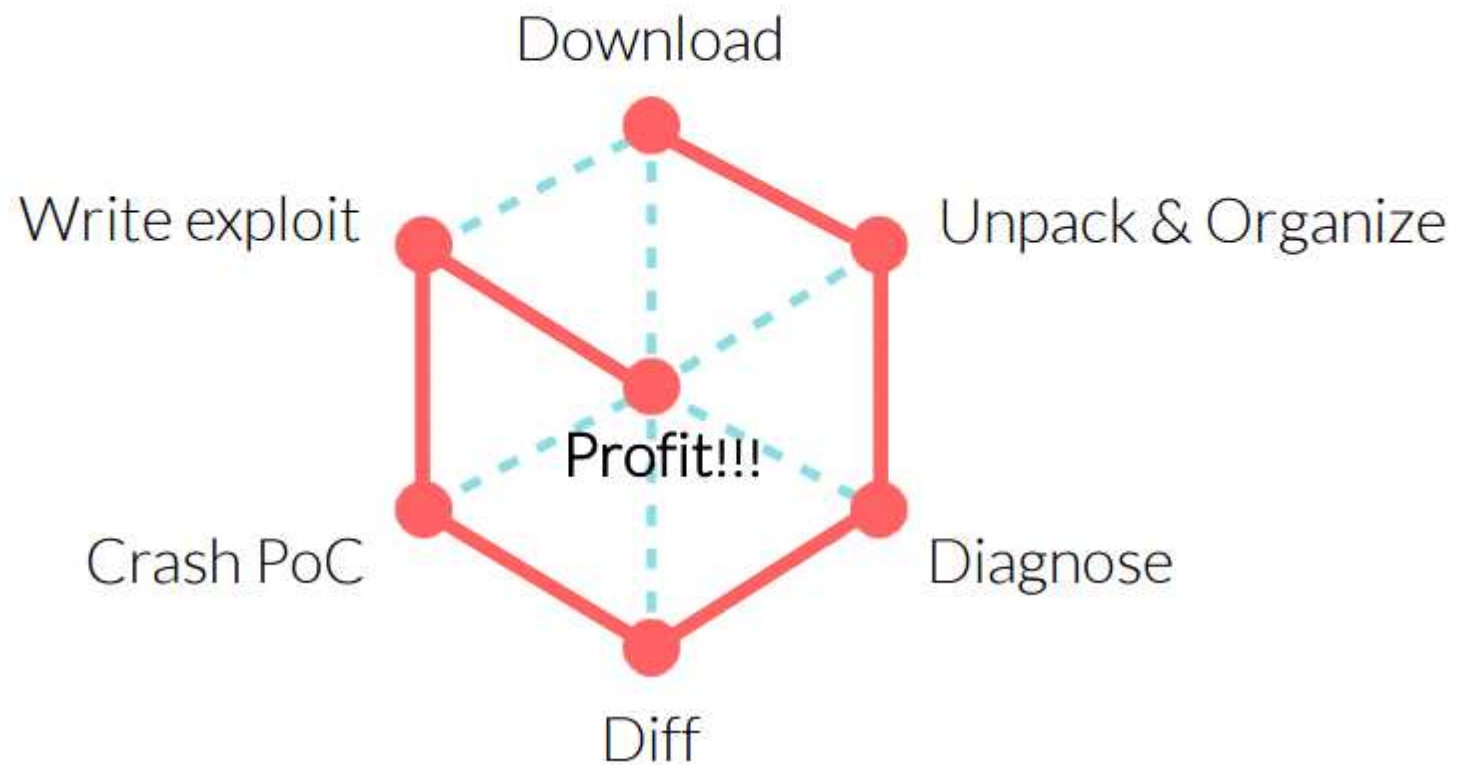
Reverse Engineering and Computer Security – Alex Sotirov

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

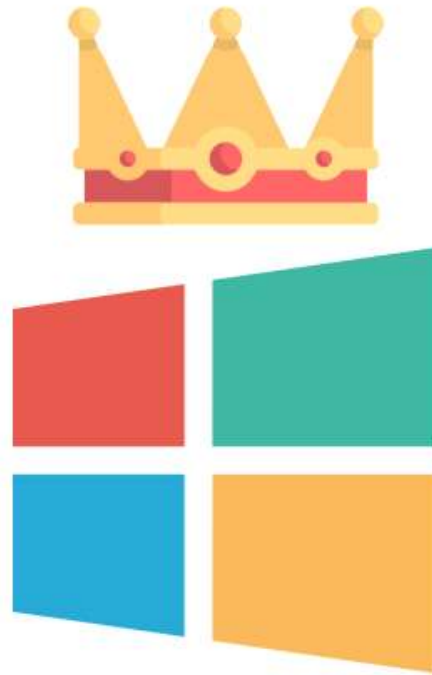
Why?



