



Stories from the

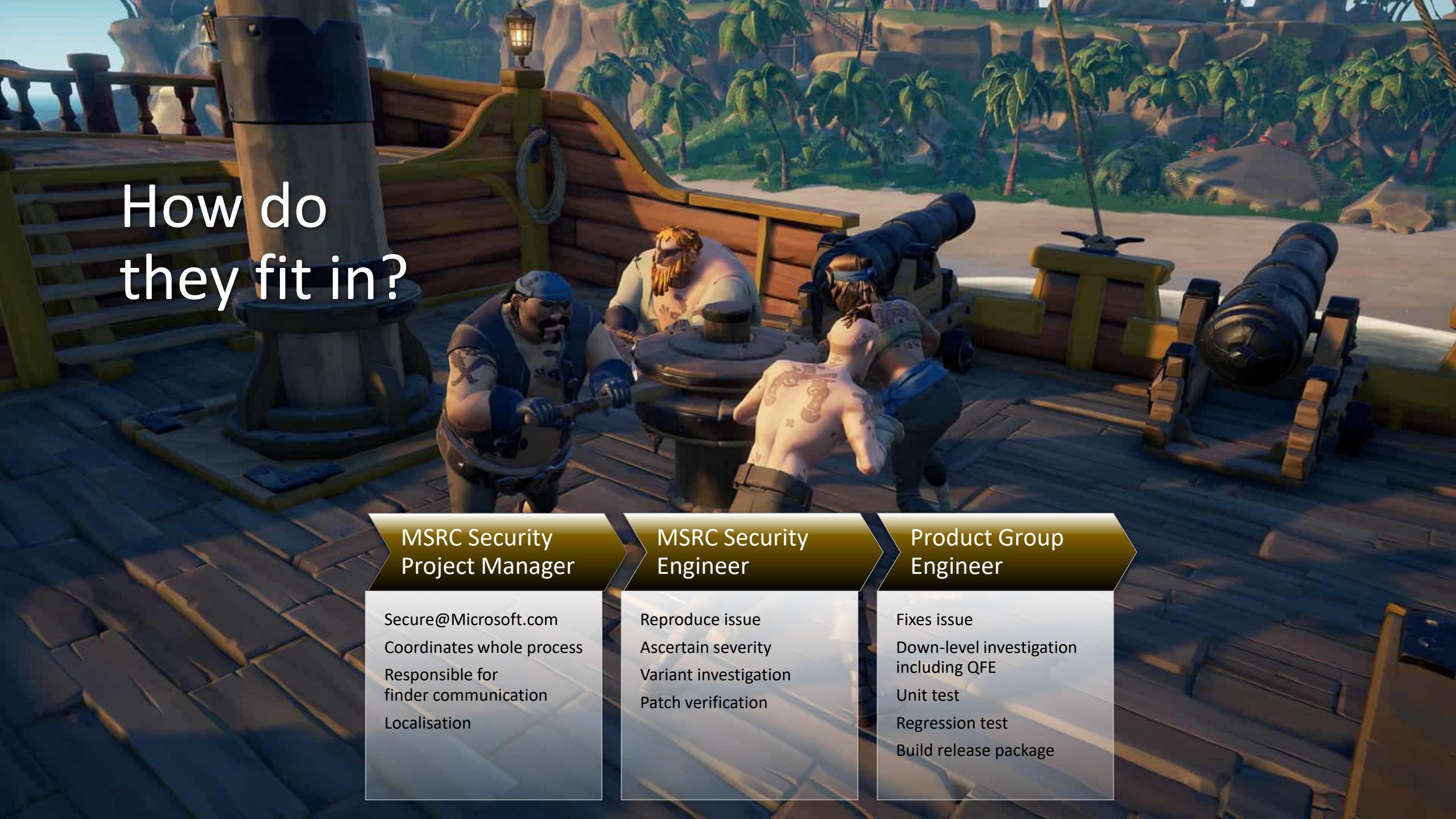
Cyber Battlefield & Protecting Customers

Microsoft Security Response Centre

MSRC Engineering



- Receives ALL externally reported vulnerabilities in ALL Microsoft products, software and services
 - From an XSS to Spectre/Meltdown
 - Reproduce (or not) the report
 - Perform Root Cause Analysis (RCA) to ascertain a severity
 - Akin to hospital initial triage
 - Work with product team as they remediate
 - Undertake a Variant Investigation
 - Takes that knowledge and researches proactive measures to protect customers



How do they fit in?

MSRC Security Project Manager

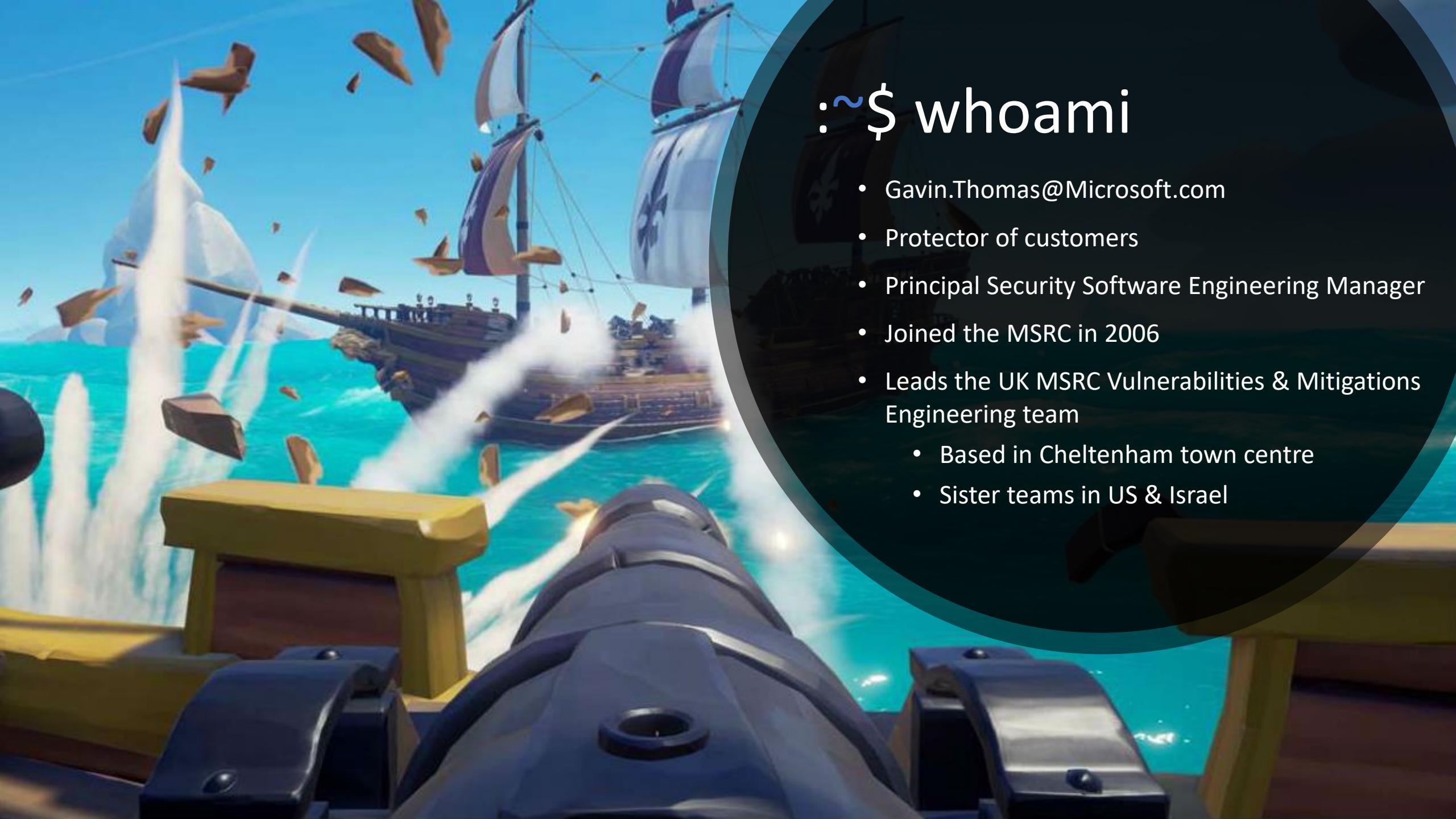
Secure@Microsoft.com
Coordinates whole process
Responsible for finder communication
Localisation

