The Wolves of Vuln Street:
The 1st System Dynamics Model of the 0day Market

Katie Moussouris
Chief Policy Officer
HackerOne
@K8em0 <— that’s a zero

Michael Siegel
Principal Research Scientist
Massachusetts Institute of Technology
@MITsloan
Collaborators

- 0day market system dynamics research funded by Facebook

Research Team
Dr. Michael Siegel, Principal Research Scientist, Sloan School, Massachusetts Institute of Technology
James Houghton, Sloan School, Massachusetts Institute of Technology
Dr. Ryan Ellis, Harvard Kennedy School
Collin Greene, Security Engineer, Facebook
Katie Moussouris, Chief Policy Officer, HackerOne
Why Model the 0day Market?
Myths and Markets – Money Isn’t Everything

DEFENSE

MIXED USE

OFFENSE
WANTED: Dead or Alive – Over $500,000 PAID

Microsoft’s Strategic Bounty Programs:

- **$100,000** for new techniques
- **$50,000** for new defenses
- **$11,000** for IE11 beta bugs
Mitigation Bypass Bounty: $100,000 for a Technique

James and the Giant Check
IE Preview (AKA Beta) Bug Bounty: All in the TIMING

- James and the Giant Check

**Marketplace Gap:**
When Defense is the only game in town

**Actual Results:**
18 serious security holes

### IE10 vs IE11 beta disclosure trends

- **IE10 beta, no bounty**
- **IE11 beta, with bounty** (PROJECTION S ONLY)
Vulnerabilities and Security

Vulnerabilities

Security
Vulnerabilities: All Different but Still Fruit
# Creating a Vulnerability Typology

<table>
<thead>
<tr>
<th>Vulnerability Characteristics</th>
<th>Quantity of Vulnerabilities ➢ Scarce - Numerous</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ease of Vulnerability Discovery ➢ Easy - Difficult to Find</td>
</tr>
<tr>
<td></td>
<td>Likelihood of Vulnerability Rediscovery ➢ Low - High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Patching Dynamics</th>
<th>Technical Difficulty of Remediation ➢ Easy - Hard to Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Logistical Difficulty of Remediation ➢ Easy - Hard to Access</td>
</tr>
<tr>
<td></td>
<td>Average Life of a Vulnerability ➢ Short - Long</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Market Dynamics</th>
<th>Third Party Market for Vulnerability ➢ Offensive, Defensive, Mixed, Etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Market Size ➢ Small - Large</td>
</tr>
<tr>
<td></td>
<td>Bug Bounty Program ➢ Yes, No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Human Dynamics</th>
<th>Attackers ➢ Criminals, States, Patriots, Etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Researcher Pool ➢ Small - Large</td>
</tr>
<tr>
<td></td>
<td>Attacker Motivation ➢ Political, Financial, Reputational</td>
</tr>
</tbody>
</table>
System Dynamics Modeling

I. Models Complex Human Systems

- Process Improvement
- Market Crises
- Government Stability
- Software Development

II. Simulates Dynamic, Nonlinear Behavior

- Hopes
- Fears
- Time

III. Formalizes Connection, Causality & Feedback

IV. Gives Structure to Data
What policy levers do we have for reducing vulnerability?

Which has the most leverage?
Undiscovered Vulnerabilities

Patching
Undiscovered Vulnerabilities

Discovery

Offensive Stockpile

Patching

Deployment
Learning, Recruiting

Offensive Capability

Leaving, Erosion

Undiscovered Vulnerabilities

Discovery

Patching

Offensive Stockpile

Patching

Deployment
Offensive Capability

Undiscovered Vulnerabilities

Defensive Capability

Learning, Recruiting

Leaving, Erosion

Discovery

Patching

Deployment

Offensive Stockpile
Smoothed, normalized, aligned bug reporting careers of the top 180 MSFT bugfinders

Weight proportional to total productivity

Years before and after peak productivity [quadratic scale]
Offensive Capability

Undiscovered Vulnerabilities

Defensive Capability

Learning, Recruiting

Leaving, Erosion

Discovery

Patching

Deployment

Offensive Stockpile
No Correlation
Some Correlation
The 0day Market System Dynamics Model
"Bug Collisions" Between Offense & Defense

- Discovery from offensive stockpile is very sensitive to the correlation. A powerful lever!
- Defensive capacity development or offensive capacity minimization have different levels of importance depending on the value of the correlation.
How does discovery correlation arise and behave?

- Fixed code base
- Heterogeneous vulnerabilities
- Common techniques between research groups
For a young piece of software

With our model parameters, 9% overlap
For a hardened piece of software

With our model parameters, 0.8% overlap
Rate of "Bug Collisions" Varies with Target

- Correlation can arise naturally due to varied discovery difficulty
- As software becomes more hardened, expect to see less correlation between discovery groups
Defenders Scale Best With Tools & Techniques
Money Changes Everything

- Be careful not to create perverse incentives
- Unintended consequences of draining resources if defense bounties are too high
Key Takeaways For Organizations

- Creating incentives for tools and techniques for vulnerability discovery is a more efficient way for defenders to drain the offensive stockpile.

- Bug bounties are still effective to help find vulnerabilities, especially in less mature software.

- The vulnerability market is not controlled by price alone.
Key Takeaways for Governments

- Many governments are in the role of both attacker and defender.
- Governments need to broaden the focus of policy debates, it is not just about whether or not to stockpile individual vulnerabilities for offense.
- Governments reap defense gains when they make vulnerability discovery tools and techniques available to defenders.
Applying this Research in the Real World

- Use Incentive programs!
- Bounty tools and techniques (e.g., fuzzers & tools that help determine exploitability). The most effective way to drain the offensive stock pile.
- Bug bounties are an effective way to help find vulnerabilities, especially in young software.

What Are We Doing?
- The Internet Bug Bounty is offering bounties for tools and techniques this year.
- We are looking to involve more organizations in our research with MIT.
It Has Not Escaped Our Notice...

- The Wolves of Vuln Street are among us

- We are studying the dynamics of the pack to make the shepherds of the Internet Defense more effective

- More models are needed to identify and mobilize other levers besides price in the 0day market
“YOU NEVER CHANGE THINGS BY FIGHTING THE EXISTING REALITY. TO CHANGE SOMETHING, BUILD A NEW MODEL THAT MAKES THE EXISTING MODEL OBSOLETE.”

- BUCKMINSTER FULLER