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



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 ▾

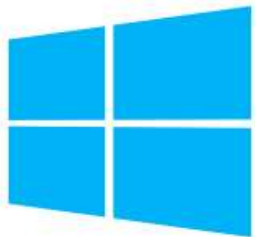
[Find the latest updates](#)

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

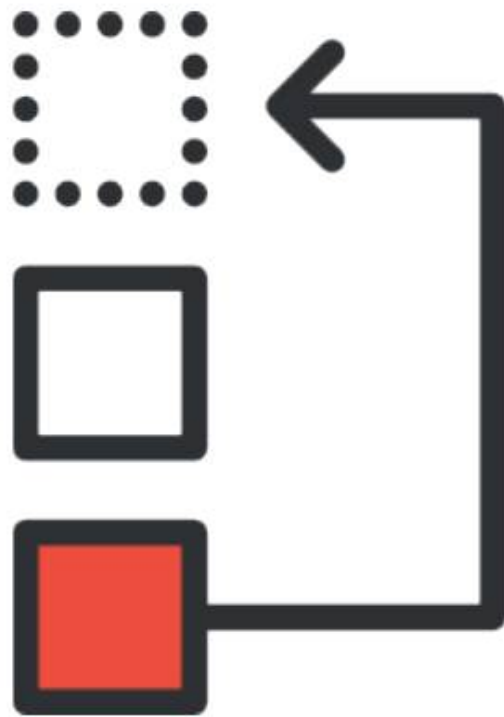


Narrow the target vulnerabilities
⇒ CVEs, Bulletins, Patch notes

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
⇒ 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 u22 = a2;
21 v7 = UAR::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 UAR **)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 = UAR::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;

```

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

April vs. May

```

23 v25 = a2;
24 v7 = UAR::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 UAR **)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 *)UAR::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 )

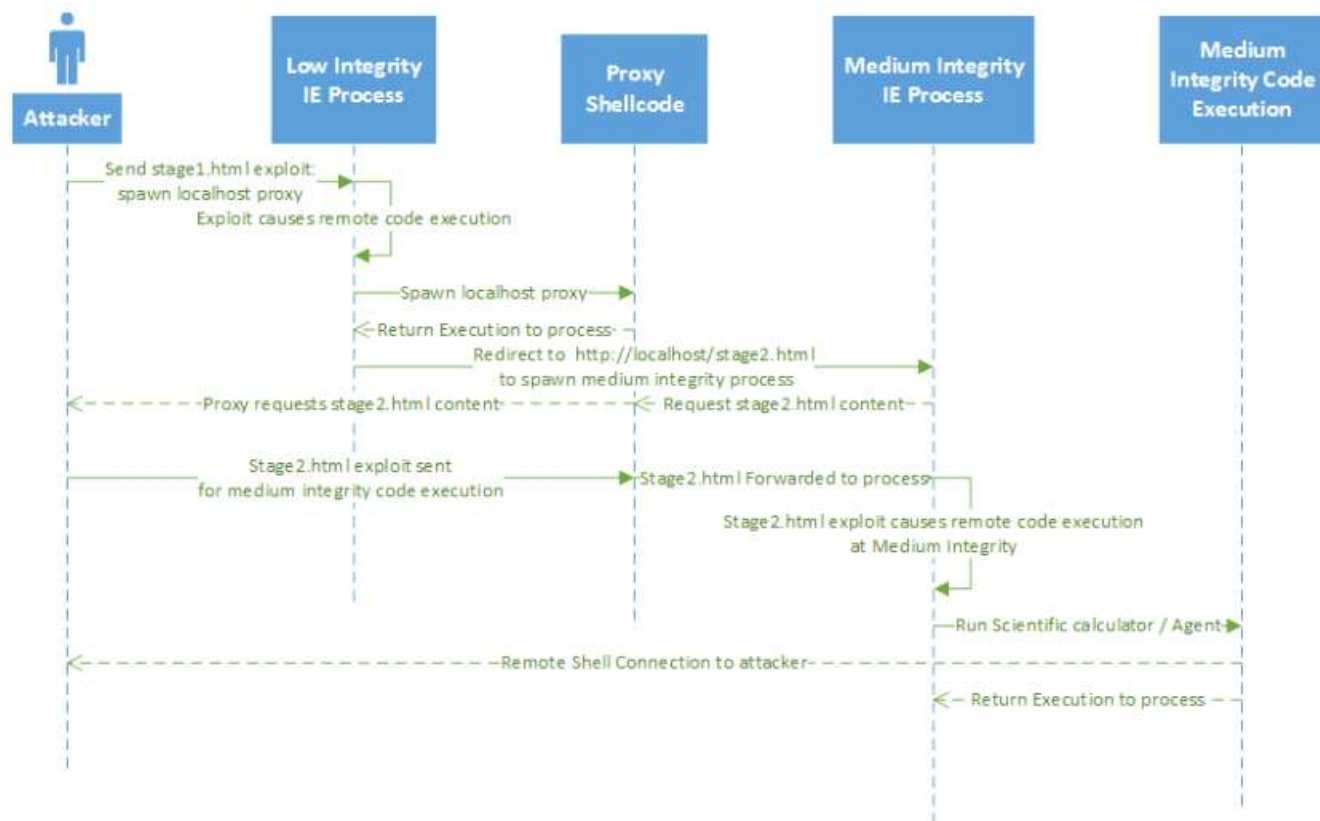
```

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

SCADA STRANGELOVE

WWW.SCADA.SL

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	85,000
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

Legend
 1000-1500 km
 1500-2000 km
 2000-2500 km
 2500-3000 km
 3000-3500 km
 3500-4000 km
 4000-4500 km
 4500-5000 km
 5000-5500 km
 5500-6000 km
 6000-6500 km
 6500-7000 km
 7000-7500 km
 7500-8000 km
 8000-8500 km
 8500-9000 km
 9000-9500 km
 9500-10000 km
 10000-10500 km
 10500-11000 km
 11000-11500 km
 11500-12000 km
 12000-12500 km
 12500-13000 km
 13000-13500 km
 13500-14000 km
 14000-14500 km
 14500-15000 km
 15000-15500 km
 15500-16000 km
 16000-16500 km
 16500-17000 km
 17000-17500 km
 17500-18000 km
 18000-18500 km
 18500-19000 km
 19000-19500 km
 19500-20000 km
 20000-20500 km
 20500-21000 km
 21000-21500 km
 21500-22000 km
 22000-22500 km
 22500-23000 km
 23000-23500 km
 23500-24000 km
 24000-24500 km
 24500-25000 km
 25000-25500 km
 25500-26000 km
 26000-26500 km
 26500-27000 km
 27000-27500 km
 27500-28000 km
 28000-28500 km
 28500-29000 km
 29000-29500 km
 29500-30000 km
 30000-30500 km
 30500-31000 km
 31000-31500 km
