

████████████████████
Cylance Webinar Series //

Presented:

May 16, 2018



CYLANCE

VS

HACKING
EXPOSED

T H I N K B E Y O N D

████████████████████ Presented By //

Stuart McClure, CEO Cylance, CNE, CCSE, ██████

Paul Mehta, Chief Architect ██████████

• ██████████ Brian Robison, Sr. Dir. of Security Technology



HOUSEKEEPING

- Audio will sound best streamed through your computer
- Please submit questions via the Q&A box
- We will post additional resources in the chat box
- Your feedback is essential, please the polling questions at the end of the webinar
- Links to the recording and presentation will be sent to you in the next few days
- Need help? Contact us at: webinars@Cylance.com

SPEAKERS



Stuart McClure

CEO and co-Founder at Cylance

[@stuartmcclure](#)

[@hackingexposed](#)



Paul Mehta

Chief Architect at Cylance



Brian Robison

Sr. Director of Security
Technology at Cylance

[@CylanceSecTech](#)

QUESTIONING THE STATUS QUO...
QUESTIONING THE STATUS QUO...
QUESTIONING THE STATUS QUO...



HACKING
EXPOSED
T H I N K B E Y O N D

Why “Think Beyond”?

Questioning the status quo... [REDACTED]



THINK BEYOND

- *Apple and Steve Jobs' "Think Different"*
- More layers <> security
- Compliance <> security
- Predictive Prevention is possible
- Reimagine your endpoint, stack, architecture
- Don't "outsource" your decision making
- Threat centric prevention, before detect and respond

AGENDA

- **Network Hack**

- EternalBlue->Doublepulsar
- Password dumping the Server
 - Update->dump->extract->retrieve

- **Drive-by Upload: Spectre and Meltdown**

- Spectre (User) – Demo on Windows
 - Dump memory from a scripting language (without reading memory)
- Meltdown (Kernel) – Demo on Linux

- **Spearphish: Operation Shaheen**

- Email->DOC->Crypto attack (with an unusual twist)

- **One more thing...**

Security Training Series
Cylance Threat Prevention
Cylance Endpoint Protection
Cylance Endpoint Control



HACKING
EXPOSED
T H I N K B E Y O N D

Hands On

Hands on examples of techniques and Cylance prevention. 



eternelblue->doublepulsar
[REDACTED]
[REDACTED]



HACKING
EXPOSED
T H I N K B E Y O N D

Server over network hack

eternelblue->doublepulsar [REDACTED]
[REDACTED]



ETERNALBLUE AND DOUBLEPULSAR

- An exploit developed by the U.S. National Security Agency (NSA)
- Leaked by The Shadow Brokers in early 2017
- Exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol.
- Weaponized in WannaCry (just had 1 year anniversary)
- Further developed in Not-Petya

- DoublePulsar is a backdoor implant tool developed by the U.S. National Security Agency's (NSA)
- Runs in kernel mode



SERVER OVER NETWORK HACK



- Windows 7 x64 server
- Vulnerable SMBv1 running
- EternalBlue (the exploit) delivering Doublepulsar (the payload)
- Controlled by fb.py, FuzzBunch, an NSA Tool for exploits and implants
- Upload files as part of a campaign

- GOAL: Obtain credentials from system and drop attacks as part of a campaign



HACKING
EXPOSED
T H I N K B E Y O N D

[REDACTED]
[REDACTED] DEMO [REDACTED]

Server over network hack

SERVER OVER NETWORK HACK – WHAT CAN WE DO?

- Patching is the only way to resolve the issue
- CylancePROTECT – prevented multiple phases of this hack



Spectre
Meltdown



HACKING
EXPOSED
T H I N K B E Y O N D

Drive-By Upload

Spectre and Meltdown [REDACTED]



EXPLOITING SPECULATIVE EXECUTION

- The effects of touching memory will remain in the CPU cache
- Cache hits are faster than misses
- By measuring memory access this time, an attacker can infer memory
- Repeating many times increases reliability



PUTTING IT ALL TOGETHER



<pre>loc_691A: ; CODE cmp rsi, r9 jz short loc_6978 cflush byte ptr [rbx+rax] mov r11, [rsi] xor rax, rax mov r10, [r8] test r10, r10 jz short loc_6948 loc_6931: ; CODE mov al, [r11] shl rax, 0Ch jz short loc_6931 mov r11, [rbx+rax] add rsi, 8 add r8, 8 jmp short loc_691A</pre>	<pre>rdtsc Read the timer lfence mov r10, rax mov rbx, [rdi] lfence rdtsc Read timer again mov r11, rax sub r11, r10 mov [r13+0], r11 add r13, 8 add rdi, 1000h dec r12 jnz short loc_6948</pre>
---	--

Processor manipulation

Memory access / time measurement

Manipulate the processor state so speculative execution touches memory!

