RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Mutiny on the Bounty: The Epic Tale of How Data Defeated Dogma

SESSION ID: STR-R02

Katie Moussouris

Senior Security Strategist
Microsoft Security Response Center

http://twitter.com/**k8em0** <-- that's a zero

Agenda

Setting the Stage

The World As We Knew It – Bounties Were Heresy

Laying the Foundation – Baseline Data and Forming Predictions

The Vulnerability Economy – Viewed by Intent

Intentional Market Disruption - Microsoft's Strategic Bounty Programs

Digging in the Data – Hypotheses Proven

Heresy Turned to Gospel – Singing from the Data Hymnal

How to Structure Your Own Bounty Programs

Who I am

Joined Microsoft in April 2007

Mother of Microsoft's **Bounty Programs, Internet Bug Bounty Panelist**

Chair of **BlueHat** Content Board

My (security*) work in bullet points:

- Linux Dev and Security Tzarina - TurboLinux, circa 2000
- Pen Tester - Artist formerly known as @stake
- Founder - Symantec Vulnerability Research (SVR)
- Founder - Microsoft Vulnerability Research (MSVR)
- Policy Maker
  - Editor for draft ISO standard on **Vulnerability Handling (30111)**
  - Lead SME for US National Body on **Vulnerability Disclosure (29147)**
  - Lead editor for Penetration Testing as it applies to Common Criteria **(20004-2**)and Secure Application Development processes **(27034-3)**

* Was a molecular biologist in a past professional life; worked on the Human Genome Project

Call Me Trimtab

"Something hit me very hard once, thinking about what one little man could do. Think of the Queen Mary—the whole ship goes by and then comes the rudder. And there's a tiny thing at the edge of the rudder called a trim tab. It's a miniature rudder. Just moving the little trim tab builds a low pressure that pulls the rudder around. Takes almost no effort at all. **So I said that the little individual can be a trim tab.** Society thinks it's going right by you, that it's left you altogether. But if you're doing dynamic things mentally, the fact is that **you can just put your foot out like that and the whole big ship of state is going to go**. So I said, **call me Trim Tab**." —Buckminster Fuller (1972)

Impossible Supertasks

Zeno's argument takes the following form:

- Motion is a supertask, because the completion of motion over any set distance involves an infinite number of steps
- Supertasks are impossible
- Therefore motion is impossible