 31500-32000 km
 32000-32500 km
 32500-33000 km
 33000-33500 km
 33500-34000 km
 34000-34500 km
 34500-35000 km
 35000-35500 km
 35500-36000 km
 36000-36500 km
 36500-37000 km
 37000-37500 km
 37500-38000 km
 38000-38500 km
 38500-39000 km
 39000-39500 km
 39500-40000 km
 40000-40500 km
 40500-41000 km
 41000-41500 km
 41500-42000 km
 42000-42500 km
 42500-43000 km
 43000-43500 km
 43500-44000 km
 44000-44500 km
 44500-45000 km
 45000-45500 km
 45500-46000 km
 46000-46500 km
 46500-47000 km
 47000-47500 km
 47500-48000 km
 48000-48500 km
 48500-49000 km
 49000-49500 km
 49500-50000 km
 50000-50500 km
 50500-51000 km
 51000-51500 km
 51500-52000 km
 52000-52500 km
 52500-53000 km
 53000-53500 km
 53500-54000 km
 54000-54500 km
 54500-55000 km
 55000-55500 km
 55500-56000 km
 56000-56500 km
 56500-57000 km
 57000-57500 km
 57500-58000 km
 58000-58500 km
 58500-59000 km
 59000-59500 km
 59500-60000 km
 60000-60500 km
 60500-61000 km
 61000-61500 km
 61500-62000 km
 62000-62500 km
 62500-63000 km
 63000-63500 km
 63500-64000 km
 64000-64500 km
 64500-65000 km
 65000-65500 km
 65500-66000 km
 66000-66500 km
 66500-67000 km
 67000-67500 km
 67500-68000 km
 68000-68500 km
 68500-69000 km
 69000-69500 km
 69500-70000 km
 70000-70500 km
 70500-71000 km
 71000-71500 km
 71500-72000 km
 72000-72500 km
 72500-73000 km
 73000-73500 km
 73500-74000 km
 74000-74500 km
 74500-75000 km
 75000-75500 km
 75500-76000 km
 76000-76500 km
 76500-77000 km
 77000-77500 km
 77500-78000 km
 78000-78500 km
 78500-79000 km
 79000-79500 km
 79500-80000 km
 80000-80500 km
 80500-81000 km
 81000-81500 km
 81500-82000 km
 82000-82500 km
 82500-83000 km
 83000-83500 km
 83500-84000 km
 84000-84500 km
 84500-85000 km
 85000-85500 km
 85500-86000 km
 86000-86500 km
 86500-87000 km
 87000-87500 km
 87500-88000 km
 88000-88500 km
 88500-89000 km
 89000-89500 km
 89500-90000 km
 90000-90500 km
 90500-91000 km
 91000-91500 km
 91500-92000 km
 92000-92500 km
 92500-93000 km
 93000-93500 km
 93500-94000 km
 94000-94500 km
 94500-95000 km
 95000-95500 km
 95500-96000 km
 96000-96500 km
 96500-97000 km
 97000-97500 km
 97500-98000 km
 98000-98500 km