MSRC Security Engineer

Reproduce issue
Ascertain severity
Variant investigation
Patch verification

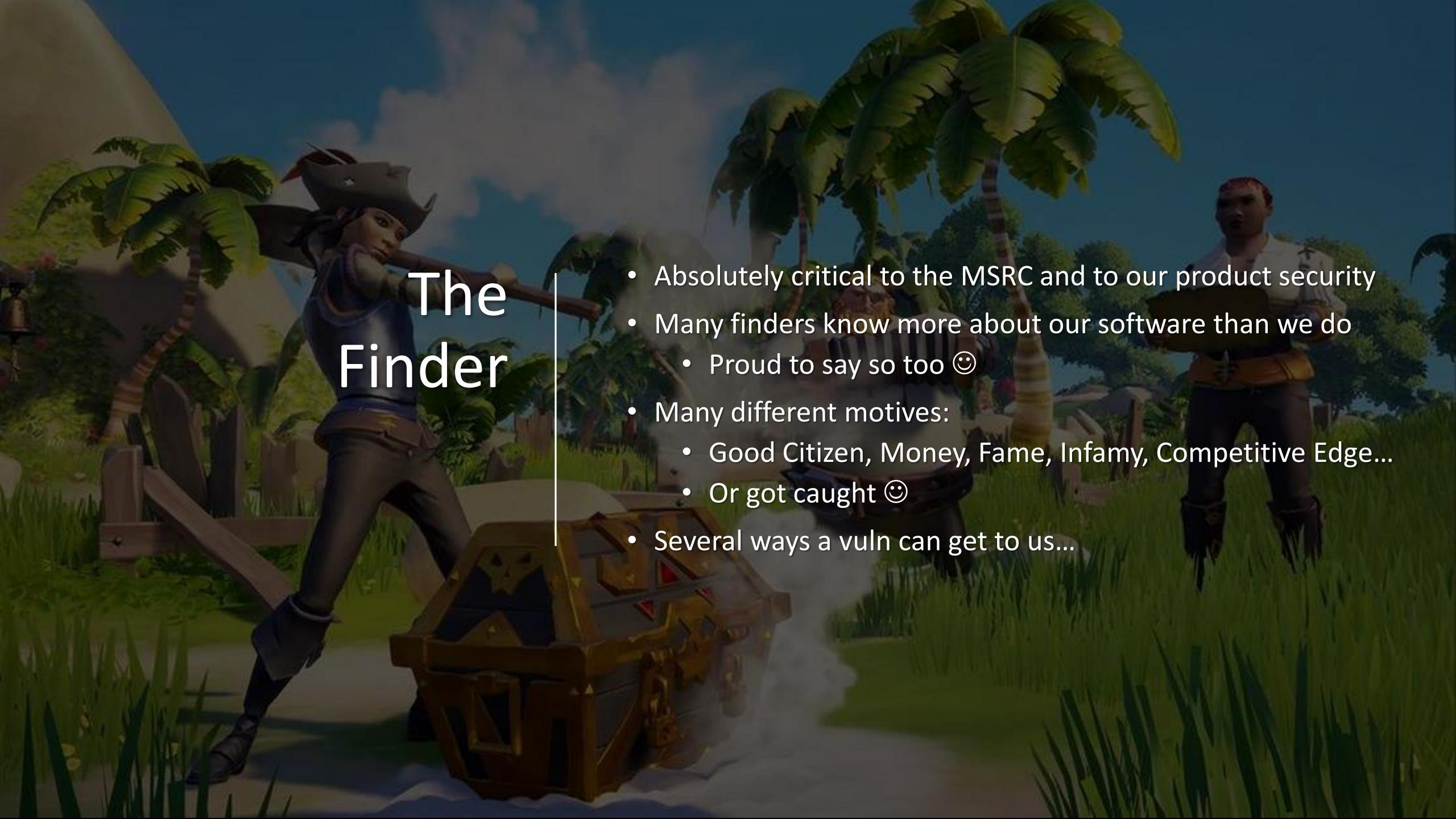
Product Group Engineer

Fixes issue
Down-level investigation including QFE
Unit test
Regression test
Build release package



:~\$ whoami

- Gavin.Thomas@Microsoft.com
- Protector of customers
- Principal Security Software Engineering Manager
- Joined the MSRC in 2006
- Leads the UK MSRC Vulnerabilities & Mitigations Engineering team
 - Based in Cheltenham town centre
 - Sister teams in US & Israel



The Finder

- Absolutely critical to the MSRC and to our product security
- Many finders know more about our software than we do
 - Proud to say so too ☺
- Many different motives:
 - Good Citizen, Money, Fame, Infamy, Competitive Edge...
 - Or got caught ☺
- Several ways a vuln can get to us...

How do Vulns get to Microsoft?

- Secure@Microsoft.com
- Receives 400+ emails a day (150,000 a year)

Report a Computer Security Vulnerability

The Microsoft Security Response Center investigates all reports of security vulnerabilities affecting Microsoft products and services. If you are a security researcher and believe you have found a Microsoft security vulnerability, we would like to work with you to investigate it.

Please note that the Microsoft Security Response Center does not provide technical support for Microsoft products. If you need assistance with something other than reporting a possible security vulnerability, please see the statement below that most closely matches your situation and expand the statement for next steps.

[Collapse All](#)

I need to report a possible security vulnerability to Microsoft.

If you are a security researcher and believe you have found a security vulnerability that meets the [definition of a security vulnerability](#) that is not resolved by the [10 Immutable Laws of Security](#), please send e-mail to us at secure@microsoft.com. To help us to better understand the nature and scope of the possible issue, please include as much of the below information as possible.