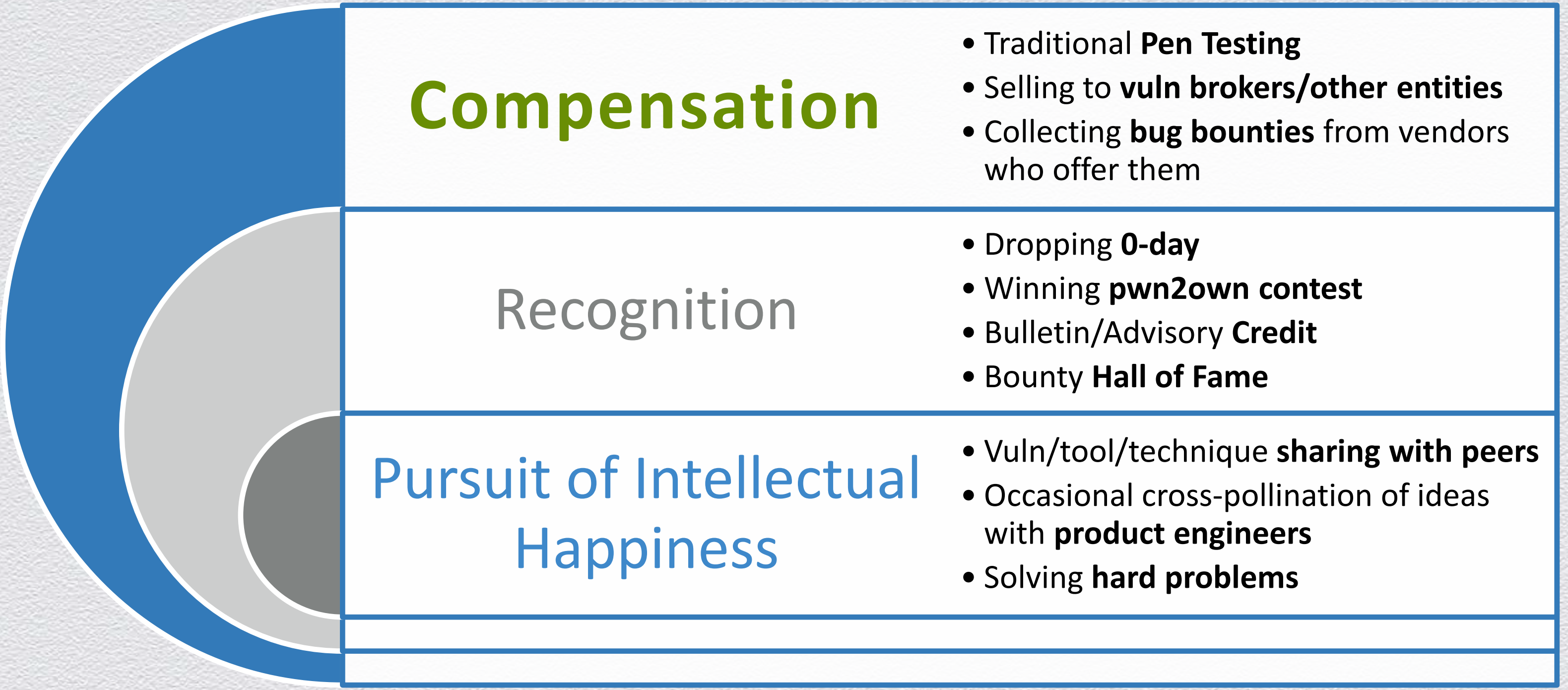
Don’t Dream It – Be It

- “Microsoft will never pay for bugs.”
- “You’ll never be able to compete with/outbid the Black Market.”
- “You’ll never be able to buy the most serious bugs.”

Data: Vulnerability Reporting Trends

- In 2010, over 90% of all bulletin-class vulnerabilities were reported directly for free.
- Not all products are created equal
- The case was made: When vulnerability reporting starts trending towards brokers instead of direct to us, we will start paying
- Now we wait…

Security Researcher Motivations/Fulfillment



Compensation

- Traditional **Pen Testing**
- Selling to **vuln brokers/other entities**
- Collecting **bug bounties** from vendors who offer them