 98500-99000 km
 99000-99500 km
 99500-100000 km
 100000-100500 km
 100500-101000 km
 101000-101500 km
 101500-102000 km
 102000-102500 km
 102500-103000 km
 103000-103500 km
 103500-104000 km
 104000-104500 km
 104500-105000 km
 105000-105500 km
 105500-106000 km
 106000-106500 km
 106500-107000 km
 107000-107500 km
 107500-108000 km
 108000-108500 km
 108500-109000 km
 109000-109500 km
 109500-110000 km
 110000-110500 km
 110500-111000 km
 111000-111500 km
 111500-112000 km
 112000-112500 km
 112500-113000 km
 113000-113500 km
 113500-114000 km
 114000-114500 km
 114500-115000 km
 115000-115500 km
 115500-116000 km
 116000-116500 km
 116500-117000 km
 117000-117500 km
 117500-118000 km
 118000-118500 km
 118500-119000 km
 119000-119500 km
 119500-120000 km
 120000-120500 km
 120500-121000 km
 121000-121500 km
 121500-122000 km
 122000-122500 km
 122500-123000 km
 123000-123500 km
 123500-124000 km
 124000-124500 km
 124500-125000 km
 125000-125500 km
 125500-126000 km
 126000-126500 km
 126500-127000 km
 127000-127500 km
 127500-128000 km
 128000-128500 km
 128500-129000 km
 129000-129500 km
 129500-130000 km
 130000-130500 km
 130500-131000 km
 131000-131500 km
 131500-132000 km
 132000-132500 km
 132500-133000 km
 133000-133500 km
 133500-134000 km
 134000-134500 km
 134500-135000 km
 135000-135500 km
 135500-136000 km
 136000-136500 km
 136500-137000 km
 137000-137500 km
 137500-138000 km
 138000-138500 km
 138500-139000 km
 139000-139500 km
 139500-140000 km
 140000-140500 km
 140500-141000 km
 141000-141500 km
 141500-142000 km
 142000-142500 km
 142500-143000 km
 143000-143500 km
 143500-144000 km
 144000-144500 km
 144500-145000 km
 145000-145500 km
 145500-146000 km
 146000-146500 km
 146500-147000 km
 147000-147500 km
 147500-148000 km
 148000-148500 km
 148500-149000 km
 149000-149500 km
 149500-150000 km
 150000-150500 km
 150500-151000 km
 151000-151500 km
 151500-152000 km
 152000-152500 km
 152500-153000 km
 153000-153500 km
 153500-154000 km
 154000-154500 km
 154500-155000 km
 155000-155500 km
 155500-156000 km
 156000-156500 km
 156500-157000 km
 157000-157500 km
 157500-158000 km
