MIRROR CHESS: WHY MATURE, PREDICTABLE SECURITY IS A DISASTER

Sam Curry
Chief Security Officer
Cybereason
@samjcurry

David Berliner
Senior Manager, Research
Cybereason
The Mirror Chess Problem
The Three Mirror Chess Problems

Mirror Adversaries

Mirror the Past

Mirror Other Fields
Maturity leads to Exploitable Predictability

- Maturity leads to consistency
- Consistent approaches can be learned
- Adversaries can affect training, influence blind spots
Ransomware for Misdirection (and Profit)

- July 2017 – ONI ransomware family seen and reported on in Japan
- Shortly thereafter - Company A sees ONI and a new variant, MBR-ONI
- Ransomware discovered to be part of a wiper, used to cover tracks and make extra profit
- If company had acted according to their ransomware response playbook, broader attack would not have been found

Traditional Investment Pyramid

Gen 3: Advanced Detection
Gen 2: (Disk-based) Indices of Aggregated Data
Gen 1: Prevention and static / perimeter security controls

Legacy Controls
SIEM
Vulnerability, Patch
Network (FW, IDS)
Endpoint (AV, HIPS)
Perimeter Protection
Identity Controls

Advanced Toolkit
Endpoint Behavioral Analysis (EDR)
Network / User Behavior (NBAD, UeBA)
Intelligence
Sandbox
Payload Analysis
“NG” SIEM

Reactive Security Strategy
Detect and Respond
Desired Spending State: NG and More Value

Value

Advanced Detection
Gen 3, now

(disk-based) Indices of Aggregated Data
Gen 2, 5-10 years

Prevention
Gen 1,
10-15 years

Legacy Comfort Zone

IT Security

Advanced Threat Toolkit
- Endpoint Behavioral Analysis (EDR)
- Network / User Behavior (NBAD, UeBA)
- Intelligence
- Sandbox
- Payload Analysis
- “NG” SIEM

Legacy Controls
- SIEM
- Vulnerability, Patch
- Network (FW, IDS)
- Endpoint (AV, HIPS)
- Perimeter Protection
- Identity Controls

Desired State
Proactive Hunting

cybereason

Cyber Security
Leaky Abstraction

SAY LEAKY ABSTRACTION
ONE MORE TIME
Adversaries can determine how security teams spend their time

Spectre and Meltdown – Patch coverage still limited for these vulnerabilities

- Security teams spending time figuring out ways to block execution through rule sets
- Taking away time from their ability to triage and secure the broader environment
Adversaries get defenders to do their dirty work for them

What if disabling Flash was the goal of the exploiters of CVE-2018-4878?

- Attackers can force defenders to take predictable remediation actions
- What if this was Word? Excel? An ICS program?
FACTS OF LIFE WITH MIRROR COMPLICATIONS
Facts of Life with Mirror Complications

- Business Need to be Open, Integrate & Cloud migrations
- Asymmetry in Rate of Innovation
- Weaknesses Inherent to Machine Learning
- Limited Resources *
- Hard to Find and Retain Talent *
- Distraction by Non-Mission Priorities *
- Single Points of Failure *
- High Cost of Resilience *

Mirror Chess Risk
Chance * Impact = Total

Weights
High (3)  Avg. (2)  Low (1)

* See Appendix for rationale on these
Business Need to be Open, Integrate & Cloud Migrations

Complication

Need to be open and integrate
Short term focus

Predictable Impact

Increase in attack surface, access options
Decrease in security reach and visibility

Predictable Response

Increasing use, reliance on automation

Mirror Problem

Lack of ability to "verify"
False sense of security

Mirror Chess Risk

<table>
<thead>
<tr>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>9</td>
</tr>
</tbody>
</table>
Asymmetry in Rate of Innovation

Adversaries innovate faster than 1) target, 2) product, 3) services

Complication

Predictable Impact
- Increase in ZeroDay techniques
- Exploits in new, uncovered vectors in Kill Chain

Predictable Response
- Lionization of ML for its own sake
- Increase in automation and ML

Mirror Problem
- Defenders get in rut of following adversaries
- Longer adversary TTL
- Set up aggregative ML effect

Mirror Chess Risk

<table>
<thead>
<tr>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>9</td>
</tr>
</tbody>
</table>
Weaknesses Inherent to Machine Learning

Complication
- Overlearning
- Not enough data + too many variables
- Statistical significance ≠ security significance