Observe the effects...
measure the time...

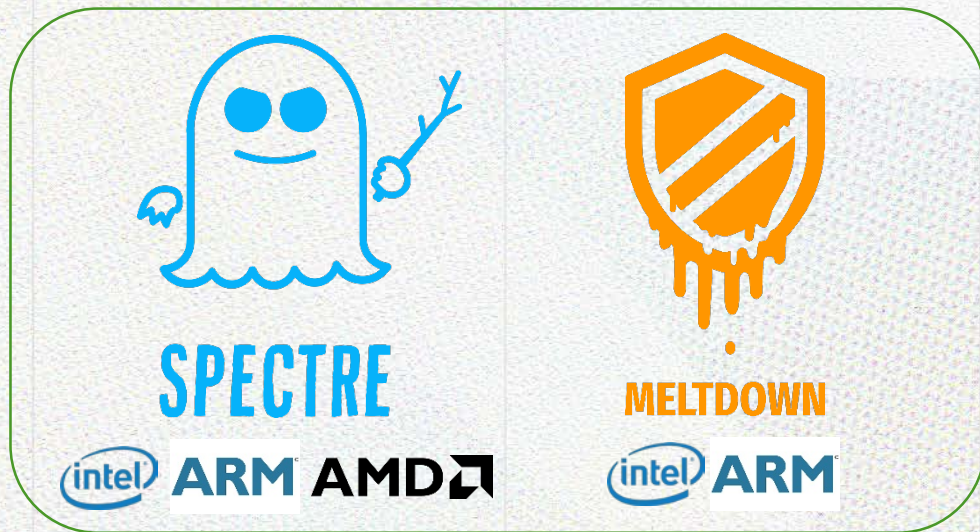
If found in the L1 cache...

...we can infer the contents of memory!



DRIVE-BY DOWNLOAD

- Windows 7 desktop
- Vulnerable Windows and Linux version running
- Meltdown on Linux
 - Show Kernel memory
- Spectre on Windows
 - Run Spectre
 - Show User memory



00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000



HACKING
EXPOSED
T H I N K B E Y O N D

The Cure Worse Than the Disease

Meltdown patch allows full memory dump [REDACTED]
[REDACTED]



PREVENTION: MELTDOWN PATCH.....?????

- Microsoft released a patch for Meltdown in January
- Kb4056897 implemented “Kernel Page Table Isolation”, or KPTI to mitigate Meltdown
 - On every context switch, page tables are swapped back and forth between kernel and userland.
 - *As you know*, page tables map virtual memory to physical memory.
 - Patch does not prevent Meltdown from leaking memory so much as it prevents the memory from being present.
- This was fixed in the March patch
- CylancePROTECT



© 2013 The Authors
All rights reserved.
No part of this publication
may be reproduced, stored
in a retrieval system, or
transmitted, in any form
or by any means, electronic,
mechanical, photocopying,
recording, or by any
information storage and
retrieval system, without
the prior written permission
of the publisher.



HACKING
EXPOSED
T H I N K B E Y O N D

Spearphish Shaheen



EXPLOIT DOCUMENT



- The exploit contained dl/exec shellcode which pulled a payload from the Pakistani FWO website.



Frontier Works Organization
(FWO)

Active : 1966-present

Country : Pakistan

Branch : Pakistan Army

- FWO is a military engineering organization, and one of the major science and technology commands of the Pakistan Army.



DOCUMENT ATTACK

- This document was downloaded from an IP that has been linked to
- C&C domain resolution using web services and attacks against Pakistani targets.
- Which for a period of a week resolved to this IP: 1**.2**.1**.1**.
 - Resolved to a subdomain of a completely unrelated topic.