 158000-158500 km
 158500-159000 km
 159000-159500 km
 159500-160000 km
 160000-160500 km
 160500-161000 km
 161000-161500 km
 161500-162000 km
 162000-162500 km
 162500-163000 km
 163000-163500 km
 163500-164000 km
 164000-164500 km
 164500-165000 km
 165000-165500 km
 165500-166000 km
 166000-166500 km
 166500-167000 km
 167000-167500 km
 167500-168000 km
 168000-168500 km
 168500-169000 km
 169000-169500 km
 169500-170000 km
 170000-170500 km
 170500-171000 km
 171000-171500 km
 171500-172000 km
 172000-172500 km
 172500-173000 km
 173000-173500 km
 173500-174000 km
 174000-174500 km
 174500-175000 km
 175000-175500 km
 175500-176000 km
 176000-176500 km
 176500-177000 km
 177000-177500 km
 177500-178000 km
 178000-178500 km
 178500-179000 km
 179000-179500 km
 179500-180000 km
 180000-180500 km
 180500-181000 km
 181000-181500 km
 181500-182000 km
 182000-182500 km
 182500-183000 km
 183000-183500 km
 183500-184000 km
 184000-184500 km
 184500-185000 km
 185000-185500 km
 185500-186000 km
 186000-186500 km
 186500-187000 km
 187000-187500 km
 187500-188000 km
 188000-188500 km
 188500-189000 km
 189000-189500 km
 189500-190000 km
 190000-190500 km
 190500-191000 km
 191000-191500 km
 191500-192000 km
 192000-192500 km
 192500-193000 km
 193000-193500 km
 193500-194000 km
 194000-194500 km
 194500-195000 km
 195000-195500 km
 195500-196000 km
 196000-196500 km
 196500-197000 km
 197000-197500 km
 197500-198000 km
 198000-198500 km
 198500-199000 km
 199000-199500 km
 199500-200000 km
 200000-200500 km
 200500-201000 km
 201000-201500 km
 201500-202000 km
 202000-202500 km
 202500-203000 km
 203000-203500 km
 203500-204000 km
 204000-204500 km
 204500-205000 km
 205000-205500 km
 205500-206000 km
 206000-206500 km
 206500-207000 km
 207000-207500 km
 207500-208000 km
 208000-208500 km
 208500-209000 km
 209000-209500 km
 209500-210000 km
 210000-210500 km
 210500-211000 km
 211000-211500 km
 211500-212000 km
 212000-212500 km
 212500-213000 km
 213000-213500 km
 213500-214000 km
 214000-214500 km
 214500-215000 km
 215000-215500 km
 215500-216000 km
 216000-216500 km
 216500-217000 km
 217000-217500 km
