ATTACK THE NEWS CYCLE

Before it Attacks You

Jerry Bryant
Director of Communications
Intel Product Assurance and Security
@jnabryant

Intro to Security Communications

> *“Security communications is the art of being the master of your own domain.”*

Intro to Security Communications

"If you don't have full contextual knowledge of a vulnerability, your communications efforts are already dead in the water"

Intro to Security Communications

GET TO CONFIDENT!

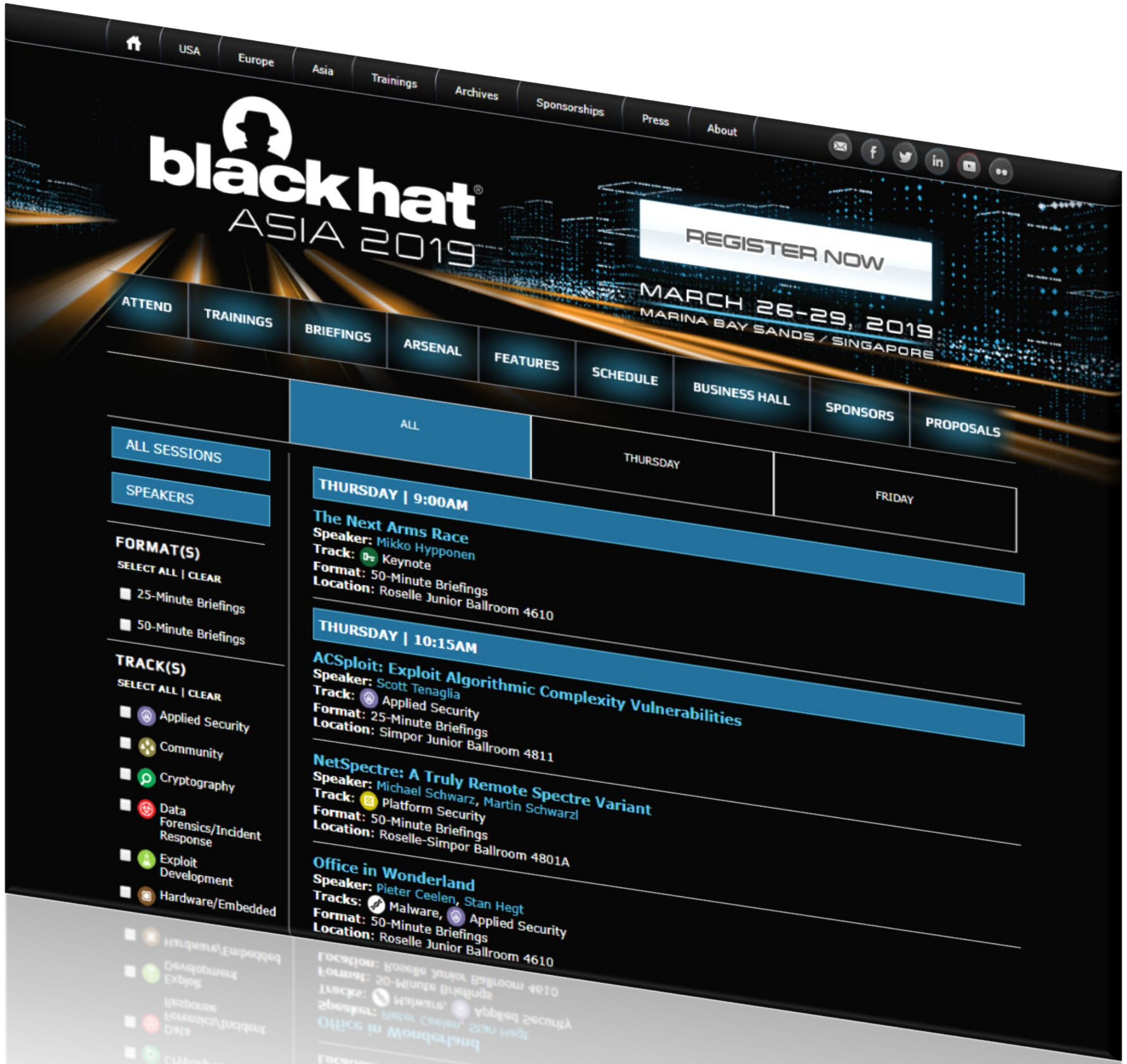
Triggers for Action

Triggers for Action

- **Branded vulnerability**

Triggers for Action

- Branded vulnerability