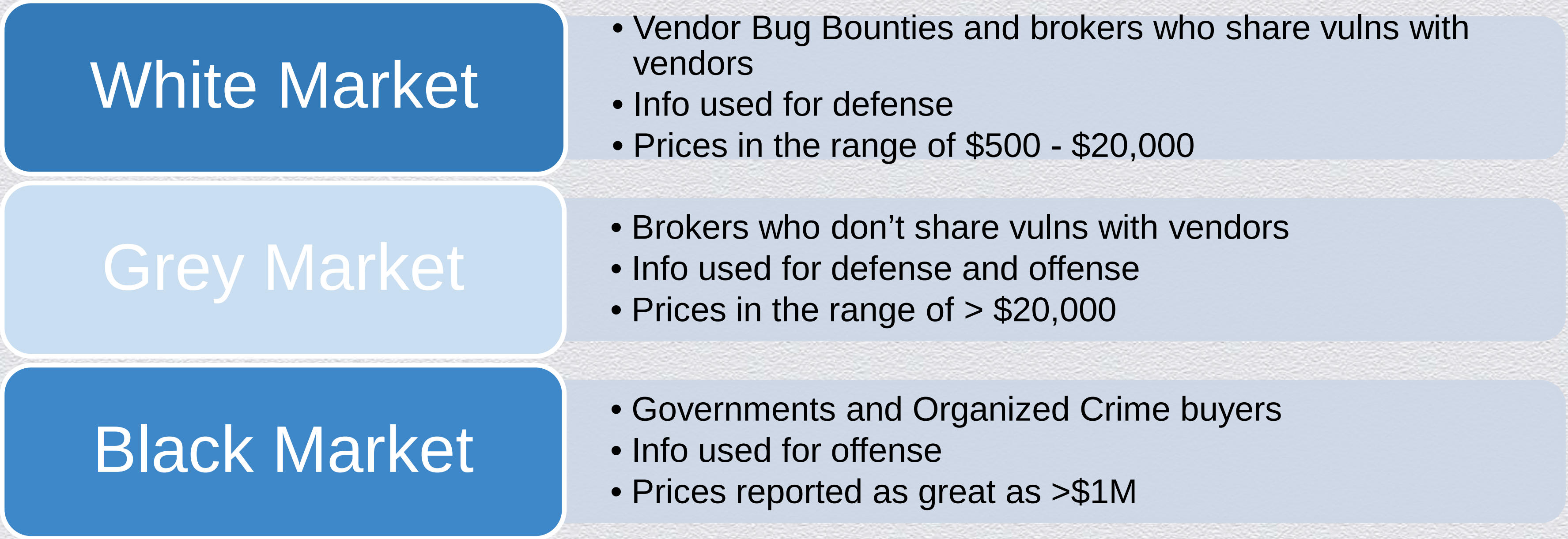
Recognition

- Dropping **0-day**
- Winning **pwn2own contest**
- Bulletin/Advisory **Credit**
- Bounty **Hall of Fame**

Pursuit of Intellectual Happiness

- Vuln/tool/technique **sharing with peers**
- Occasional cross-pollination of ideas with **product engineers**
- Solving **hard problems**

The Vulnerability Economy



White Market

- Vendor Bug Bounties and brokers who share vulns with vendors
- Info used for defense
- Prices in the range of $500 - $20,000

Grey Market

- Brokers who don’t share vulns with vendors
- Info used for defense and offense
- Prices in the range of > $20,000

Black Market

- Governments and Organized Crime buyers
- Info used for offense
- Prices reported as great as >$1M

The White Market Usually Does Not Compete Directly With Other Markets

The Price Increases Depending on the Vulnerability’s Intended Use

Impossible SuperTask Accomplished: June 19, 2013

Microsoft announced the launch of multiple incentive (bounty) programs for both previously unknown vulnerabilities and for techniques that improve defenses against exploits.

Goooooaaaalllllssss!!!!

- Security Goals
  - Learn about residual vulnerabilities and new mitigation bypass techniques as early as possible after release
- Community Goals
  - Engage with new researchers and harness their beautiful minds aligned with our engineering timelines
- Vulnerability Market Disruption Goals
  - Create attractive year-round compensation for researchers who generally sell to the white market
  - Provide a monetary outlet for defensive research
  - Shorten the expected usefulness of vulnerabilities and exploits purchased on the Black Market