 217500-218000 km
 218000-218500 km
 218500-219000 km
 219000-219500 km
 219500-220000 km
 220000-220500 km
 220500-221000 km
 221000-221500 km
 221500-222000 km
 222000-222500 km
 222500-223000 km
 223000-223500 km
 223500-224000 km
 224000-224500 km
 224500-225000 km
 225000-225500 km
 225500-226000 km
 226000-226500 km
 226500-227000 km
 227000-227500 km
 227500-228000 km
 228000-228500 km
 228500-229000 km
 229000-229500 km
 229500-230000 km
 230000-230500 km
 230500-231000 km
 231000-231500 km
 231500-232000 km
 232000-232500 km
 232500-233000 km
 233000-233500 km
 233500-234000 km
 234000-234500 km
 234500-235000 km
 235000-235500 km
 235500-236000 km
 236000-236500 km
 236500-237000 km
 237000-237500 km
 237500-238000 km
 238000-238500 km
 238500-239000 km
 239000-239500 km
 239500-240000 km
 240000-240500 km
 240500-241000 km
 241000-241500 km
 241500-242000 km
 242000-242500 km
 242500-243000 km
 243000-243500 km
 243500-244000 km
 244000-244500 km
 244500-245000 km
 245000-245500 km
 245500-246000 km
 246000-246500 km
 246500-247000 km
 247000-247500 km
 247500-248000 km
 248000-248500 km
 248500-249000 km
 249000-249500 km
 249500-250000 km
 250000-250500 km
 250500-251000 km
 251000-251500 km
 251500-252000 km
 252000-252500 km
 252500-253000 km
 253000-253500 km
 253500-254000 km
 254000-254500 km
 254500-255000 km
 255000-255500 km
 255500-256000 km
 256000-256500 km
 256500-257000 km
 257000-257500 km
 257500-258000 km
 258000-258500 km
 258500-259000 km
 259000-259500 km
 259500-260000 km
 260000-260500 km
 260500-261000 km
 261000-261500 km
 261500-262000 km
 262000-262500 km
 262500-263000 km
 263000-263500 km
 263500-264000 km
 264000-264500 km
 264500-265000 km
 265000-265500 km
 265500-266000 km
 266000-266500 km
 266500-267000 km
 267000-267500 km
 267500-268000 km
 268000-268500 km
 268500-269000 km
 269000-269500 km
 269500-270000 km
 270000-270500 km
 270500-271000 km
 271000-271500 km
 271500-272000 km
 272000-272500 km
 272500-273000 km
 273000-273500 km
 273500-274000 km
 274000-274500 km
 274500-275000 km
 275000-275500 km
 275500-276000 km
 276000-276500 km
 276500-277000 km