Predictable Impact
- Creates blind spots
- Increases options to adversaries

Predictable Response
- Add more ML (vicious circle)
- Deploy traditional countermeasures on top of ML

Mirror Problem
- Poison the well
- Chaotic output
- Increased risk
- Erosion of trust in ML

Mirror Chess Risk

<table>
<thead>
<tr>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Avg.</td>
<td>6</td>
</tr>
</tbody>
</table>

OTHER
# The Basic Complications

<table>
<thead>
<tr>
<th>Complication</th>
<th>Mirror Chess Risk</th>
<th>Rationale / Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chance</td>
<td>Impact</td>
</tr>
<tr>
<td>Limited Resources *</td>
<td>High</td>
<td>Avg.</td>
</tr>
<tr>
<td>Hard to Find and Retain Talent *</td>
<td>Avg.</td>
<td>Avg.</td>
</tr>
<tr>
<td>Distraction by Non-Mission Priorities *</td>
<td>Avg.</td>
<td>Avg.</td>
</tr>
<tr>
<td>Single Points of Failure *</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>High Cost of Resilience *</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

* See Appendix for rationale on these
MIRROR COMPLICATIONS FOR NEXT-GEN TECHNOLOGIES
Traditional countermeasures can be ignored

Pseudo-randomness can sometimes be predicted and filtered out

Graphic: https://www.nde-ed.org/EducationResources/CommunityCollege/EddyCurrents/Procedures/SignalFiltering.htm

Graphic: https://www.nde-ed.org/EducationResources/CommunityCollege/EddyCurrents/Procedures/SignalFiltering.htm
Noise to signal ratio

- Hard to be fast and smart
- Garbage-in, garbage-out
- Promise of AI: find the signal
- Dangers of AI used here:
  - How to find new signals
  - Create a new queue and noise in that queue
  - Adversaries can trigger AI to contribute to the noise!
Behavior Changes, Invalidating Patterns

Over time...

- Good begins to look like bad
- Bad begins to look like good
- Sam’s corollary to Metcalf’s Law:
  - Same network over time increases in value over time with no change in the size
Policy-driven systems become counterproductive with scale
THE ASPIRATIONAL SOC
Machine Learning as Building Block for Next Gen Sec

- Artificial Intelligence, Machine Learning, Data Science, Automation
- Easy to trump-up (trickle down)
- Security lags advances, most is still hype*
- Massive potential

* See presentation on Security Analytic by Sam Curry and Yonatan Striem-Amit from RSA Conference 2017 (SEM-M04) for more
The Next Generation

We might be able to...

- Authenticate without passwords
- Authorize without policies or rules or any knowledge *a priori*
- Prevent malware and malicious operations
- Limit damage and improve health
- Find the needle in a haystack
- Reverse the cyber advantage

But we might as Humans also...

- Get stuck in “ruts”
- Trust, but forget to verify
- Understand the abstraction, but not the root cause
- Not train our next generation of defenders
- Lose sight of the mission
- Make our organizations less secure
What good looks like –
E.g. the Incident Response Challenge

<table>
<thead>
<tr>
<th>Before (Best case)</th>
<th>Hypothetical Company</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>5M Events / day</td>
<td>Manufacturing or Finance</td>
<td>5M Events / day</td>
</tr>
<tr>
<td>50K Suspicions</td>
<td>100K Endpoints</td>
<td>100K Suspicions</td>
</tr>
<tr>
<td>150 Incidents Caught</td>
<td>120 Incidents Caught</td>
<td>120 Incidents Caught</td>
</tr>
<tr>
<td>100 TP (5 Risky TP) + 50 FP; 20 FN missed</td>
<td>110 TP (7 Risky TP) + 10 FP; 10 FN missed</td>
<td></td>
</tr>
<tr>
<td>92 Incidents Resolved</td>
<td>120 Incidents Resolved</td>
<td></td>
</tr>
<tr>
<td>4.6 Risky incidents Remediated</td>
<td>7 Risky incidents Remediated</td>
<td></td>
</tr>
<tr>
<td>20 TP incidents never found</td>
<td>4 hrs / person free to hunt FNs!</td>
<td></td>
</tr>
</tbody>
</table>

8 people per shift
1 hour per incident, 4 hours per risky incident

8 people per shift with better triage
30 min per incident, still 4 hours per risky incident
MITIGATIONS FOR MIRROR CHESS RISKS
Established Doctrine of Risks