Microsoft's Bounty Programs

Over $253,000 PAID

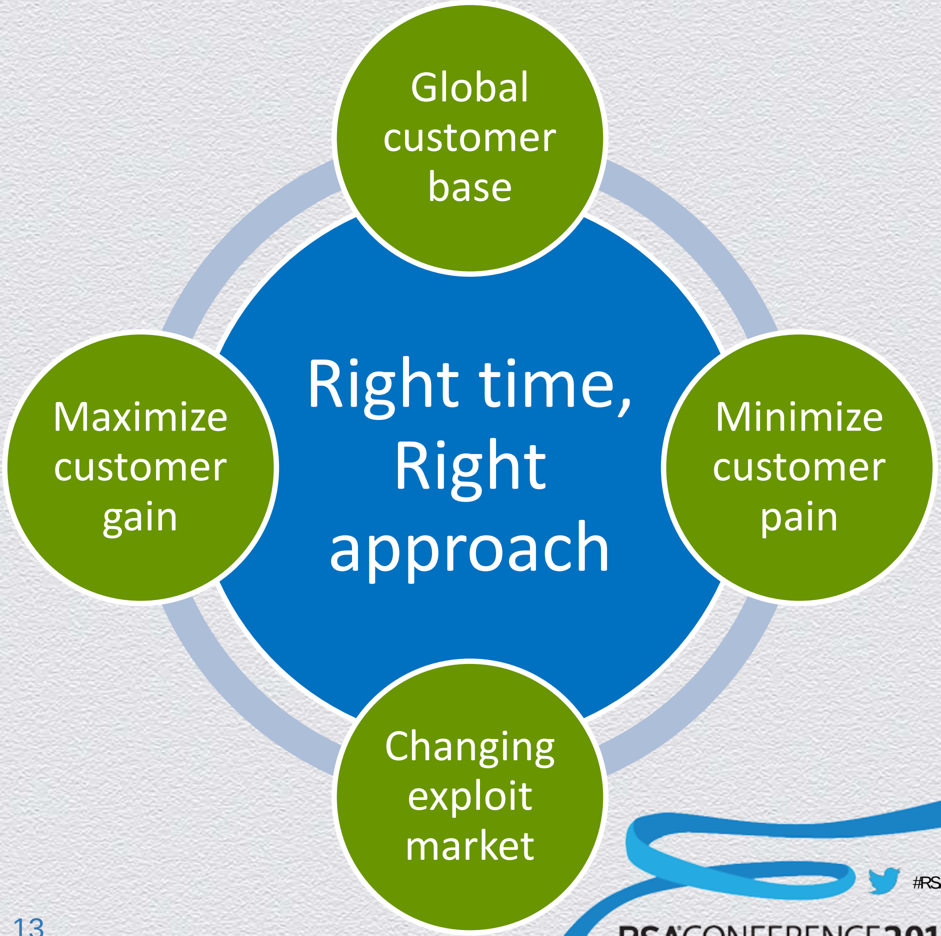
Strategic Impact

Why Bounty?

Bounties are not one size fits all

Finding the right approach for customers

Creating a win-win for hackers & you



Right time, Right approach

Global customer base

Minimize customer pain

Changing exploit market

Maximize customer gain

Microsoft bounty programs

Mitigation Bypass Bounty

Microsoft will pay up to **$100,000 USD** for truly novel exploitation techniques against protections built into the latest version of our operating system (Windows 8.1 Preview)

BlueHat Bonus for Defense

Microsoft will pay up to **$50,000 USD** for defensive ideas that accompany a qualifying Mitigation Bypass bounty submission

IE11 Preview Bug Bounty

Microsoft paid up to **$11,000 USD** for critical-class vulnerabilities that affect IE 11 Preview on the latest version of Windows (Windows 8.1 Preview), including bugs with privacy implications