 277000-277500 km
 277500-278000 km
 278000-278500 km
 278500-279000 km
 279000-279500 km
 279500-280000 km
 280000-280500 km
 280500-281000 km
 281000-281500 km
 281500-282000 km
 282000-282500 km
 282500-283000 km
 283000-283500 km
 283500-284000 km
 284000-284500 km
 284500-285000 km
 285000-285500 km
 285500-286000 km
 286000-286500 km
 286500-287000 km
 287000-287500 km
 287500-288000 km
 288000-288500 km
 288500-289000 km
 289000-289500 km
 289500-290000 km
 290000-290500 km
 290500-291000 km
 291000-291500 km
 291500-292000 km
 292000-292500 km
 292500-293000 km
 293000-293500 km
 293500-294000 km
 294000-294500 km
 294500-295000 km
 295000-295500 km
 295500-296000 km
 296000-296500 km
 296500-297000 km
 297000-297500 km
 297500-298000 km
 298000-298500 km
 298500-299000 km
 299000-299500 km
 299500-300000 km
 300000-300500 km
 300500-301000 km
 301000-301500 km
 301500-302000 km
 302000-302500 km
 302500-303000 km
 303000-303500 km
 303500-304000 km
 304000-304500 km
 304500-305000 km
 305000-305500 km
 305500-306000 km
 306000-306500 km
 306500-307000 km
 307000-307500 km
 307500-308000 km
 308000-308500 km
 308500-309000 km
 309000-309500 km
 309500-310000 km
 310000-310500 km
 310500-311000 km
 311000-311500 km
 311500-312000 km
 312000-312500 km
 312500-313000 km
 313000-313500 km
 313500-314000 km
 314000-314500 km
 314500-315000 km
 315000-315500 km
 315500-316000 km
 316000-316500 km
 316500-317000 km
 317000-317500 km
 317500-318000 km
 31800

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



THE COMPUTER SECURITY GROUP AT UC SANTA BARBARA



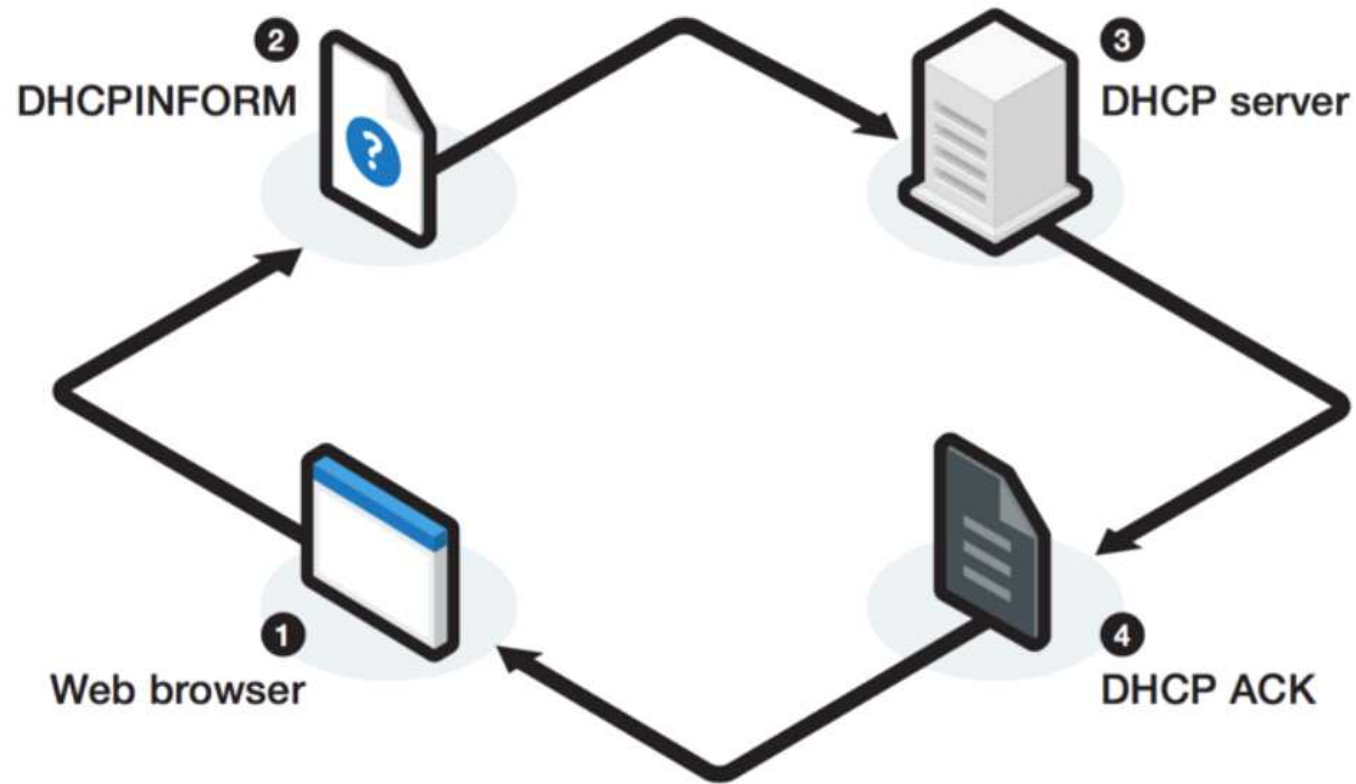
CYBER
GRAND_CHALLENGE



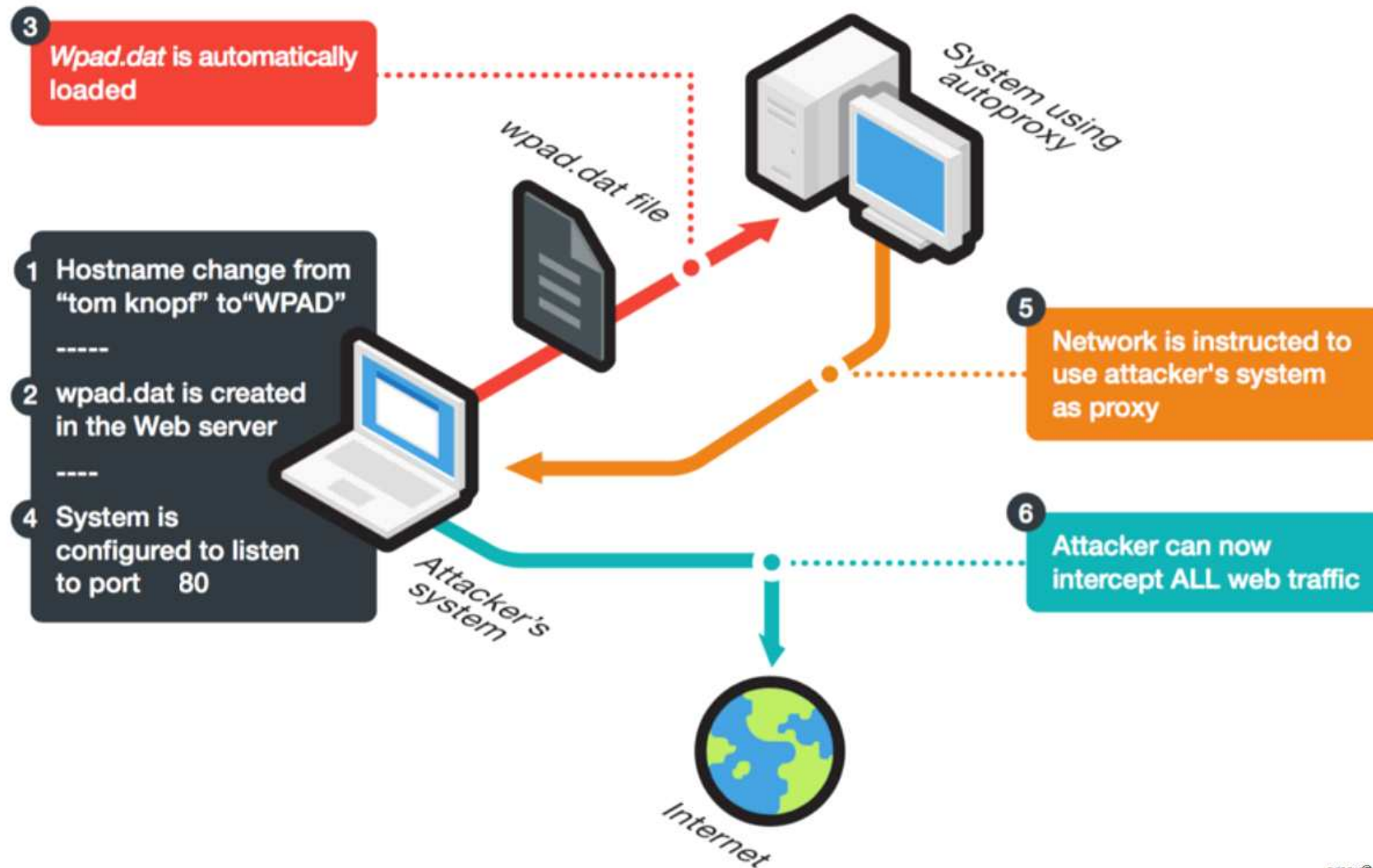


what is WPAD

DHCP Discovery Method



WPAD experiment #1











5



ENIGMA
A USENIX CONFERENCE

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

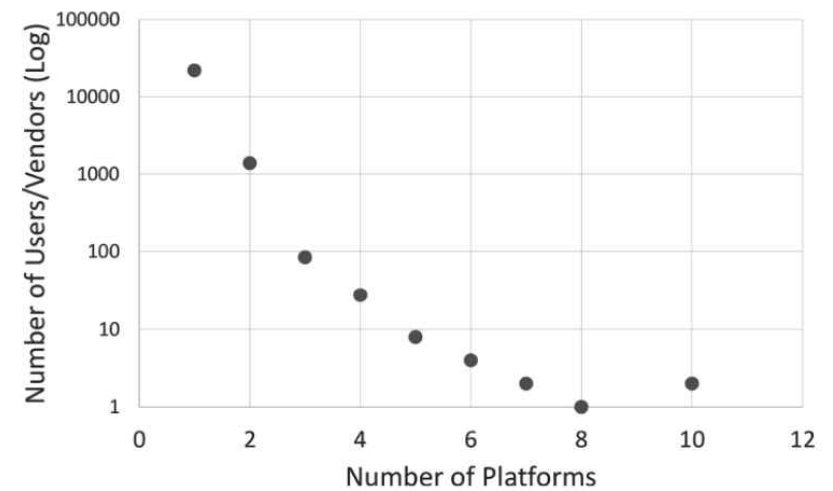
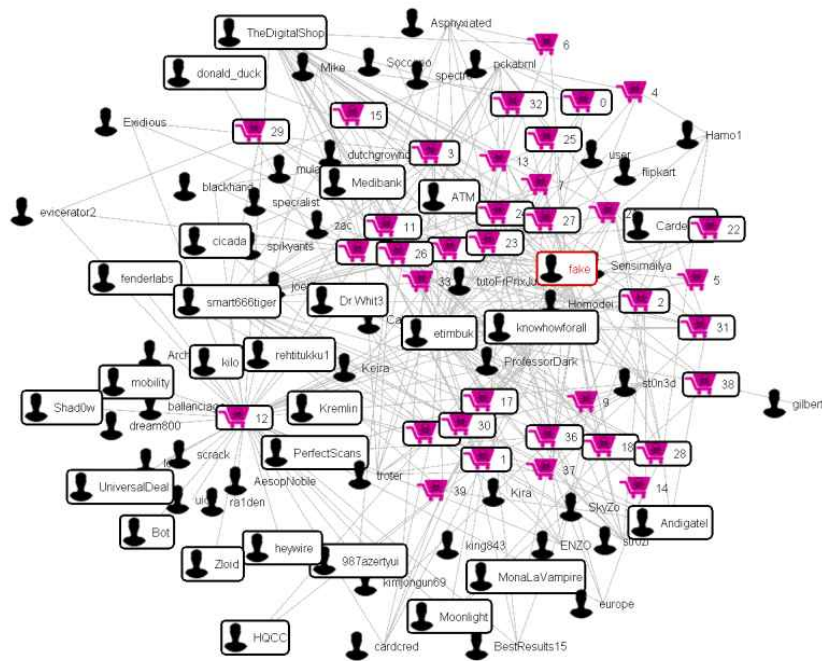
Agenda

- ❖ 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

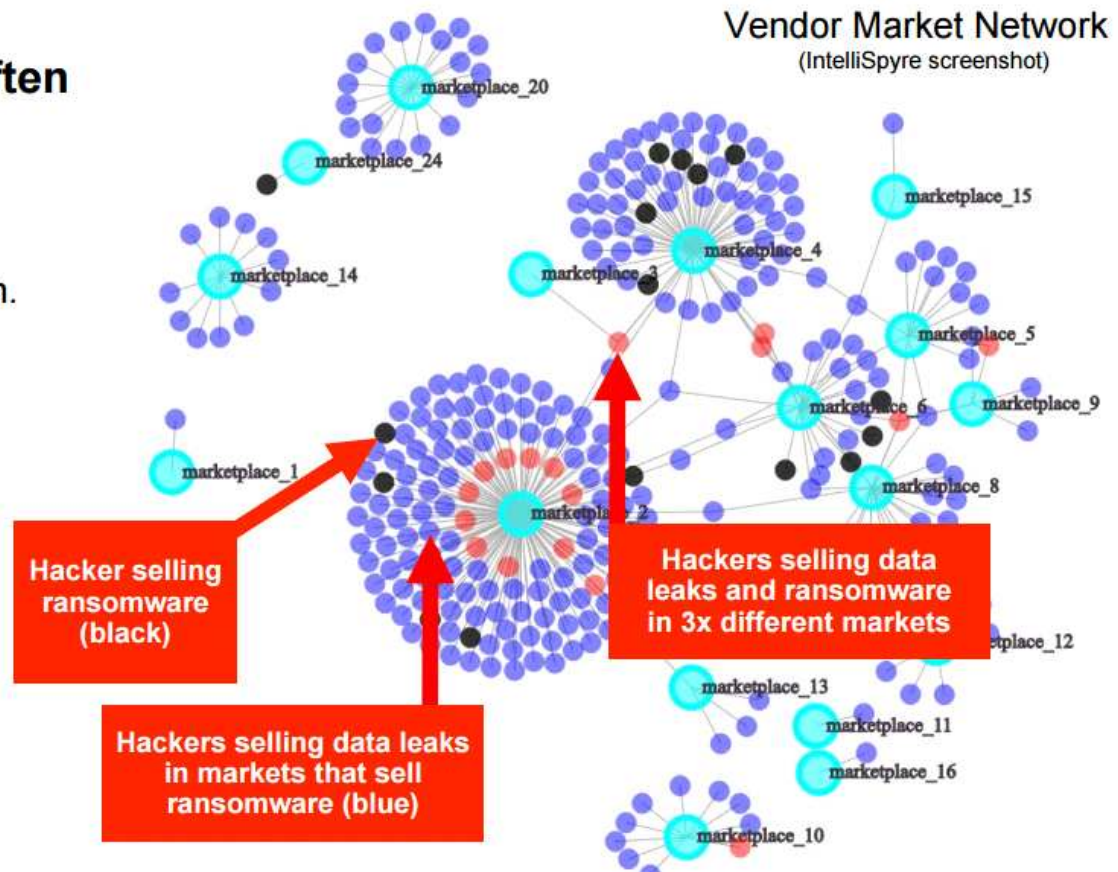
Use Case: Social Network Analysis

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.



