

# Following Advanced Modern Cyber Surveillance

Presentation by **Jack**  
November 2020



# Agenda

Time	Activity
15:15 – 15:35	What do I actually do? How did I get here?
15:35 – 15:55	Practical Session
15:55 – 16:00	Any questions?

# 1

What do I actually  
do?

# I am a Senior Threat Analyst.



Research **Advanced Persistent Threats (APT)** by reverse engineering and using Threat Intelligence tools



Document my findings into reports in a *timely* manner to help analysts and stakeholders in a variety of organisations



Develop *signatures* to help identify future behaviour from the same APT



*Consult* on threats to organisations



# Why do I have a job



# Reverse Engineering? Malware?

- I find a malicious “sample” and try to learn as much as possible about its functionality.
- A “samples” contents can range from executables, documents, apps, to unknown file formats
- Reverse engineering an executable can be tricky; you must have knowledge of compilers, assembly and Windows API.
- They look **scary**, but after a while you get used to them.

0115C9B0	E8 7AB90000	call <pe-sieve32.sub_116833C>	EntryPoint
0115C9C2	E9 95FEFFFF	jmp pe-sieve32.115C85C	
0115C9C7	8BFF	mov edi,edi	sub_115C9C7
0115C9C9	55	push ebp	
0115C9CA	8BEC	mov ebp,esp	
0115C9CC	51	push ecx	
0115C9CD	8365 FC 00	and dword ptr ss:[ebp-4],0	
0115C9D1	56	push esi	
0115C9D2	8D45 FC	lea eax,dword ptr ss:[ebp-4]	
0115C9D5	50	push eax	
0115C9D6	FF75 0C	push dword ptr ss:[ebp+C]	
0115C9D9	FF75 08	push dword ptr ss:[ebp+8]	
0115C9DC	E8 F6B90000	call <pe-sieve32.sub_11683D7>	
0115C9E1	8BF0	mov esi,eax	
0115C9E3	83C4 0C	add esp,C	
0115C9E6	85F6	test esi,esi	
0115C9E8	75 18	jne pe-sieve32.115CA02	
0115C9EA	3945 FC	cmp dword ptr ss:[ebp-4],eax	
0115C9ED	74 13	je pe-sieve32.115CA02	
0115C9EF	E8 B6060000	call <pe-sieve32.sub_115D0AA>	
0115C9F4	85C0	test eax,eax	
0115C9F6	74 0A	je pe-sieve32.115CA02	
0115C9F8	E8 AD060000	call <pe-sieve32.sub_115D0AA>	

IDA View-A



```
.text:0041662C 070 04 00 46 AC sw $a2, (buffer+4 - 0x100036B0)($v0)
.text:00416630 070 08 00 47 AC sw $a3, (buffer+8 - 0x100036B0)($v0)
.text:00416634 070 14 00 00 10 b loc_416688
.text:00416638 070 0C 00 48 AC sw $t0, (buffer+0xC - 0x100036B0)($v0)
.text:0041663C # -----
.text:0041663C loc_41663C: # CODE XREF: monitor_printf+5Ctj
.text:0041663C 070 44 00 A2 8F lw $v0, 0x60+var_1C($sp)
.text:00416640 070 18 00 84 8F la $a0, dword_10000000
.text:00416644 070 1C 00 85 8F la $a1, unk_490000
.text:00416648 070 9C FF 42 24 addiu $v0, -0x64
.text:0041664C 070 10 00 A2 AF sw $v0, 0x60+var_50($sp)
.text:00416650 070 38 00 A2 8F lw $v0, 0x60+var_28($sp)
.text:00416654 070 40 00 A7 8F lw $a3, 0x60+var_20($sp)
.text:00416658 070 20 83 99 8F la $t9, sprintf
.text:0041665C 070 14 00 A2 AF sw $v0, 0x60+var_4C($sp)
.text:00416660 070 34 00 A2 8F lw $v0, 0x60+var_2C($sp)
.text:00416664 070 3C 00 A6 8F lw $a2, 0x60+var_24($sp)
.text:00416668 070 80 36 84 24 addiu $a0, (buffer - 0x10000000) # s
.text:0041666C 070 18 00 A2 AF sw $v0, 0x60+var_48($sp)
.text:00416670 070 30 00 A2 8F lw $v0, 0x60+var_30($sp)
.text:00416674 070 28 18 A5 24 addiu $a1, (a02d02d02d02d02 - 0x490000) # "%02
.text:00416678 070 01 00 E7 24 addiu $a3, 1
.text:0041667C 070 09 F8 20 03 jalr $t9 ; sprintf
.text:00416680 070 1C 00 A2 AF sw $v0, 0x60+var_44($sp)
.text:00416684 070 20 00 8C 8F lw $gp, 0x60+var_40($sp)
.text:00416688 # -----
.text:00416688 loc_416688: # CODE XREF: monitor_printf+98tj
.text:00416688 070 18 00 84 8F la $a0, dword_10000000
.text:0041668C 070 28 88 99 8F la $t9, vsnprintf
.text:00416690 070 21 30 00 02 move $a2, $s0 # format
.text:00416694 070 C1 36 84 24 addiu $a0, (buffer+0x11 - 0x10000000) # s
0001667C: 0041667C: monitor_printf4 (Synchronized with Pseudoc
```