Digging Through the Data - Hypotheses Proven

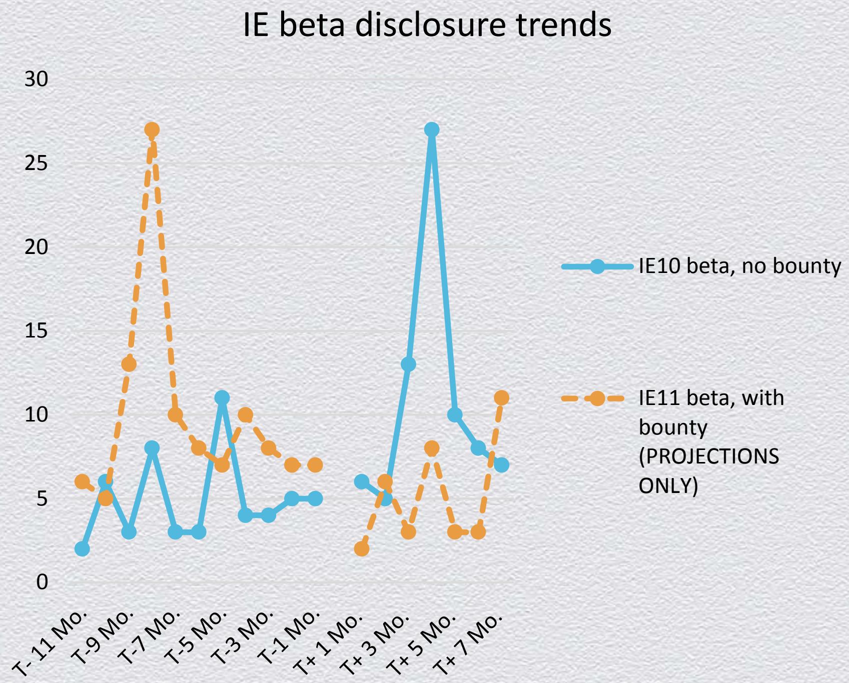
My histograms don’t lie

IE Preview Bug Bounty: All in the timing

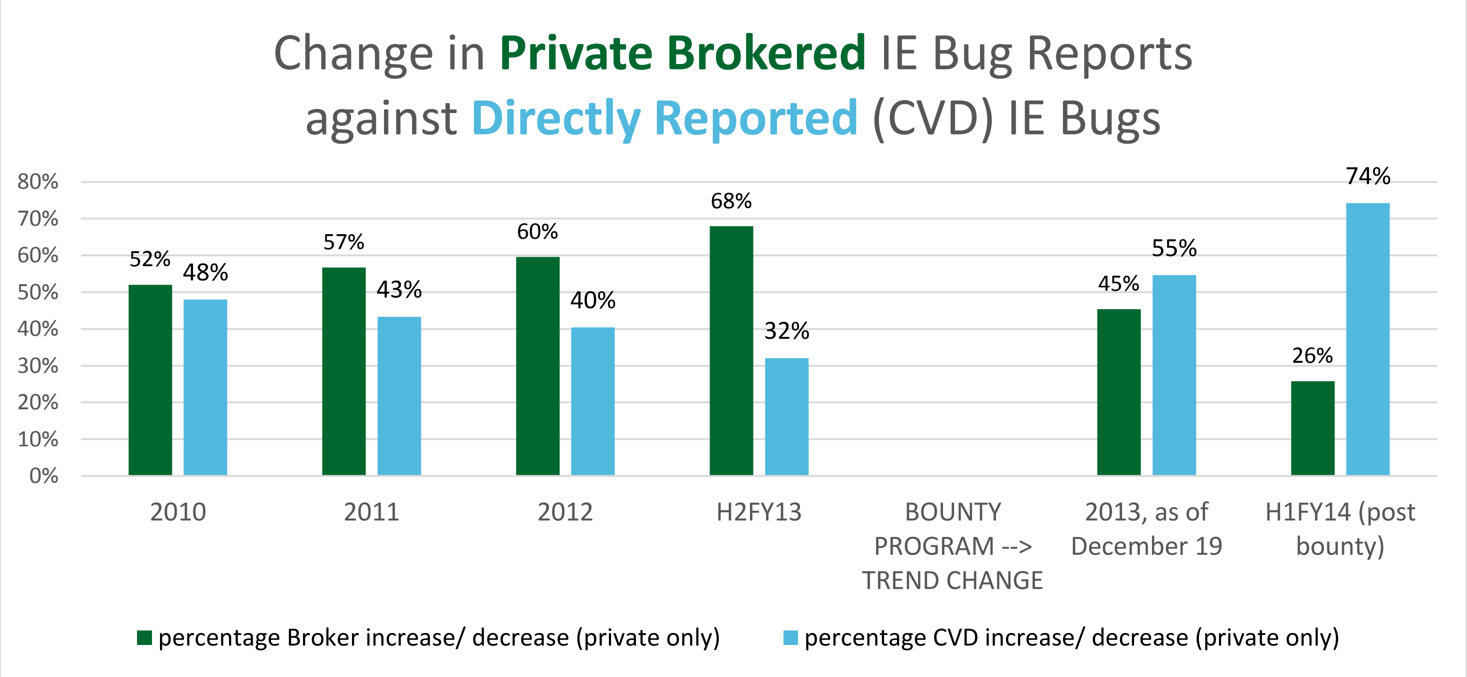
- Running a bounty program during the Preview (beta) period for IE11 affords us the opportunity to address the greatest number of issues with the least impact to our customers

  Vulnerability brokers don’t generally offer payment for OUR browser in beta, so we’re pleased to address that gap in the marketplace in this pilot program

- Results: 23 submissions, 18 bulletin-class issues – including 4 sandbox escapes