Cisco

INNOVATION GRAND CHALLENGE

Win a share of \$250,000 to jumpstart your venture.

Submissions have closed for judging.
2016 semifinalist [have been announced!](#)

*IntelliSpyre made
the semi-finals*

15 semi-finalists

7x from U.S.

2x cybersecurity

1x from Arizona

5718

SUBMISSIONS

15

SEMIFINALISTS

6

FINALISTS

3

WINNERS



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

CRCS
Centre for Research on
Cryptography and Security

www.fi.muni.cz/crocs

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



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

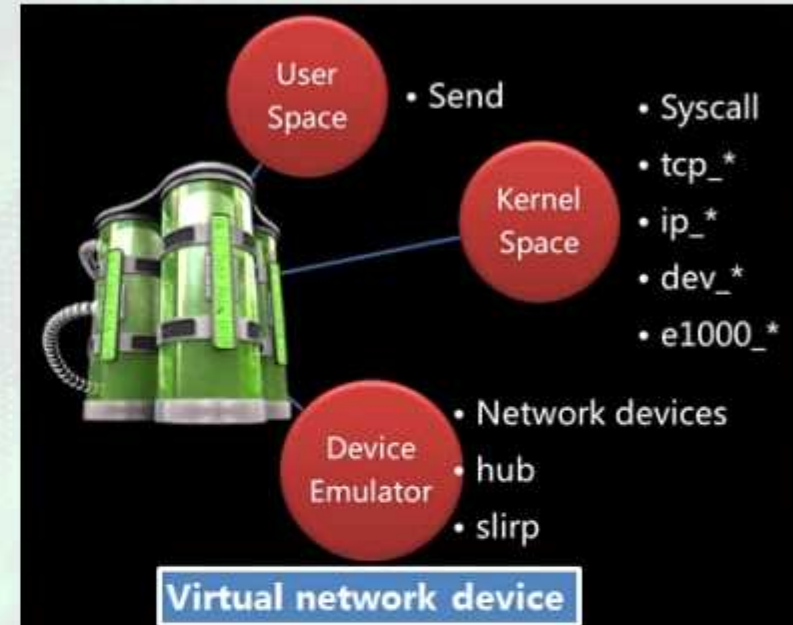
Agenda

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

VULNERABILITIES IN QEMU

Device Simulator Data Flow

Guest Machine



Host Machine

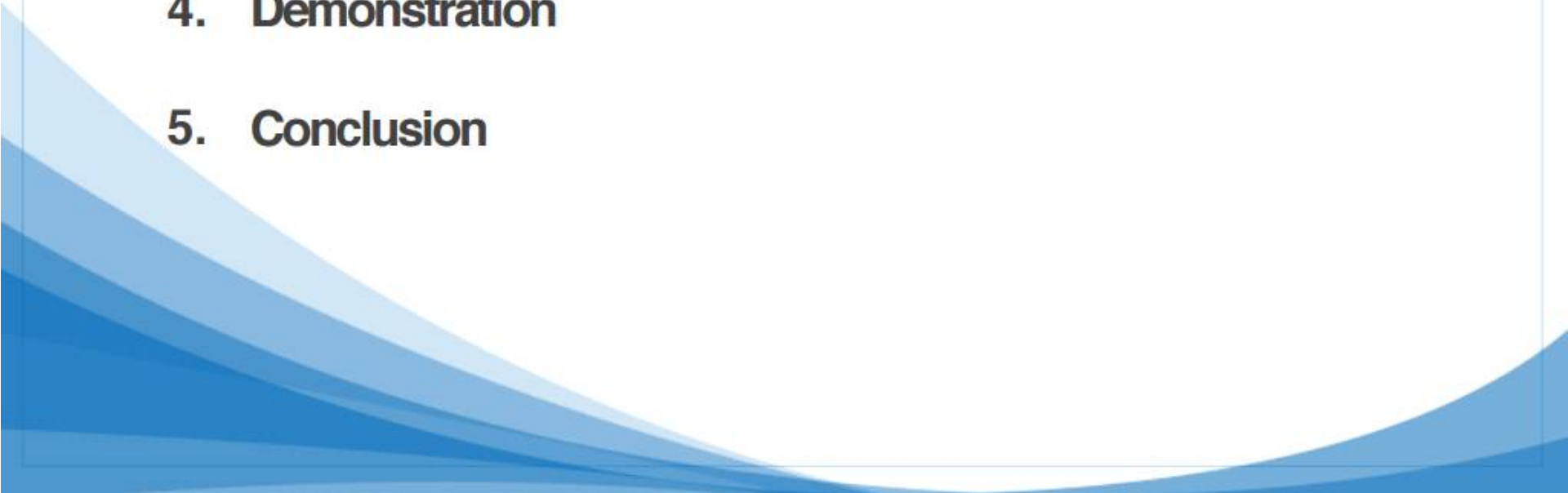
Q&A

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





Smart Platform Security

tel. 02 575 3339 / fax. 02 575 3340

www.inetcop.net

(주)아이넷캡



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

TEACHING THE NEW DOG OLD TRICKS

PHP7 Memory Internals
for Security Researchers

Yannay Livneh | Security
Researcher