Pseudocode-A

```
int monitor_printf(const char *a1, ...)
{
    int *v2; // $s1
    size_t v3; // $s2
    int i; // $s0
    int result; // $v0
    struct timeval v6; // [sp+28h] [-38h] BYREF
    struct tm v7; // [sp+30h] [-30h] BYREF
    va_list va; // [sp+74h] [+14h] BYREF

    va_start(va, a1);
    if ( gettimeofday(&v6, 0) >= 0 )
        && localtime_r(&v6.tv_sec, &v7) )
    {
        sprintf(
            buffer,
            "%02d.%02d.%02d.%02d.%02d",
            v7.tm_mday,
            v7.tm_mon + 1,
            v7.tm_year - 100,
            v7.tm_hour,
            v7.tm_min,
            v7.tm_sec);
    }
    else
    {
        strcpy(buffer, "00.00.00 00:00:00");
    }
    v2 = &monitor_conns;
    v3 = vsnprintf(
        &buffer[17],
        0x3EFu,
        a1,
        0001667C: monitor_printf:15 (41667C (Synchroniz
```

# How did I get here? [2009]














Game Maker Home   YoYo Games Glog   Wiki   GMC Rules and Forum Rules

Calendar   Members   Search   Help

Welcome Guest ( [Log In](#) | [Register](#) )

Game Maker Community

Welcome back; your last visit was: *Today, 05:40 AM*  
Game Maker Community latest news: [Staff Changes](#)

General				 Collapse
Forum	Topics	Replies	Last Post Info	
 <b>Announcements</b> This forum will only contain official announcements by the administrators of this community. No replies are possible here.	82	32	 Last Post Jun 11 2009, 11:26 PM In: <a href="#">Staff Changes</a> By: <a href="#">KC LC</a>	
 <b>Forum Rules and Regulations</b> READ this forum for rules that pertain to this board. You will find updates to current rules and amendments to the rules. Forum Led by: <a href="#">Local Moderators</a>	13	0	 Last Post Aug 1 2009, 12:37 PM In: <a href="#">Signature And Avatar Rules</a> By: <a href="#">KC LC</a>	
 <b>The Community</b> This forum is meant for discussions about this community. Please read the rules and pinned topics prior to posting. Subforums: <a href="#">Spam Box</a> Forum Led by: <a href="#">Local Moderators</a>	5170	121182	 Last Post Today, 04:17 AM In: <a href="#">It's Been A While.</a> By: <a href="#">FredFredrickson</a>	
 <b>Web Site Announcements</b> This forum is the place for you to announce your <i>Game Maker</i> related web sites to the rest of the community. <b>No forum announcements allowed.</b> Forum Led by: <a href="#">Local Moderators</a>	3879	44354	 Last Post Today, 02:50 AM In: <a href="#">Bh Game Store</a> By: <a href="#">bobhoil</a>	
 <b>Team Requests</b> This forum is for requesting team members for your projects. Forum Led by: <a href="#">Local Moderators</a>	2477	103	 Last Post Today, 04:56 AM In: <a href="#">Game For All Ages Team..</a> By: <a href="#">Pimpinitout</a>	



# How did I get here? [2012]

The screenshot displays the OllyDbg interface with the CPU window showing assembly code. A dialog box titled "Assemble at 00401000" is open, showing the instruction "JMP SHORT 00401013" and the option "Fill with NOPs" checked. The registers window on the right shows the EIP register at 770F9CD, which is the address of the "ntdll.770F9CD" function. The memory window at the bottom shows the address 00401000, which is the start of the "YourFirstCrackme" function. The assembly code in the CPU window includes instructions like "PUSH 0", "CALL C:\Program Files\YourFirstCrackme\YourFirstCrackme.exe", and "JMP SHORT 00401013".