- **Conference talk planned**



FORMAT(S)
SELECT ALL | CLEAR

□ 25-Minute Briefings
□ 50-Minute Briefings

TRACK(S)
SELECT ALL | CLEAR

□ Applied Security
□ Community
□ Cryptography
□ Data Forensics/Incident Response
□ Exploit Development
□ Hardware/Embedded

THURSDAY | 9:00AM

The Next Arms Race
Speaker: Mikko Hypponen
Track: Keynote
Format: 50-Minute Briefings
Location: Roselle Junior Ballroom 4610

THURSDAY | 10:15AM

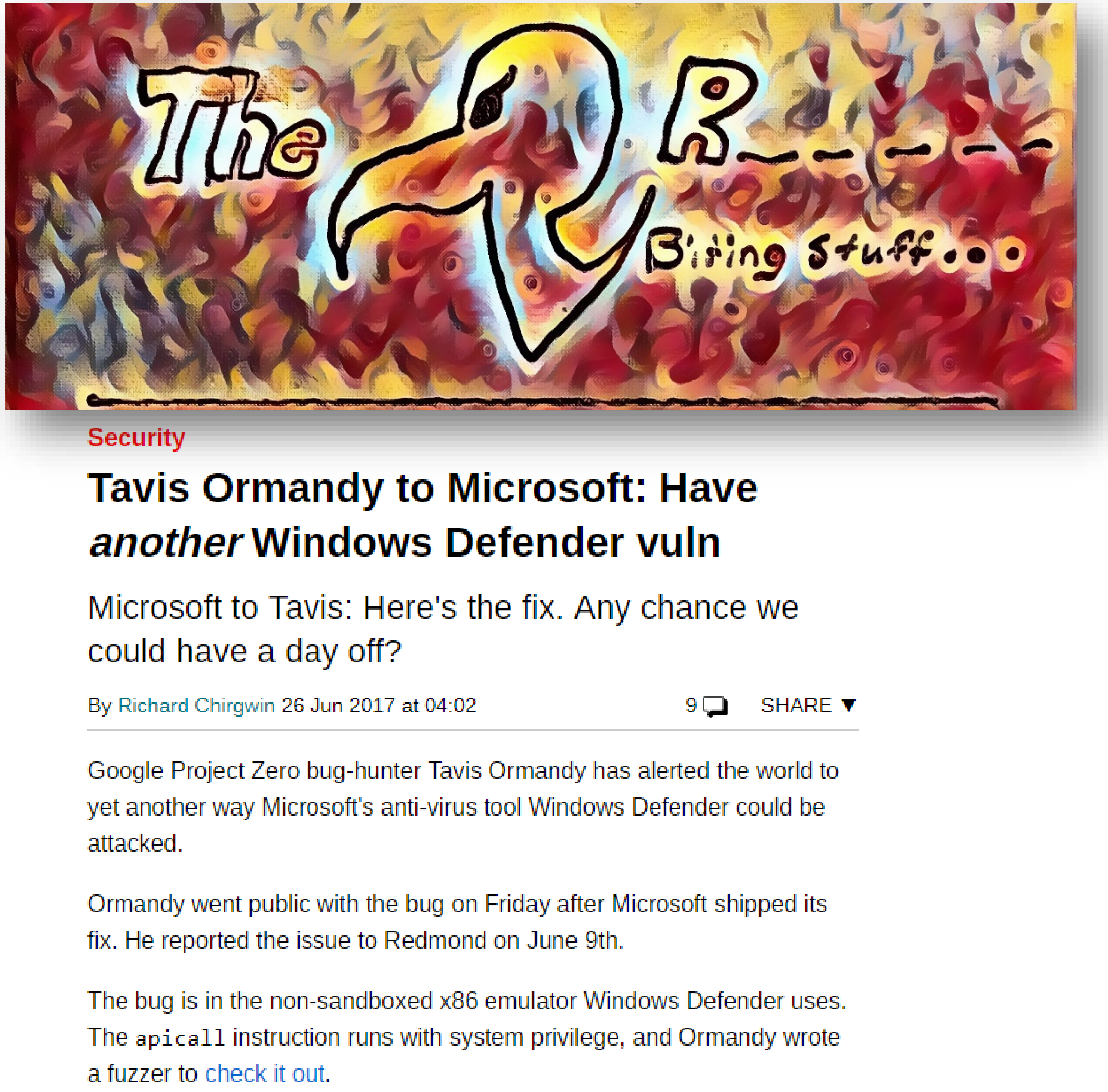
ACSploit: Exploit Algorithmic Complexity Vulnerabilities
Speaker: Scott Tenaglia
Track: Applied Security
Format: 25-Minute Briefings
Location: Simpor Junior Ballroom 4811

