Following Advanced Modern Cyber Surveillance
## Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:35 – 15:55</td>
<td>Practical Session</td>
</tr>
<tr>
<td>15:55 – 16:00</td>
<td>Any questions?</td>
</tr>
</tbody>
</table>
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.
How did I get here? [2009]
How did I get here? [2012]
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
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
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

• [github.com/rcx/tinyPE/blob/master/smallest-pe.exe](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/](https://mh-nexus.de/en/hxd/) (Or any hex editor)

• x32dbg - [https://sourceforge.net/projects/x64dbg/files/snapshots/](https://sourceforge.net/projects/x64dbg/files/snapshots/) (Or any debugger)

• A Windows Laptop

• [https://defuse.ca/online-x86-assembler.htm](https://defuse.ca/online-x86-assembler.htm) (If you want try to play around)
Whats going on

### Assembly

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

### Code

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

Jack Simpson
Senior Analyst

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 for further details.