- Type of issue (buffer overflow, SQL injection, cross-site scripting, etc.)
- Product and version that contains the bug, or URL if for an online service
- Service packs, security updates, or other updates for the product you have installed
- Any special configuration required to reproduce the issue
- Step-by-step instructions to reproduce the issue on a fresh install
- Proof-of-concept or exploit code
- Impact of the issue, including how an attacker could exploit the issue

Microsoft follows Coordinated Vulnerability Disclosure (CVD) and, to protect the ecosystem, we request that those reporting to us do the same. To encrypt your message to our PGP key, please download it from the [Microsoft Security Response Center PGP Key](#). You should receive a response within 24 hours. If for some reason you do not, please follow up with us to ensure we received your original message. For further information, please visit the [Microsoft Security Response Policy and Practices page](#) and read the [Acknowledgment Policy for Microsoft Security Bulletins](#).



Searching the Interwebz for Gold

From: Axel Souchez

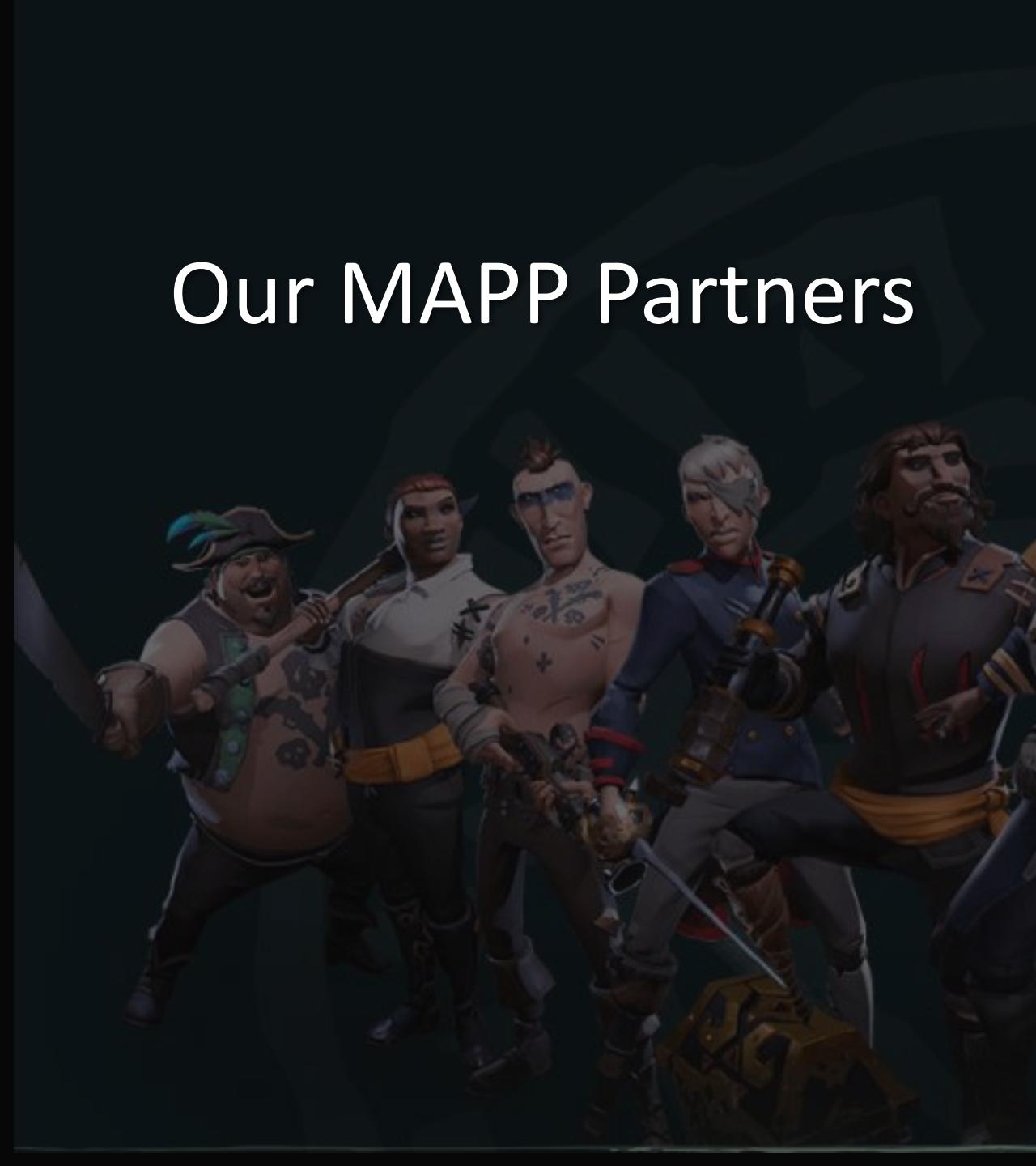
```
NTSTATUS WmipReceiveNotifications(
    PWMIRECEIVENOTIFICATION ReceiveNotification,
    PULONG OutBufferSize,
    PIRP Irp
)
{
    ...
    OBJECT_EVENT_INFO *ObjectArray;
    OBJECT_EVENT_INFO StaticObjects[MANY_NOTIFICATION_OBJECTS];
    ...
    HandleCount = ReceiveNotification->HandleCount; ← attacker controlled
}

MS16-014 Windows Elevation of Privilege Vulnerability CVE-2016-0040 Meysam Firozi @R00tkitSmm

if (ObjectArray == NULL)
{
    return (STATUS_INSUFFICIENT_RESOURCES);
}
else {
    ObjectArray = StaticObjects;
}
#if DBG
    RtlZeroMemory(ObjectArray, HandleCount * sizeof(OBJECT_EVENT_INFO));
#endif
```

The function isn't exported, but can be reached through the WMI device driver interface
(WmipIoControl/ IOCTL_WMI_RECEIVE_NOTIFICATIONS)

Our MAPP Partners



- Microsoft Active Protections Program (MAPP)
- MAPP partners have ears on the ground, can hear things we might miss
- Hunting for Zero-days and APT activity





aka.ms/bugbounty



Bounty Programmes

Program Name	Up to (USD):
Speculative Execution Side Channel Bounty	\$250,000
Microsoft Hyper-V Bounty Program	\$250,000
Bounty for Defence	\$100,000*
Mitigation Bypass Bounty	\$100,000
Windows Defender Application Guard	\$30,000
Windows Insider Preview	\$15,000
Microsoft Edge on Windows Insider Preview	\$15,000
Microsoft Office Bounty Program	\$15,000
Microsoft .NET Core and ASP.NET Core Bug Bounty Program	\$15,000
Microsoft Cloud Bounty	\$15,000