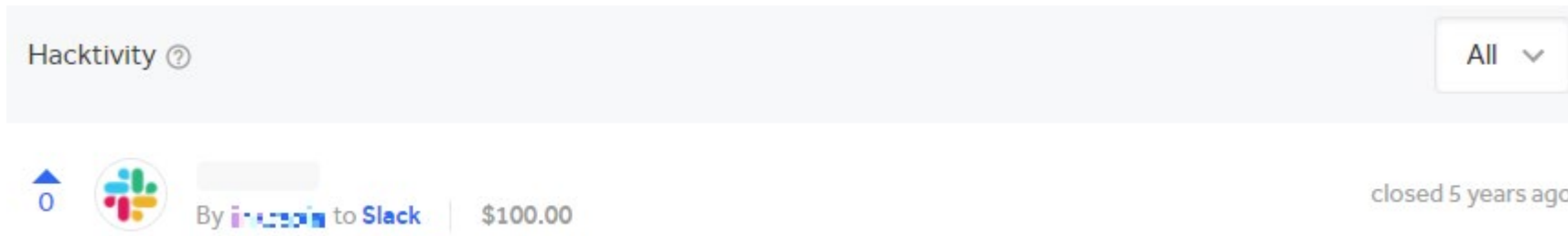
10,950 views • 25 May 2012

25 3 SHARE SAVE ...



# How did I get here? [2015]

- Went to London Metropolitan University on a 3 year course on Cyber Security and Forensics
- Started participating on bug bounties and CTFs related to pentesting
- Started researching malware and documenting on a blog
- Attempted to find vulnerabilities in software

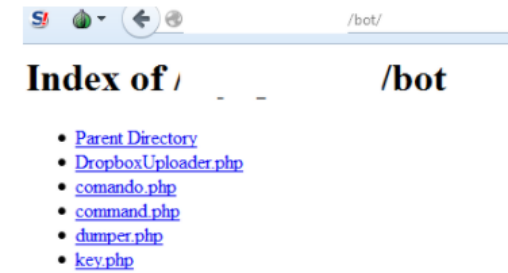


## FighterPOS – DIY Malware

AUGUST 8, 2015

I would first like to credit TrendMicro with their initial research on [FighterPOS](#). There have been an emergence of new domains for FighterPOS recently and I discovered a whole load of other possible domains that could be used for the command and control. This particular piece of malware uses an open source VB6 piece of malware called 'vnLoader'. The author of FighterPOS has either got himself or asked someone else to create a modified version to use as POS malware.

A correlation of all the panel domains is that they have no index in most directories, you can wade through most of the website without any problems allowing me to discover some differences to vnLoader and some strange pages. vnLoader was littered with SQL injections allowing anyone to take control of a panel easily. It seems the malware owner has fixed this or the hosting providers WAF is working well.



# How did I get here? [2017]

- Went through a load of interviews through recruiters for cyber security based roles
  - Usually didn't go well
  - Constantly had recruiters on my back
  - Was sent largely to financial firms
  - **That** interview which made me move away from security positions in finance
- Tweeted that I would like a job in cyber security and got a great response
  - Got a bunch of interviews
  - Chose the one which suited me and was happy with
  - Kept at it ever since



# Advice

- Build a profile of yourself if possible
- Don't worry about not having technical skills straight away
- Segment work/university work and personal projects (If you want one)
- Engage in infosec communities online/offline (Meetups, Twitter threads, conferences etc.)
- Don't be disheartened by rejection
- Parts of infosec are cliquey

# 2

Practical Session



# Considerations

- A 20 minute malware analysis session isn't going to be helpful
- Showing a malicious sample doesn't seem like a great idea
- Reversing legitimate software is a no go
- Let me show you a technique attackers use!

# What you will need

- <https://github.com/rcx/tinyPE/blob/master/smallest-pe.exe> – Trust me its not malicious, but I understand if you are not comfortable
- HxD - <https://mh-nexus.de/en/hxd/> (Or any hex editor)
- x32dbg - <https://sourceforge.net/projects/x64dbg/files/snapshots/> (Or any debugger)
- A Windows Laptop
- <https://defuse.ca/online-x86-assembler.htm> (If you want try to play around)

# Whats going on

## Assembly

```
mov eax,dword ptr fs:[30]
mov al,byte ptr ds:[eax+2]
test al,al
jne 40018B
push 6B63616A
```

## Code

```
byte[] var eaxRet = GetPEB();
byte[] var retDebug = eaxRet[2];
if(retDebug == 0x01)
{
    goto exception
}
else
{
    normal_func ...
}
```

# 3

Questions?



# Thanks

**Jack Simpson**

Senior Analyst

[jack.p.simpson@pwc.com](mailto:jack.p.simpson@pwc.com)

@linkcabin

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2020 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.