NetSpectre: A Truly Remote Spectre Variant
Speaker: Michael Schwarz, Martin Schwarzl
Track: Platform Security
Format: 50-Minute Briefings
Location: Roselle-Simpor Ballroom 4801A

Office in Wonderland
Speaker: Pieter Ceelen, Stan Hegt
Tracks: Malware, Applied Security
Format: 50-Minute Briefings
Location: Roselle Junior Ballroom 4610

Triggers for Action

- Branded vulnerability
- Conference talk planned
- **Researchers generated media before**



Security

Tavis Ormandy to Microsoft: Have *another* Windows Defender vuln

Microsoft to Tavis: Here's the fix. Any chance we could have a day off?

By Richard Chirgwin 26 Jun 2017 at 04:02 9 SHARE ▼

Google Project Zero bug-hunter Tavis Ormandy has alerted the world to yet another way Microsoft's anti-virus tool Windows Defender could be attacked.

Ormandy went public with the bug on Friday after Microsoft shipped its fix. He reported the issue to Redmond on June 9th.

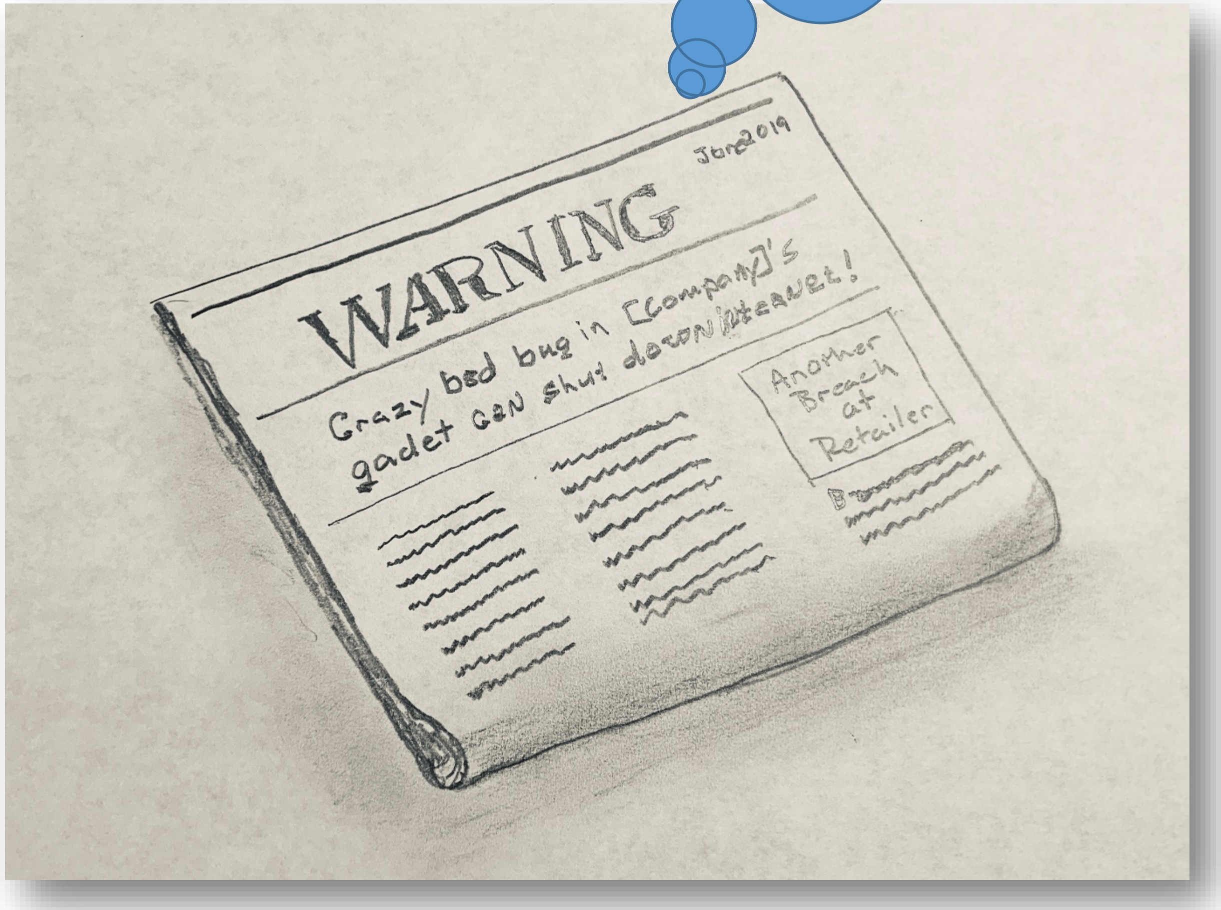
The bug is in the non-sandboxed x86 emulator Windows Defender uses. The `apicall` instruction runs with system privilege, and Ormandy wrote a fuzzer to check it out.