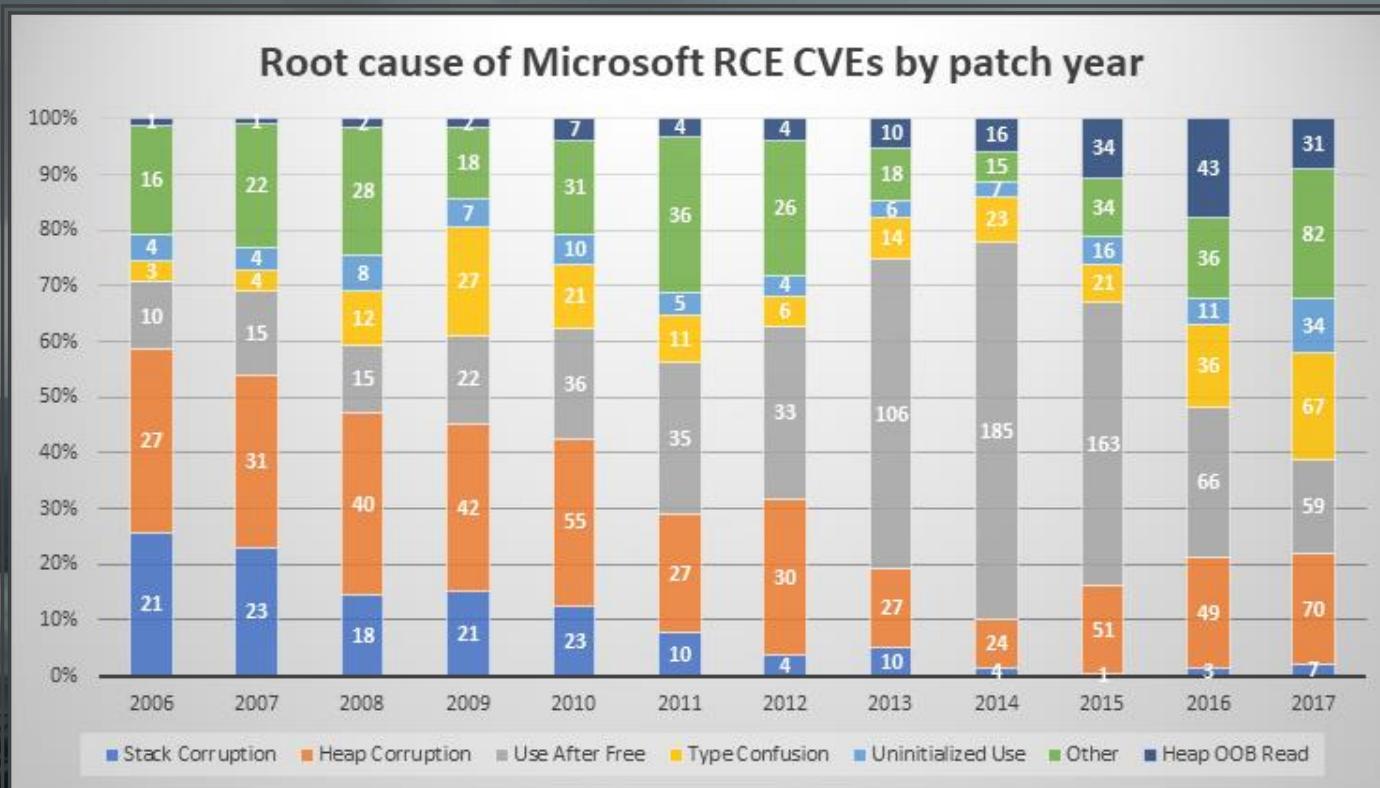
A detailed 3D rendering of a historical-style sailing vessel, likely a galleon or pirate ship. The deck is filled with wooden barrels, metal crates, and rows of mounted cannons. The ship is positioned on a calm, light blue ocean under a clear sky.

Vulnerabilities are Precious

- Paying for them via a bounty is great but:
 - Judication process can be tricky
 - Unpaid research...
 - Managing finder's is quite difficult!
- Can you remove a bounty?
 - We tried, odd results, backlash ☺
- Some (not all) bounties get significant 'hopeful' submissions
 - Unless you have automation that becomes very expensive quickly

We closely study Vulnerability Root Cause trends

Microsoft security engineers categorize the root cause of every vulnerability and look for patterns



**Stack Corruption:
Cookies and Static Analysis**

Use After Free: memGC

Type Confusion: TypeProtect

Sad Attackers = Happy Microsoft

#What the [REDACTED] ?#14 0days were killed by Yuki Tuesday pic.twitter.com/qiLMOY1QbO

CxElement::CreateElement函数中将以前调用的 MSHTML!HeapAlloc函数改成了 MSHTML!_MemIsolatedAllocClear函数，其中使用的是MSHTML!g_hIsolatedHeap堆，这招够狠！

Translati >>>

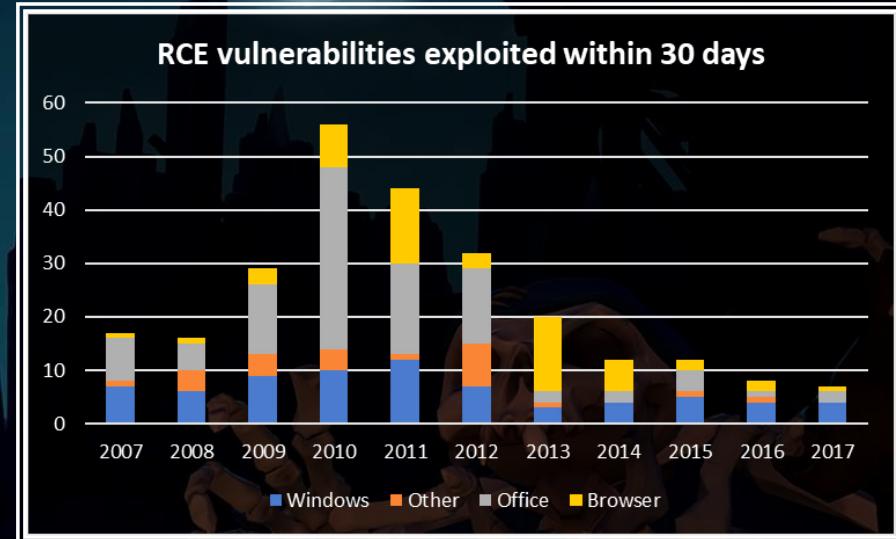
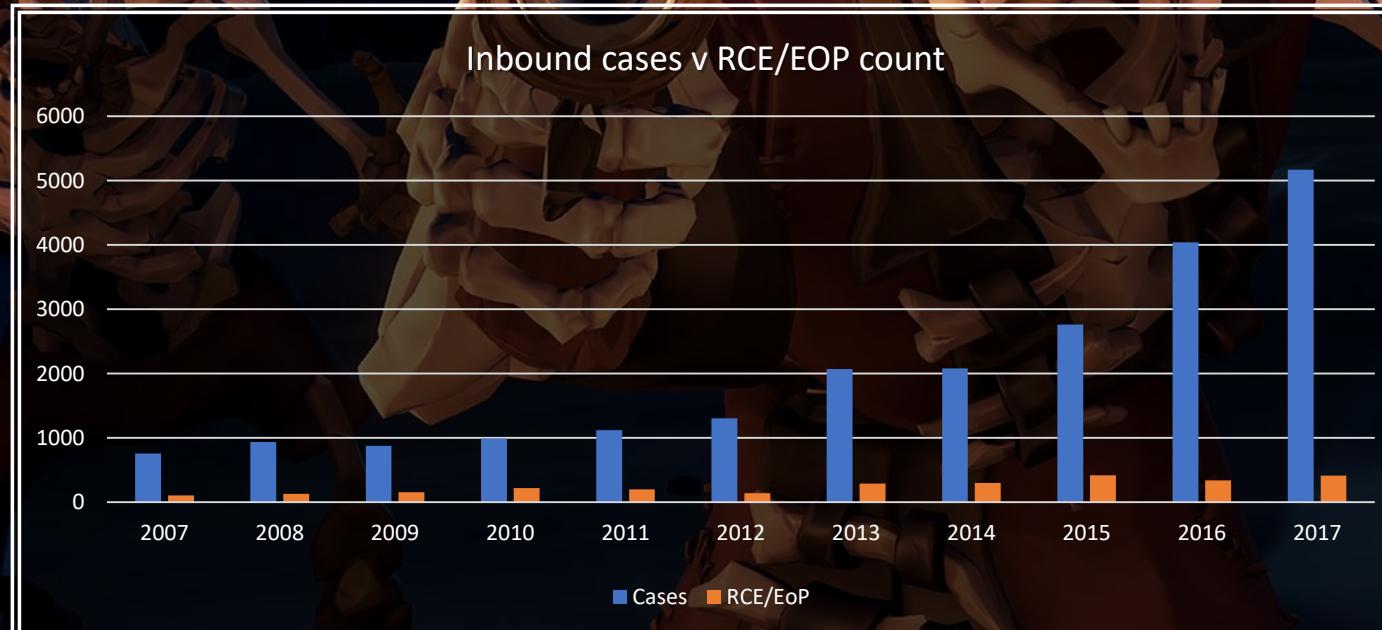
CxxxElser MSHTML
Watching the world cup while testing my PoCs against the latest IE patch. 90% of my PoCs won't work. I thought the result must be wrong? Looking more deeply, there is something new in IE again. Now, UAF would be extremely difficult. (bu MSHTML!MemoryProtection::CMemoryProtector::ProtectedFree). Seems we need to focus on type confusion bugs in the future.