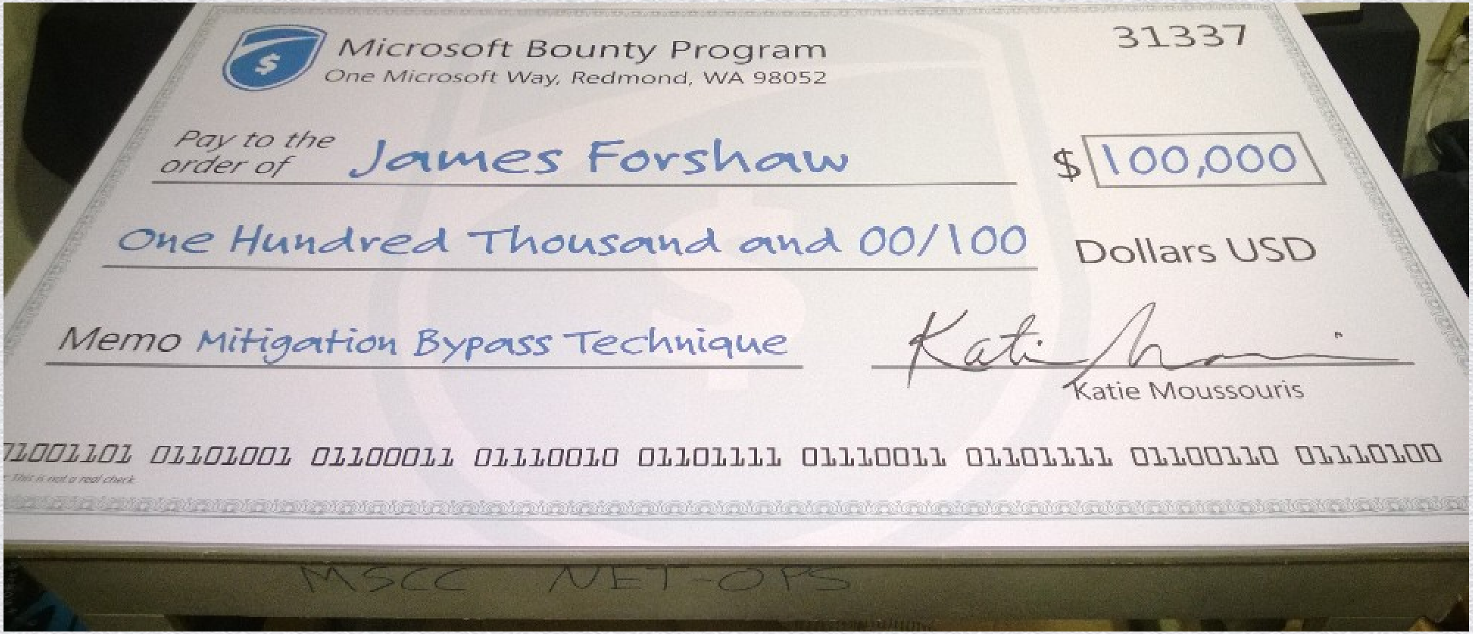


IE 11 Preview Bounty --> Reverses Reporting Trend



Change in **Private Brokered** IE Bug Reports against **Directly Reported** (CVD) IE Bugs

Mitigation Bypass Bounty: $100,000
James and the Giant Check Presented 12/12/13



Microsoft Bounty Program
One Microsoft Way, Redmond, WA 98052

31337

Pay to the order of James Forshaw

$ 100,000

One Hundred Thousand and 00/100 Dollars USD

Memo Mitigation Bypass Technique

Katie Moussouris

1001101 01101001 01100011 01110010 01101111 01110011 01101111 01100110 01110100

This is not a real check

Bounty Program Evolution

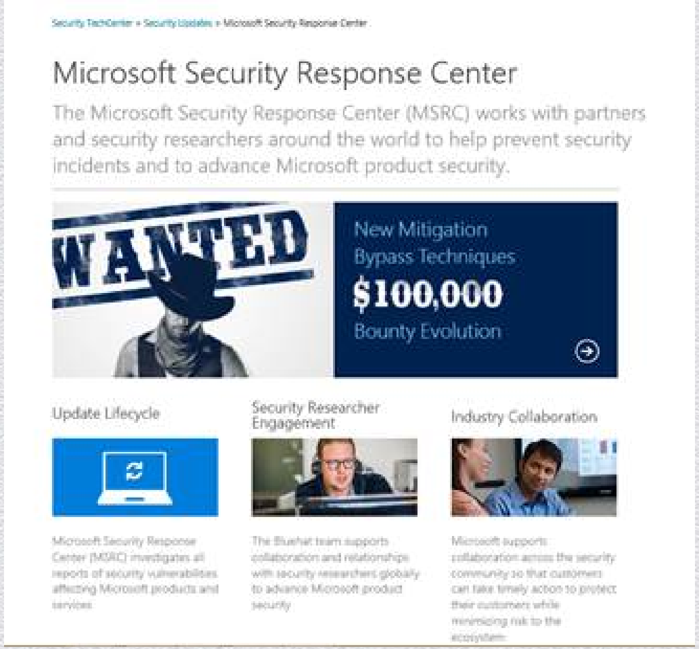
Mitigation Bypass Bounty – NOW OPEN TO ANYONE WHO TURNS IN A DISCOVERY FROM THE WILD

Helps us learn how to block new exploitation techniques and entire classes of attacks

Decreases time that a targeted attack will stay undetected

Undermines the investment of the black market – will those prices start to drop?