@jnabryant

Triggers for Action

- Branded vulnerability
- Conference talk planned
- Researchers generated media before
- **Can be perceived as worse than it is/complex attack scenario**

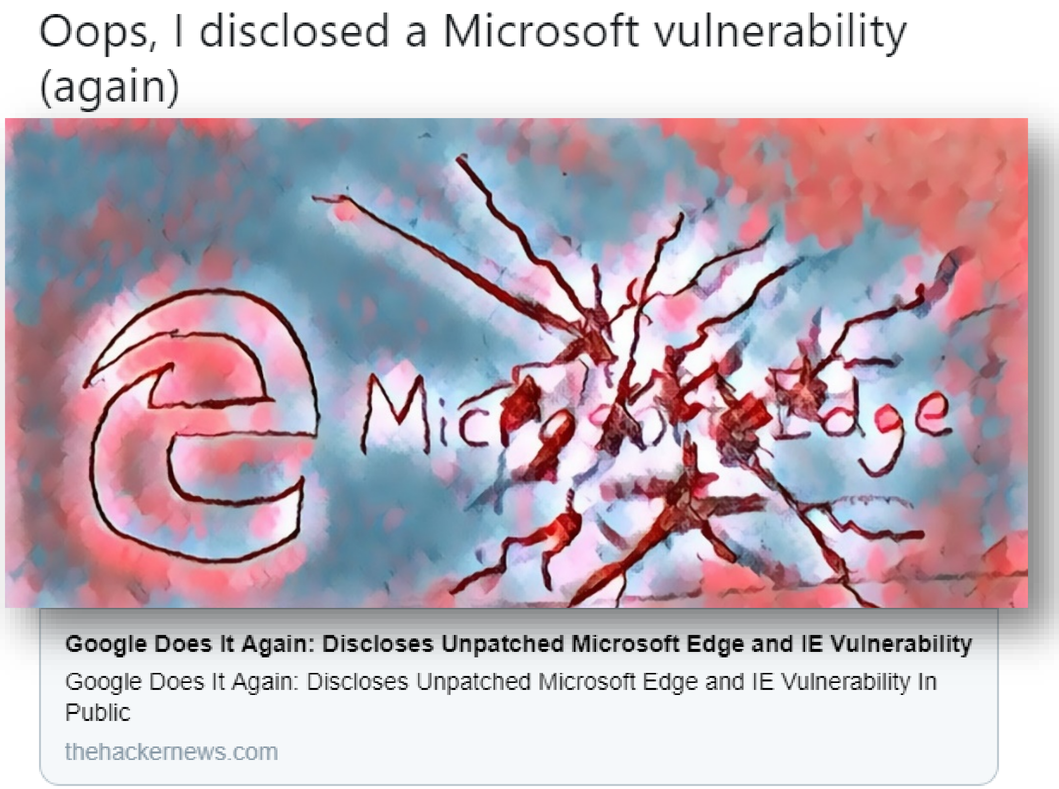
But wait… you need physical access AND admin on the target!