>>>

	2014/6/11 7:55	HTML Document
9_patched.html	2014/6/11 7:56	HTML Document
10_patched.html	2014/6/11 7:57	HTML Document
11_patched.html	2014/6/11 7:57	HTML Document
12.html	2014/6/11 7:57	HTML Document
13.html	2014/6/11 7:58	HTML Document
14_patched.html	2014/6/11 7:59	HTML Document
15_patched.html	2014/6/11 7:59	HTML Document
16.html	2014/6/11 8:00	HTML Document
17_patched.html	2014/6/11 8:00	HTML Document

Vulnerabilities and Exploits: Different Beasts

- Vulnerabilities reported to MSRC - increased six fold
- RCE/EOP vulnerabilities receiving updates - increased four fold
- Exploits since 2010 peak - decreased by eight fold



No resting on laurels

- Let's delve into those 2017 RCE exploits....
 - Most related to APTs in some way
 - APTs using exploits and getting caught
 - STRONTIUM
 - Lazarus / ZINC
 - Leaky ships:
 - Vault 7 & Shadow Broker
 - Then used by other APTs
- MSRC not blasé
 - Pwn2Own, Power of Community

Microsoft Secure

Our commitment to our customers' security

November 1, 2016

 TERRY MYERSON
Executive Vice President, Windows and Devices Group

in Windows, Windows Defender Advanced Threat Protection, Endpoint Security, Threat Protection, Research

Windows is the only platform with a customer commitment to investigate reported security issues and proactively update impacted devices as soon as possible. And we take this responsibility very seriously.

Recently, the activity group that Microsoft Threat Intelligence calls [STRONTIUM](#) conducted a low-volume spear-phishing campaign. **Customers using Microsoft Edge on Windows 10 Anniversary Update are known to be protected from versions of this attack observed in the wild.** This attack campaign, originally identified by Google's Threat Analysis Group, used two zero-day vulnerabilities in Adobe Flash to



Conferences
Having Boots on the Ground

It's not all about vulnerabilities

“Deny macros from the ‘outside’ ”

DR624D21A64CEC905A9E64E7ED361CE612ED087B [Read-Only] [Compatibility Mode] - Word

Security baseline for Office 2016 and Office 365 ProPlus apps – FINAL

Aaron Margosis February 13, 2018

Rate this article ★★★★
Share 39 Twitter 157 LinkedIn 0 Comments 0

Microsoft is pleased to announce the *final* release of the recommended security configuration baseline settings for Microsoft Office Professional Plus 2016 and Office 365 ProPlus 2016 apps. There are no changes from the draft release we published a few weeks ago, other than minor corrections within the spreadsheet.

Highlights of this baseline:

- Streamlined baseline
- Stronger macro security
- Defending against malware by blocking Flash ActiveX activation within Office documents

Download the content here: [Office-2016-baseline](#), or as part of the [Security Compliance Toolkit](#).

The downloadable attachment to this blog post includes importable GPOs, scripts for applying the GPOs to local policy, a custom administrative template (ADMX) file for Group Policy settings, all the recommended settings in spreadsheet form and as Policy Analyzer rules. The recommended settings correspond with the Office 2016 administrative templates version 4639 released on December 15, 2017; we have included those ADMX and ADML files in a zip file in the package's Templates subdirectory.

Instead of retaining the entire Office 2013 baseline and simply adding settings that were newly introduced in the Office 2016 GPOs, we have conducted a thorough review of all available configuration settings – as we did beginning with the Windows 10 baselines – including in the baseline only those settings that address contemporary security threats. In the process we removed over eight dozen settings that had been in previous baselines but that were determined not to advance security posture in a meaningful way, and added a handful of new settings. The result is a more streamlined, purposeful baseline that is easier to configure, deploy, and validate.