Stay tuned for further developments…



Security TechCenter » Security Updates » Microsoft Security Response Center

Microsoft Security Response Center

The Microsoft Security Response Center (MSRC) works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.

New Mitigation Bypass Techniques

$100,000

Bounty Evolution

Update Lifecycle

Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services.

Security Researcher Engagement

The BlueHat team supports collaboration and relationships with security researchers globally to advance Microsoft product security.

Industry Collaboration

Microsoft supports collaboration across the security community so that customers can take timely action to protect their customers while minimizing risk to the ecosystem.

Intentional Disruption of Existing Markets

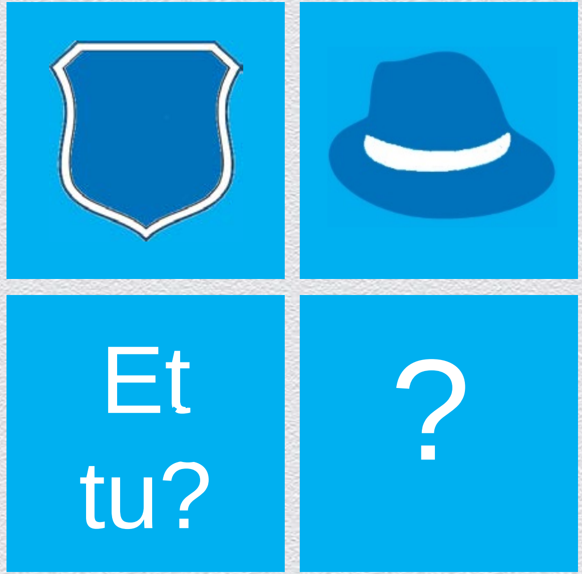
Microsoft Bounties are designed to change the dynamics and the economics of the current vulnerability market.

- **Market Gap Advantage:** Offering bounties for bugs when other buyers typically are not buying them (e.g. **during the preview/beta period**) helps get bugs before markets trade them.
- **Ongoing $100,000 Bounty:** Offering bounties year-round to learn about new techniques earlier helps us build defenses faster, **without waiting for a contest**.
- **Decreasing Time An Attack goes Undetected:** Offering large bounties for techniques that are being used in active attacks helps **devalue black market investments earlier**.

http://blogs.technet.com/b/bluehat/archive/2013/11/01/bounty-evolution-100-000-for-new-mitigation-bypass-techniques-wanted-dead-or-alive.aspx

Heresy No More – Data over Dogma

- Invest in Your SDL
  - Software security starts with the foundation of secure design and implementation
  - Develop tools and expertise to minimize the number of security issues that make it through
- Determine What Finders are Doing with YOUR Vulns
  - Do they report directly to you or via brokers? What is the TREND?
  - What is the reporting trend you can support with DATA?
- Structure Your Own Programs With Customers In Mind
  - Focus on catching bugs EARLIER, when they can be most easily addressed, before users are affected
  - Create WIN-WIN between the security research community and your customers
- Happy to help you navigate the new waters…



How to Structure Your Own Bounty Programs

Set Goals
Measure Trends
Study the Markets
Build Operational Capabilities

How to Structure Your Own Bounty Programs: Decide on the Outcome You Want

- Prioritize based on clear **goals** and play with your **variables**
- Evaluate the results and focus often
  - Protect largest group of **existing customer base**
    - Bounty products with the most market share
  - Make **newest products** more secure
    - Bounty products in the latest versions only
  - Learn about vulnerabilities **as early as possible** after release
    - Bounty during the beta period
  - **Disrupt the adversaries**
    - Bounty specialized targeted attack techniques

How to Structure Your Own Bounty Programs: Measure (at least) Twice

- Measure your reporting trends:
  - What are the **trends for different products** in terms of direct vs brokered reports?
  - Which products are most heavily **traded on the markets**? Are prices going up or down?
  - If none, focus on your SDL…and on getting more customers!
  - What are your bug count trends year over year?
    - Going up in number and severity – **Invest in your SDL**!
    - Going down in number, up in complexity – Congrats!