June 2019
WARNING
Crazy bad bug in [Company]'s gadget can shut down internet!
Another Breach at Retailer

@jnabryant

Triggers for Action

- Branded vulnerability
- Conference talk planned
- Researchers generated media before
- Seems worse than it is/complex attack scenario
- **Early disclosure**



Oops, I disclosed a Microsoft vulnerability (again)

Google Does It Again: Discloses Unpatched Microsoft Edge and IE Vulnerability

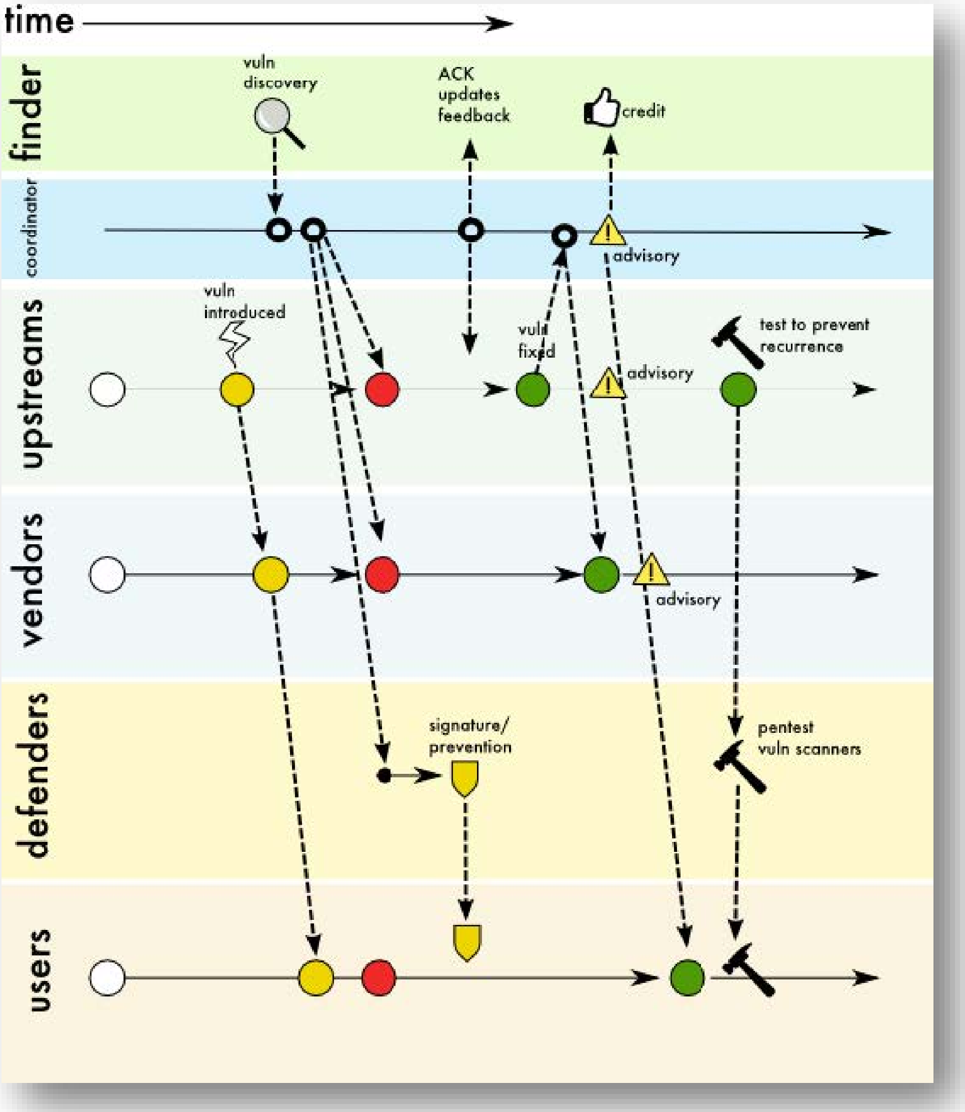
Google Does It Again: Discloses Unpatched Microsoft Edge and IE Vulnerability In Public