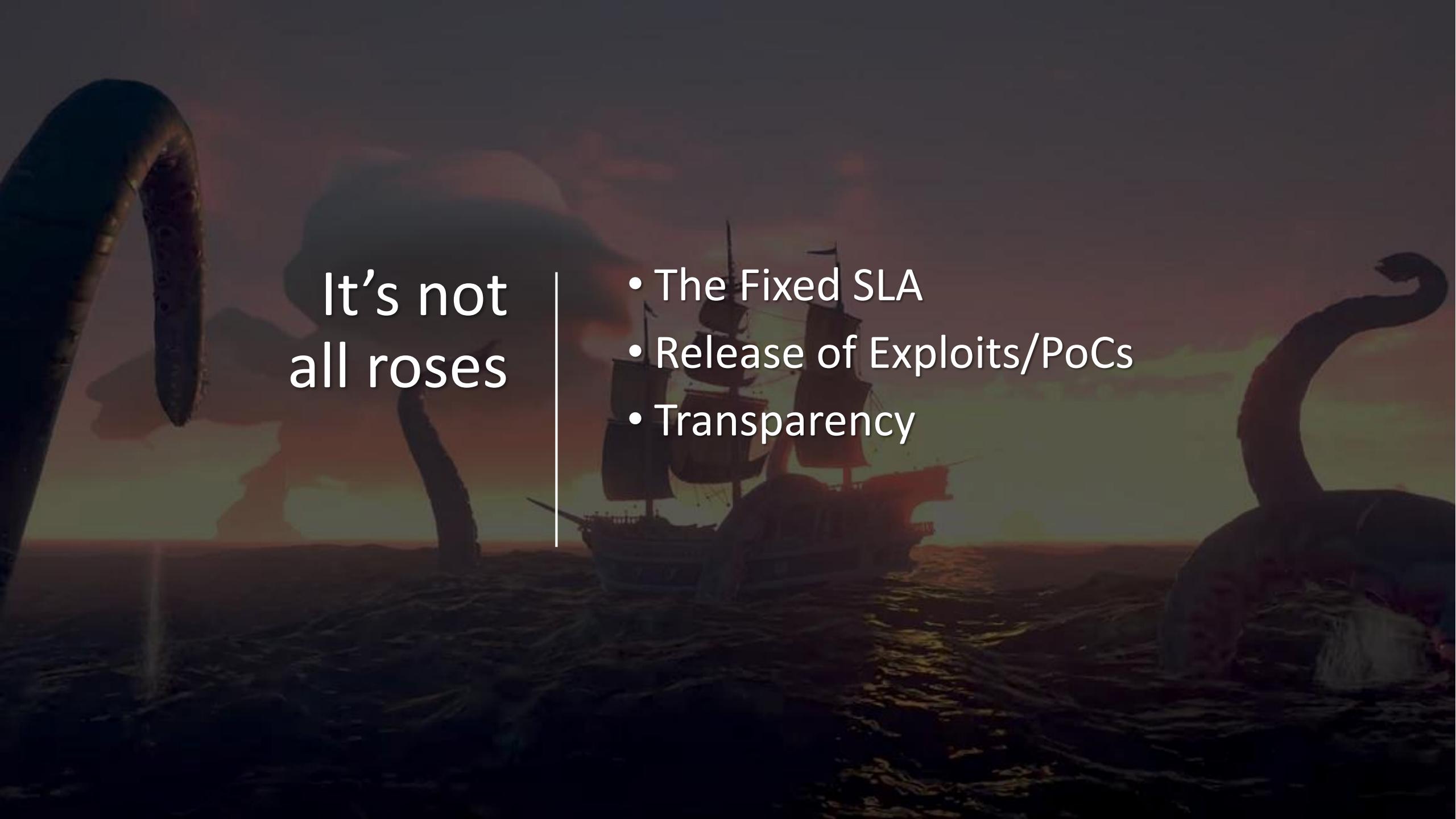
Macro security

Office's support for macros remains a vital tool for enterprise automation and at the same time a vector for attack, so macro security remains an important consideration. Office 2016 introduced a new GPO setting, "Block macros from running in Office files from the Internet" that was also later [backported](#) to Office 2013. Enabling the setting disables macros embedded in Office documents that came from the internet, including through email from an external sender. Office displays a notification that does not give the user an option to enable the macros. This baseline enables the setting for all apps that offer it: Excel, PowerPoint, Visio, and Word. Because this setting affects only Office documents received from the Internet that contain embedded macros, we anticipate that enabling this setting should rarely if ever cause operational problems for enterprises. The settings do not affect documents that are received from the enterprise's Intranet or Trusted Sites zones.

The baseline also retains the "VBA Macro Notification Settings" options from our previous baselines that require that macros embedded in Office documents be signed by a trusted publisher. We recognize that some organizations have had workflows and processes relying on such macros for a long time, and that enforcing these particular settings can cause operational issues. It can also be challenging to identify all the documents and VBA projects that need to be signed. We will continue considering moving these settings into a separate GPO to make it easier to switch the settings on or off without affecting the rest of the baseline. Please let us know via the comments on this post what you think of that idea.

Blocking Flash activation

We have also added a setting to the custom "MS Security Guide" ADMX that prevents the Adobe Flash ActiveX control from being loaded by Office applications. Vulnerabilities in Adobe Flash are often exploited by sending the victim a Microsoft Office document that contains



It's not
all roses

- The Fixed SLA
- Release of Exploits/PoCs
- Transparency

The Fixed SLA

- Where failure to adhere to an SLA, results in full disclosure
- Microsoft believes in Coordinated Vulnerability Disclosure (CVD)
- Generally speaking, SLAs are very positive to the industry
- Some fixes ‘are really hard’ and deserve more time
 - Mitigations, strategic fixes, refactoring and re-engineering are better than simple ‘point fixes’
- Variants can be difficult to find, fix and update in time
 - In the past we needed to back out variants to hit a deadline
 - Some variants were more severe and easier to find than the original issue

The Fixed SLA...

- Penalised for regression testing, penalised again if an issue is discovered
- Regression testing is **imperative** to security...
- Much time wasted fighting pointless fights
- Sometimes there are major issues, no need to make things worse for customers →
- One size does not fit all, Spectre/Meltdown →
- Prioritization should be based on real risk to customers

February 2017 security update release

Rate this article ★★★★



MSRC Team February 14, 2017

Share 302

933

0

0

UPDATE: 2/15/17: We will deliver updates as part of the planned March Update Tuesday, March 14, 2017.

Our top priority is to provide the best possible experience for customers in maintaining and protecting their systems. This month, we discovered a last minute issue that could impact some customers and was not resolved in time for our planned updates today.

After considering all options, we made the decision to delay this month's updates. We apologize for any inconvenience caused by this change to the existing plan.

MSRC

The Register®
Biting the hand that feeds IT



Security

Mad March Meltdown! Microsoft's patch for a patch for a patch may need another patch

If at first, er, second, ah, third, no, fourth, you fail, sadly, you're probably Redmond

By Shaun Nichols in San Francisco 3 Apr 2018 at 19:05 53 □ SHARE ▼

Release of Exploits/PoCs

- Release of vulnerability 'Proof of Concepts' and exploits can be very damaging, WannaCry:
 - 150+ countries, 200,000+ computers impacted
 - \$10+ million in ransom, \$8+ billion in business disruption costs
- Customers needlessly punished
- WannaCry, NotPetya & Exploit Kits highlight 'even today' customers for various reasons sometimes **don't update**
- Internal 2016 review highlighted PoCs making their way to Exploit Kits (Angler, Nuclear) between 10 and 40 days after update available
 - Many Adobe Flash vulns in Exploit Kits were only integrated after POC was released
- Collisions are rare, no SMB case in 2016...
- Deter release of PoC for as long as possible

NEWS

[Home](#) | [UK](#) | [World](#) | [Business](#) | [Politics](#) | [Tech](#) | [Science](#) | [Health](#) | [Family & Education](#)

Technology

NHS 'could have prevented' WannaCry ransomware attack

© 27 October 2017 |



Analysis - by Rory Cellan-Jones, technology correspondent

For many executives, a serious cyber-attack is now very high on their list of risks to their organisations and a priority for disaster planning.