How to Structure Your Own Bounty Programs: Vulnerability Economy Research

- **Watch the Markets** for Your Vulnerabilities (White, Grey, Black)
  - Do the markets open before dawn (during the Beta period)?
  - **Identify gaps** you can fill with your own incentive programs
  - Identify where there is only a black market (no White or Grey)
  - Consider negotiating with the White and Grey Markets – **could you work together**?
- Watch how the Markets React to Your Bounties
  - What are the **pricing trends** after your bounties in White, Grey, Black markets?
  - Are some rising, with others falling?

Bounty Strategy Done? - Start Here With Ops

- Ensure a robust **vulnerability handling process (refer to ISO 30111**)
- Determine your realistic bug servicing capabilities and **augment resources** accordingly
- Consider **temporary or permanent outsourcing** of various components of the process
  - Bug Intake and Finder Relations
  - Technical Triage and Repro
  - Remediation Recommendation
  - Remediation creation, testing, release
- **Feedback into your SDL** what you learn, ideally in real time
- Adjust according to trends in your vulns, and your own shifting business priorities

Resources/Links

Microsoft Security Response Center
www.microsoft.com/msrc

Microsoft Bounty Programs
www.microsoft.com/bountyprograms

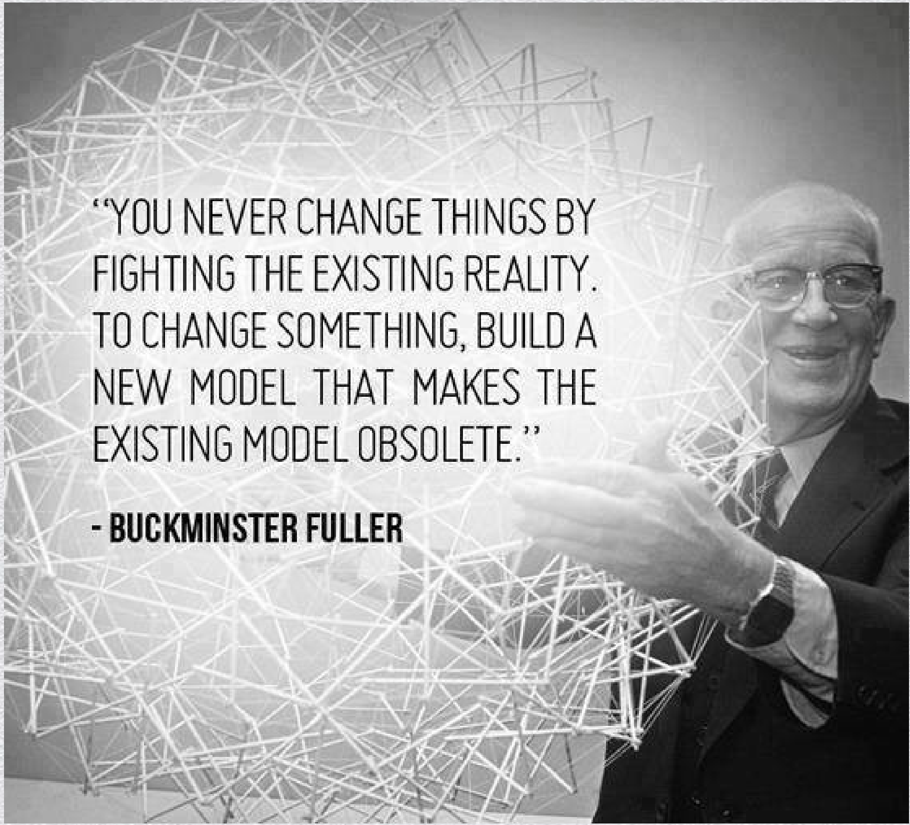
BlueHat Blog
http://blogs.technet.com/b/bluehat/

Via Twitter
Me: @k8em0 (that's a zero)
Microsoft:
@MSftSecResponse

Submit an ORIGINAL mitigation bypass technique: secure@Microsoft.com
Pre-register to submit a FOUND mitigation bypass technique:
doa@Microsoft.com

The Internet Bug Bounty: http://hackerone.com/ibb

Don’t Fight The Existing Models



“YOU NEVER CHANGE THINGS BY FIGHTING THE EXISTING REALITY. TO CHANGE SOMETHING, BUILD A NEW MODEL THAT MAKES THE EXISTING MODEL OBSOLETE.”

- BUCKMINSTER FULLER

Microsoft