thehackernews.com

@jnabryant

Triggers for Action

- Branded vulnerability
- Conference talk planned
- Researchers generated media before
- Seems worse than it is/complex attack scenario
- Early disclosure
- **Multiple products/parties affected**



@jnabryant

Triggers for Action

- Branded vulnerability
- Conference talk planned
- Researchers generated media before
- Seems worse than it is/complex attack scenario
- Early disclosure
- Multiple products/parties affected
- **High severity/easily exploited**

STRATEGIES AND TACTICS

Strategies and Tactics

- **Be the authoritative voice from the beginning**

- Establish triggers (some general, some will be case by case)
- If you hit a trigger, execute your plan (sometimes you have to anticipate the trigger will occur)
- Look for anomalies and adjust
- Breaking into jail is always a risk

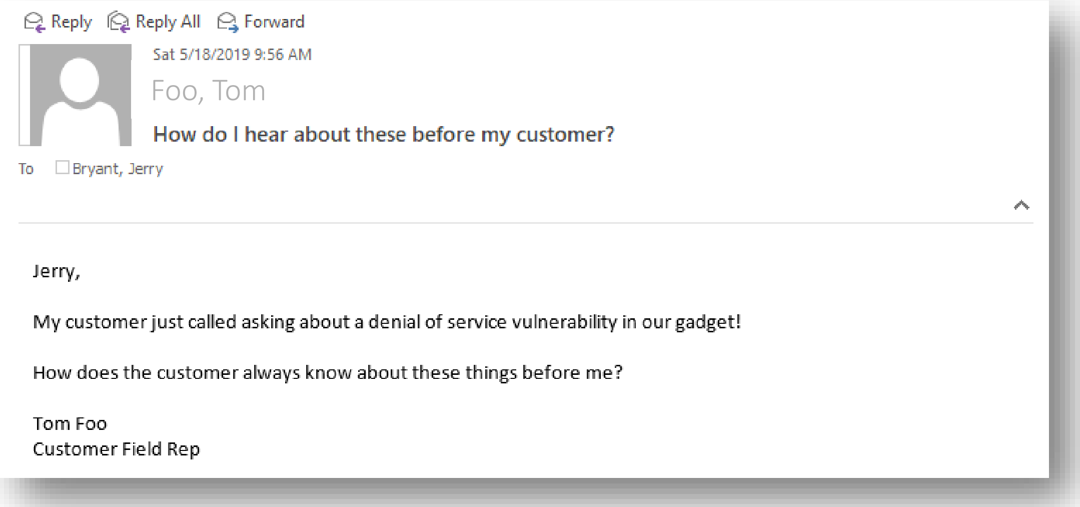
Strategies and Tactics

- Be the authoritative voice from the beginning
- **Burn all the fuel before it starts a fire**

@jnabryant

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- **Arm all the people**



Sat 5/18/2019 9:56 AM

Foo, Tom

How do I hear about these before my customer?

To □Bryant, Jerry

Jerry,

My customer just called asking about a denial of service vulnerability in our gadget!