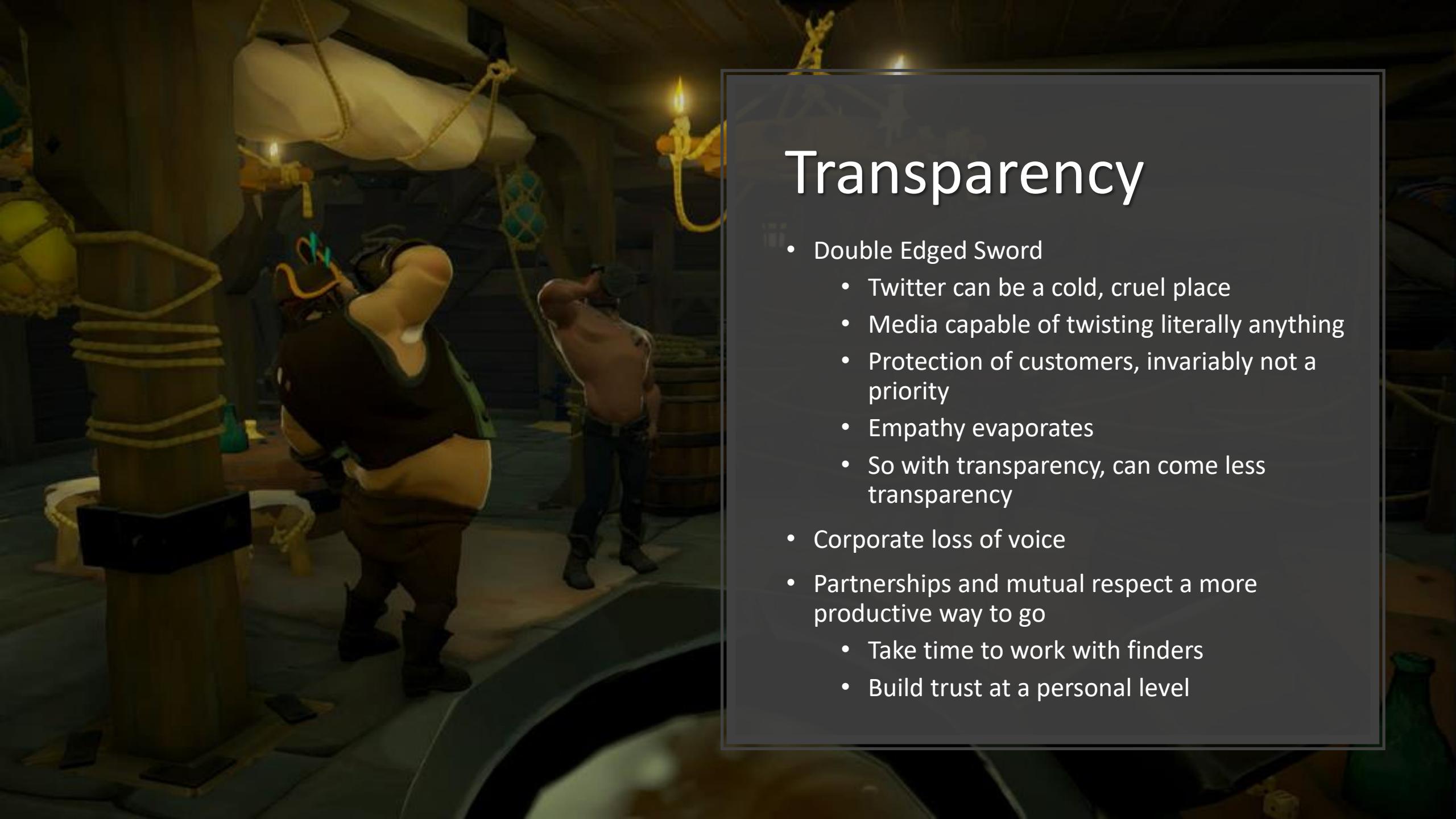
So what is most shocking in this report is the lack of planning at a local level in the NHS for such an event.

To be fair, the Department of Health had developed a plan - it was just that it had not been properly communicated or tested in the NHS trusts. When disaster struck, nobody seemed to know who was in charge or what to do.

Of course, all of this could have been avoided if security patches had been applied to protect the Windows 7 systems common throughout the NHS. Once again, there had been warnings sent out by NHS Digital, but many trusts failed to act upon them - though in that they were no different from many organisations around the world that were also hit.

Boeing hit by WannaCry virus, but says attack caused little damage

Originally published March 28, 2018 at 3:16 pm | Updated March 28, 2018 at 9:16 pm



Transparency

- Double Edged Sword
 - Twitter can be a cold, cruel place
 - Media capable of twisting literally anything
 - Protection of customers, invariably not a priority
 - Empathy evaporates
 - So with transparency, can come less transparency
- Corporate loss of voice
- Partnerships and mutual respect a more productive way to go
 - Take time to work with finders
 - Build trust at a personal level

10 Years, what's changed?

- VR and exploit creation is expensive
 - Exploit in Windows fetches \$300,000
- The small pool of external security researchers are now spread amongst many platforms, looking at an increasingly harder problem
- The industry needs finders, but ROI and trust is low →
- Moved from finding bugs to removing bug classes
- An increasing percentage of finders are expecting fixes at the speed of Twitter, but speed of update is almost irrelevant due to lack of collisions

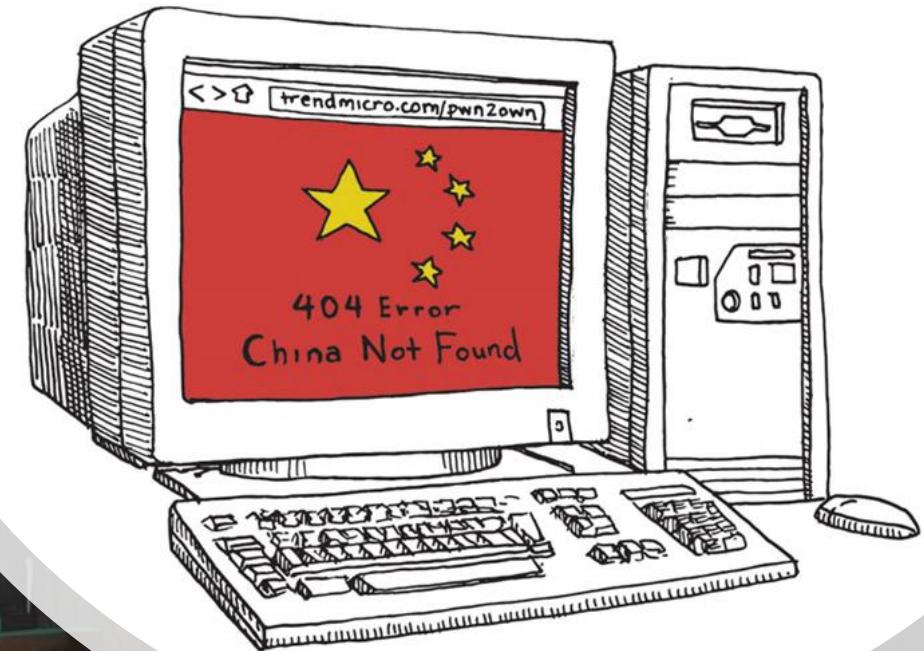
China hoards its hackers Everyone loses

country is MIA at one of the year's most important security competitions.



