THE PAST, THE FUTURE, AND

... wait, where the hell are we now?
Hello, this is me
Disclaimer

The opinions and positions expressed herein are mine only and do not represent the views of any current or previous employer, including Intel Corporation or its affiliates.

This presentation has no intention to advertise or devalue any current or future technology.
Scripting monkey,
Malware analyst,
Reverse engineer,
Advanced threat detection,
Nation state malware observer,
Incident response,
And then I went low level.
(HITB \m/ -.-\m/)
Why
GOING LOW
We are all searching for something

Known - Bad
Known - Good
Non Known - Good
A PARADOX

Anti-virus is dead, they said.
Pattern matching is defeated, they claimed.
Then they came up with IOCs,
and stuffed them with patterns.
Spot the problem.
Businesses will business.
Scaling is hard.
Why it will always work but never does.

The Threat Detection Myth
All the wonders we could do,
if things just worked the way they should.

From AV to sandboxes,
from sandboxes to static analysis,
from static analysis to RE tools wonderland.

courtesy of @guedou
What the Intel® SDM taught me about reading

Some problems are answered by half a line of text within 4810 pages. Some problems aren’t.
What conference expo halls taught me about security
My field trip into policy world and the art of nation state 1:1
The A and the P of the T

APT big game hunting, like Carl would

Row row row your boat
Sneak up in the stream.
Lock n' Load in tactic mode
United States Marines.

Shut the F*ck Up Carl
Advanced Technology Is...Advanced
What nation state malware taught me about cyber war
I read 20 years of mostly-fail at cyber norms at the UN, and now you can too!

How to use this repository

Organisation & naming conventions

- Files have been renamed to reflect UN document IDs rather than job numbers (which are useless); slashes and full stops are omitted

  - e.g., A/RES/53/70 == ARESS370.pdf; A/C.1/70/PV.21 == AC170PV21.pdf; A/61/161 == A61161.pdf

- Highlights and markups are mine; don’t touch them

- Alternate and/or original language translation

Symbols

- A/ indicates a document of the General Assembly

- A/RES/##/### & ARES#### indicate a resolution

When all you have is a hammer, everything looks like APT28.

2:16 PM - 22 Aug 2017

@evacide
The unspeakable horrors of real world incident response

or, why I’m happy nation state APT isn’t SO much of a thing

Security and other professions.
The updatability problem.
Believe and the lack of believe.
The NSA has linked the WannaCry computer worm to North Korea
GOING LOW

There is a world beyond x86.
Drive, guts, pain resistance.
Patience, and more patience.

halvarflake
@halvarflake

CPU microarchitecture is a world of black magic, dragons, and endless trial & error.

10:21 AM - 27 Nov 2017
.. my first bug at Intell
All my hello worlds

... in Intel SGX
... as Linux kernel module
... in uCode
... (redacted)
The meaning of growth

The only time when you are actually growing, is when you’re uncomfortable

[Thomas Oppong, medium.com]
BlackHoodie

Free & women-only reverse engineering bootcamp
3 editions since 2015 - 15, 32 & 67 attendees
17 nationalities, 5 continents

As damn challenging as possible
Dunno, but I like it...
Creating Space

Pushing folks to dig deeper
• and go further
• and push boundaries
• and try harder
MINORITY DRIVEN BOOTCAMPS
I just hacked Minesweeper flags on all the mines starting. I'm currently person on earth.

Kernel Shim Engine for fun and not so much (but still a little?) profit

Or how to write a super long title for nothing :)

e17 talk on flash lable
What Portland taught me about being yourself
Thank you!