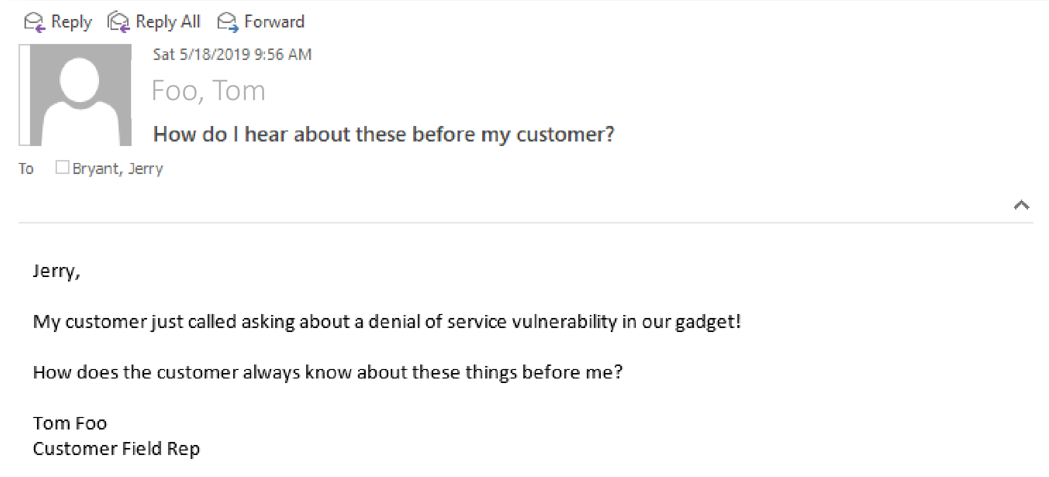
How does the customer always know about these things before me?

Tom Foo
Customer Field Rep

Note: Tom Foo is a fictional character ;-)

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- **Arm all the people**



Sat 5/18/2019 9:56 AM

Foo, Tom

How do I hear about these before my customer?

To □Bryant, Jerry

Jerry,

My customer just called asking about a denial of service vulnerability in our gadget!

How does the customer always know about these things before me?

Tom Foo
Customer Field Rep

Proactively provide info for:

- Customer support centers (Q&A)
- Field reps
  - Establish internal distribution
  - Training
  - Regional response coordinators
- Executives

Note: Tom Foo is a fictional character ;-)

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- Arm all the people
- **Make the most out of public statements**

- Don’t repeat the problem
- Short and to the point
- Authoritative
- Personalize it (if possible)

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- Arm all the people
- **Make the most out of public statements**

- Don’t repeat the problem
- Short and to the point
- Authoritative
- Personalize it (if possible)

Not so Good	*“[Company name] is aware of the Denial of Service vulnerability in our gadget and we have issued an update to address it. We take all security issues seriously and work quickly to evaluate and mitigate them.” – Company Spokesperson*

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- Arm all the people
- **Make the most out of public statements**

- Don’t repeat the problem
- Short and to the point
- Authoritative
- Personalize it (if possible)

Not so Good	*“[Company name] is aware of the Denial of Service vulnerability in our gadget and we have issued an update to address it. We take all security issues seriously and work quickly to evaluate and mitigate them.” – Company Spokesperson*
Much Better	*“The vulnerability has been mitigated in Security Advisory 2019-0001. Customers who apply the update are not at risk.” – Jerry Bryant, Director of Security Communications*

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- Arm all the people
- Make the most out of public statements
- **Influence the influencer**

- Pay attention to people media like to quote frequently
- Begin reaching out to them just prior to announcing something or publishing advisories
- Have a technical conversation with them
- Help them understand how you think about the "issue"

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- Arm all the people
- Make the most out of public statements
- Influence the influencer
- **Media Engagement**

Build relationships BEFORE the crisis

- If you release advisories on a set schedule, that's an opportunity
- Schedule F2F meetings at conferences
- Have proactive security news? Brief the media
- May still write a negative story but at least they are educated on your capabilities

Strategies and Tactics

- Be the authoritative voice from the beginning
- Burn all the fuel before it starts a fire
- Arm all the people
- Make the most out of public statements
- Influence the influencer
- Media Engagement
- **Alert the CERT**