Violet Blue, @violetblue
03.16.18 in Security

1079
Shares

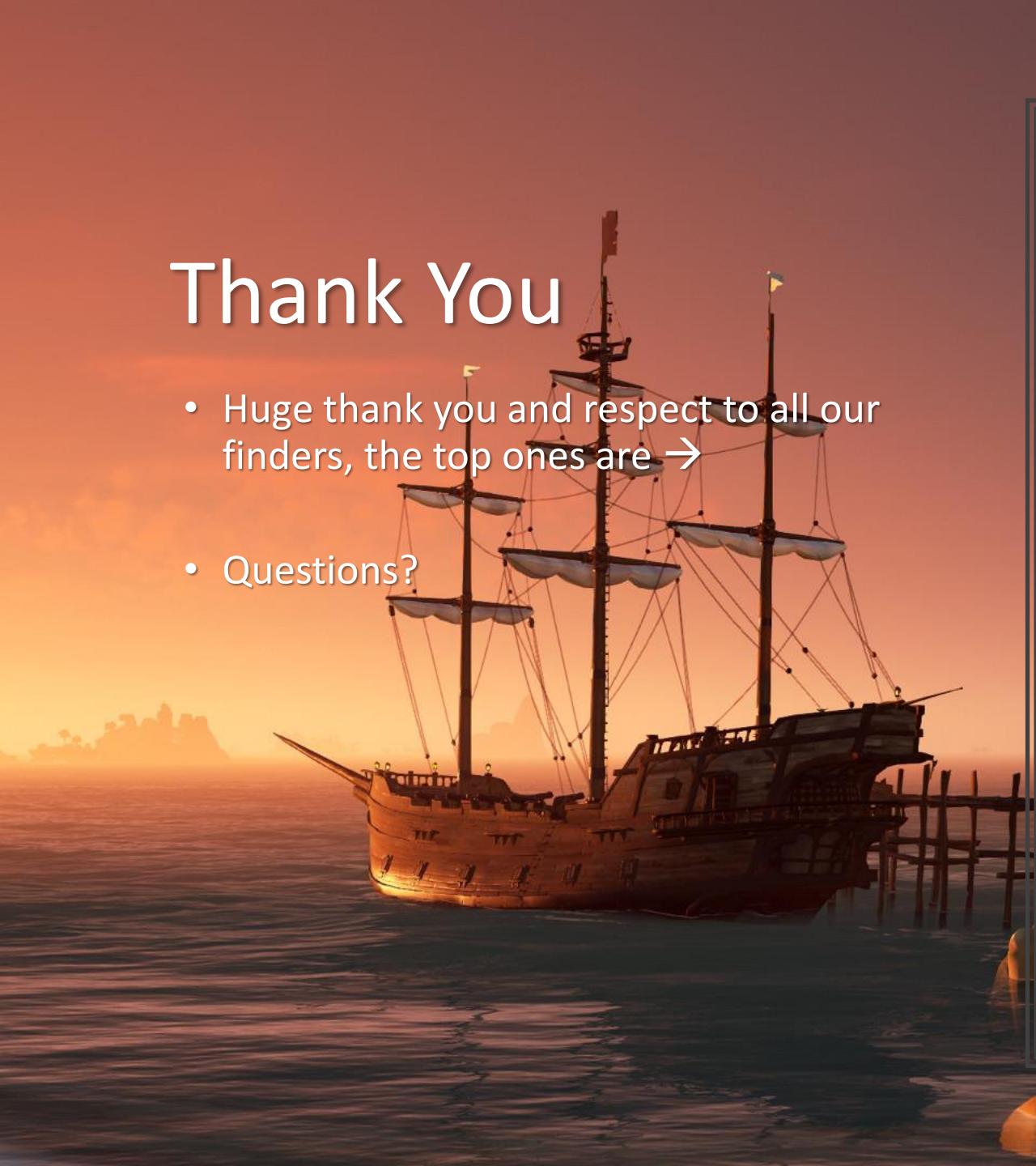


Where are we going?

- More focus:
 - Protecting Cloud and AI Services
 - Validating the Supply Chain
 - Validating Open Source
 - Removing memory corruption vulns OAFA
 - Is Rust the answer?
- More vulns, not fewer ☺
- Greater automation to handle those vulns

Thank You

- Huge thank you and respect to all our finders, the top ones are →
- Questions?



ABDEL HAFID AIT CHIKH
ADRIAN IVASCU
AJAY KULAL
ALEX IONESCU
ANATOLII BENCH
ANDREAS SANDBLAD
ANDY DAVIS
ANTON IVANOV
ARUN SHARMA
ASHAR JAVED
ATTE KETTUNEN
BEE13OY
BEN HAWKES
BEREND-JAN WEVER
BILLY LEONARD
BO QU
CAMERON DAWE
CAMERON VINCENT
CDSRC2016
CHENDONG LI
CHRIS EVANS
COSTIN RAIU
DAN CASELDEN
DHANESH KIZHAKKINAN
FORTINET TECHNOLOGIES
GENWEI JIANG
HAIFEI LI
HAMZA BETTACHE
HEIGE
HENRY LI
HUI GAO
ILJA VAN SPRUNDEL
IVAN FRATIC
JOOSEAN
JAANUS KÄÄP
JACK TANG
JACK WHITTON
JAEHUN JEONG
JAFAR HASAN
JAMES FORSHAW
JIN CHEN
JUN KOKATSU
JUNGHOON LEE
KAI KANG
KAI SONG
KARIM VALIEV
LI KEMENG
LINAN HAO
LIU LONG
LONG (DANIEL) JIN
LUCAS LEONG
LUCIANO CORSALINI
MANDEEP JADON
MARCIN TOWALSKI
MARIO HEIDERICH
MARTIN BARBELLA
MASATO KINUGAWA
MATEUSZ JURCZYK
MICHAEL BOLSHOV
MORITZ JODEIT
MYEONGGIL CHOI
NATALIE SILVANOVICH
NICOLAS DOLGIN
NICOLAS GREGOIRE
NOAM RATHAUS
PAVEL AVGUSTINOV
PETER ALLOR
PETER HLAVATY
PFLASH PUNK
QIUPENG
QIXUN ZHAO
REGINA WILSON
RICHARD SHUPAK
RICHARD WARREN
RODOLFO GODALLE, JR.
RYAN HANSON
SAURABH PUNDIR
SCOTT BELL
SEBASTIEN MORIN
SHAHMEER AMIR
SHEFANG ZHONG
SHI JI
STEFAN KANTHAK
STEVEN SEELEY
STEVEN VITTITOE
SUMCOGITO
TAO YAN
TAVIS ORMANDY
TIGONLAB
TONGBO LUO
WENXIANG QIAN
WINSON LIU
XIAOCAO FAN
YANGKANG (@DN PUSHME)
YORICK KOSTER
YU YANG
YUKI CHEN
ZHENG HUANG
ZHENGWEN BIN

Screenshots/Artwork
From Sea of Thieves by Microsoft / Rare



Sea of Thieves®