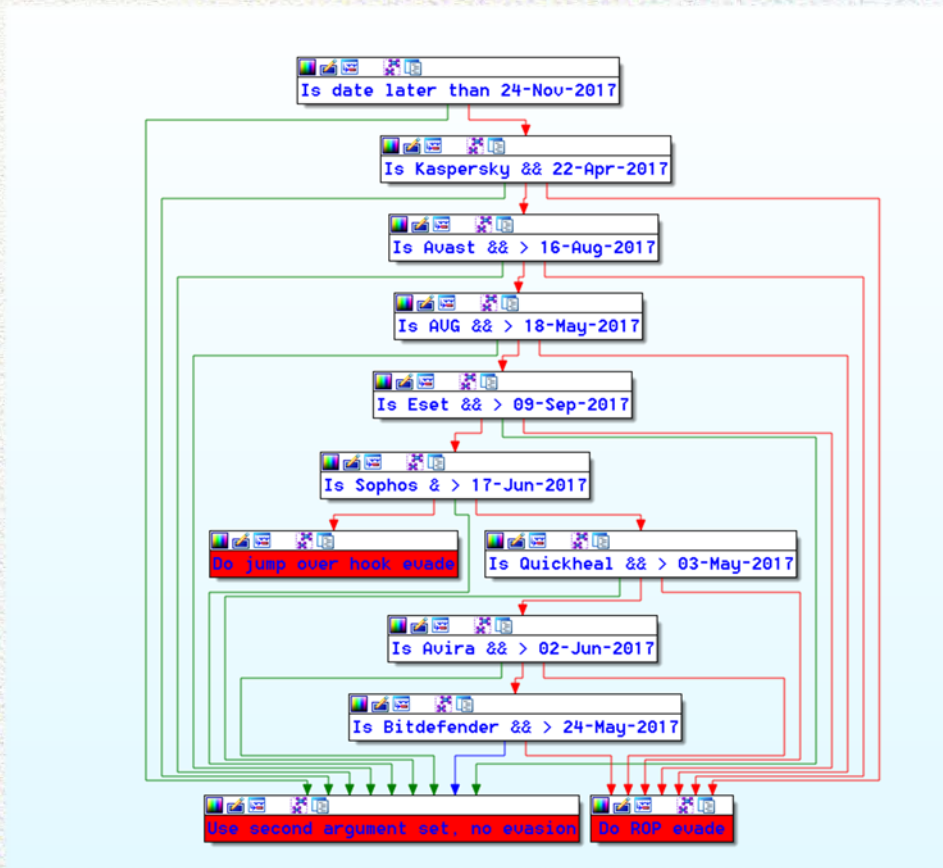
EVOLUTION

- The shellcode has evolved over time.
 - Earlier exploit docs contained basic download & execute shellcode.
 - More recent examples use multi-stage embedded payloads.
- Our samples matched based on source of the payload as well as shellcode similarities, known as code-sharing.

EVASION CAPABILITIES

- They used a relatively unique means of obfuscating function calls to evade Kaspersky.
- They went through a lot of trouble to do this among other evasions, only to stop in sync

EVASION CAPABILITIES – ANTIVIRUS???



-
-
-
-

HACKING
EXPOSED
T H I N K B E Y O N D

[REDACTED]
[REDACTED] DEMO [REDACTED]

Spearphish Shaheen

PREVENTION

- CylancePROTECT Script Control prevents initial vector, pre-execution engine detects and prevents dropper from executing

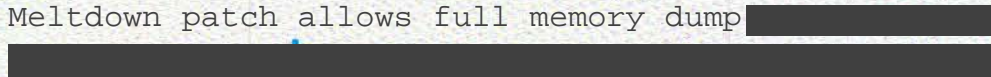
2013-07-13 10:00:00
2013-07-13 10:00:00
2013-07-13 10:00:00



HACKING
EXPOSED
T H I N K B E Y O N D

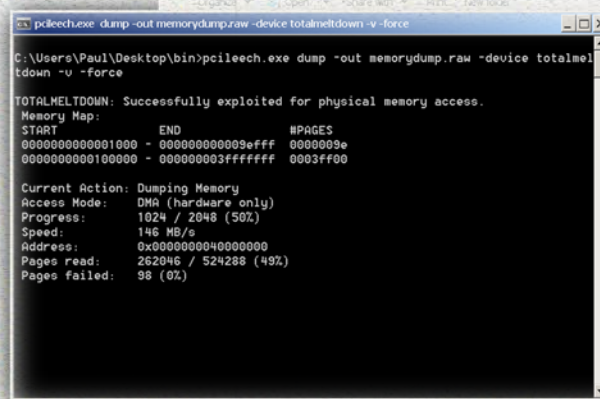
One more thing...

Meltdown patch allows full memory dump



TOTAL MELTDOWN

- On Windows 7 x64, this patch introduced a larger security hole...
 - The user/supervisor bit was set to user
 - Allowed user-mode code access to the page tables... oops
- This means userland code can access page tables and dump kernel memory with ease at 100MB+/s



```
pcileech.exe dump -out memorydump.raw -device totalmeltdown -v -force
C:\Users\Paul\Desktop\bin>pcileech.exe dump -out memorydump.raw -device totalmeltdown -v -force

TOTALMELTDOWN: Successfully exploited for physical memory access.
Memory Map:
START      END      #PAGES
000000000001000 - 000000000009ffff 0000009e
000000000100000 - 0000000003ffffff 0003ffff

Current Action: Dumping Memory
Access Mode:  DMA (hardware only)
Progress:     1024 / 2048 (50%)
Speed:       146 MB/s
Address:     0x0000000040000000
Pages read:  262046 / 524288 (49%)
Pages failed: 98 (0%)
```

HACKING EXPOSED

THINK BEYOND

QUESTIONS AND ANSWERS

Polling Questions

HACKING EXPOSED

T H I N K B E Y O N D

[REDACTED]
[REDACTED] THANK YOU [REDACTED]