Multidimensional content

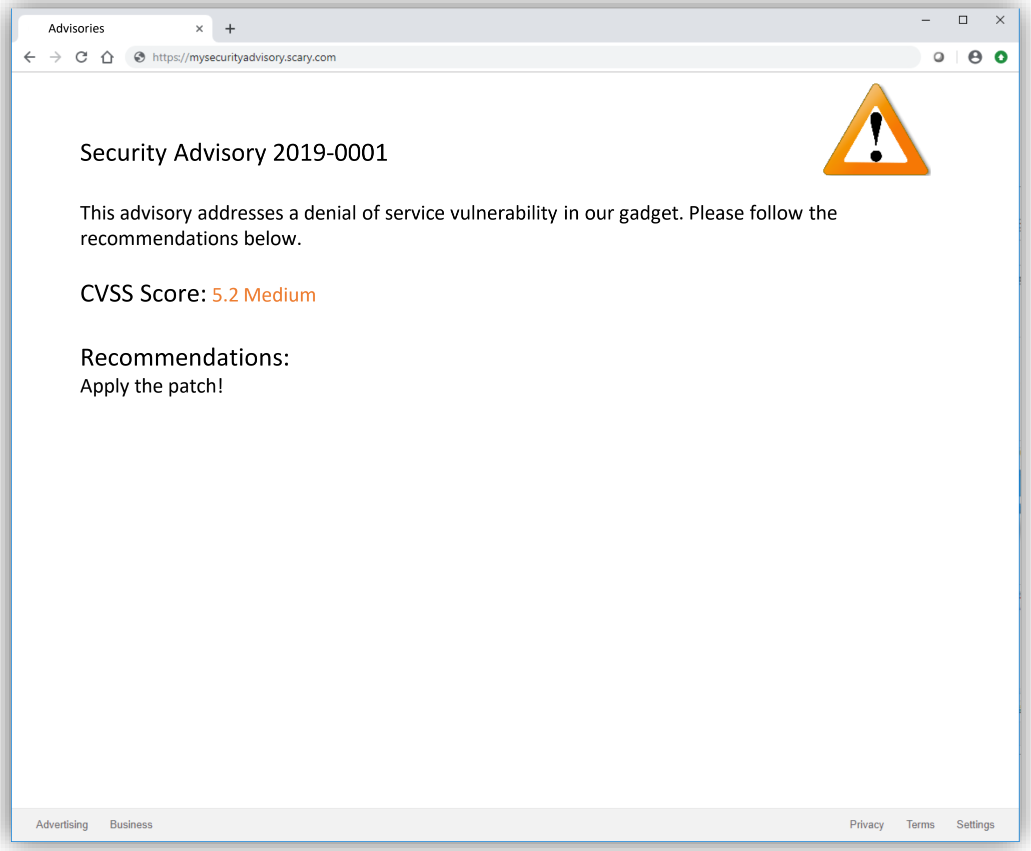
Align All Your External Content

Ensure all of your external content aligns to tell your security story and demonstrate your capabilities to respond

Your Security Website

- Ensure it tells your whole product security story
- Not for product marketing
- Should demonstrate the investment made in security response
  - PSIRT team
  - Specialized engineering skills (your folks know how to hack)
- Give customers confidence in your capability

Bulletins and Advisories – Serve a Purpose



Security Advisory 2019-0001

This advisory addresses a denial of service vulnerability in our gadget. Please follow the recommendations below.

CVSS Score: 5.2 Medium

Recommendations:
Apply the patch!

- They don't tell the whole story
- Focus is on issue description, affected products, severity, and actions customers should take to mitigate
- Institutional language can be scary
- They don't always provide enough context for prioritization

@jnabryant

Blogs and Social Media

- Build your incident response presence on Twitter
  - Spread the message far and wide
- Use your blog to
  - Have THE authoritative place for your security response topics
  - Help customers/media understand how to prioritize your security updates
  - Show your deep technical capabilities by providing your own analysis of the more critical issues

The transition

Transition to Good News

- You might not be in the spotlight today…
- Every organization’s path might be different
- Study your situation and develop a strategy
- You can’t build this from the bottom up
- Expect a multi-year effort
- Success is measured by
    - Normalization of security issues (become business as usual)
    - Customer confidence in your capability to manage issues and incidents
    - A more positive tone in social and media references

Transition to Good News

"We make awful news just bad."

- Christopher Budd -

Transition to Good News

“We make bad news good.”

- Jerry Bryant -

Questions?