“To be prepared everywhere is to be weak everywhere”
Art of War, Sunzi

“The most effective way to stem the tide of risk aversion is for Marines to build trust at all levels…”
- Lt. Col. Gregory A. Thiele

Trust Equation: David Maister, Charles M. Green and Rob Galford, *The Trusted Advisor*
Strategies for Risk Reduction

People Development

- Encouraging trust / rewarding risk taking
- 10th Man / Devil’s Advocate Office
- Rotating the 10th Man
- Mentorship / apprenticeship
Strategies for Risk Reduction

People Development
- Encouraging trust / rewarding risk taking
- 10th Man / Devil’s Advocate Office
- Rotating the 10th Man
- Mentorship / apprenticeship

Processes
- Checking blind spots (Crazy Ivan)
- Free Hunting
- Retrospective / post-mortem
- Cross fertilizations SecOps with DevSec, DevOps and DevSecOps
Strategies for Risk Reduction

People Development
- Encouraging trust / rewarding risk taking
- 10th Man / Devil’s Advocate Office
- Rotating the 10th Man
- Mentorship / apprenticeship

Processes
- Checking blind spots (Crazy Ivan)
- Free Hunting
- Retrospective / post-mortem
- Cross fertilizations SecOps with DevSec, DevOps and DevSecOps

Machine Learning
- Aging data / retraining
- Transparency of automation tools and processes
- Root cause tracing with output from AI / ML
## How to apply

<table>
<thead>
<tr>
<th>How to secure...</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next Week</strong></td>
<td>Review common attack patterns: how your IR processes might bias against detecting innovations</td>
</tr>
<tr>
<td><strong>Next Three Months</strong></td>
<td>Develop training to improve intuition, craft, mastery in IR team Review blind spots created by playbooks</td>
</tr>
<tr>
<td><strong>Next Six Months</strong></td>
<td>Review blind spots created by investment decisions</td>
</tr>
<tr>
<td><strong>... And Remember</strong></td>
<td>Beware abstraction Ensure the next generation share “trust but verify”</td>
</tr>
</tbody>
</table>

*Understand and share your limitations.*

*Remember, you have carbon based intelligence.*
### How to apply

<table>
<thead>
<tr>
<th>How to secure...</th>
<th>Processes</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next Week</strong></td>
<td>Review common attack patterns: how your IR processes might bias against detecting innovations</td>
<td>Share second-order risk from maturity process</td>
</tr>
<tr>
<td><strong>Next Three Months</strong></td>
<td>Develop training to improve intuition, craft, mastery in IR team Review blind spots created by playbooks</td>
<td>Review how investment decisions are led by external influence (avoid “industry-think”)</td>
</tr>
<tr>
<td><strong>Next Six Months</strong></td>
<td>Review blind spots created by investment decisions</td>
<td></td>
</tr>
<tr>
<td><strong>... And Remember</strong></td>
<td>Beware abstraction Ensure the next generation share “trust but verify”</td>
<td>Maturity always leads to some exploitable predictability. Find it first (reduce security debt).</td>
</tr>
</tbody>
</table>
# How to apply

<table>
<thead>
<tr>
<th>How to secure...</th>
<th>Processes</th>
<th>Management</th>
<th>Technology (as a practitioner)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next Week</strong></td>
<td>Review common attack patterns: how your IR processes might bias against detecting innovations</td>
<td>Share second-order risk from maturity process</td>
<td>Review tools for SPF, create compensating controls</td>
</tr>
<tr>
<td><strong>Next Three Months</strong></td>
<td>Develop training to improve intuition, craft, mastery in IR team. Review blind spots created by playbooks</td>
<td>Review how investment decisions are led by external influence (avoid “industry-think”)</td>
<td>Discuss redundancy and blind spots with vendors (remember, vendors want to be your only provider)</td>
</tr>
<tr>
<td><strong>Next Six Months</strong></td>
<td>Review blind spots created by investment decisions</td>
<td></td>
<td>Practitioners and Vendors partner to counter adversary influence, improving ML resilience against relevant threats Improve your rate of innovation as a KPI</td>
</tr>
<tr>
<td><strong>... And Remember</strong></td>
<td>Beware abstraction. Ensure the next generation share “trust but verify”</td>
<td>Maturity always leads to some exploitable predictability. Find it first (reduce security debt).</td>
<td>Work with companies that understand and share their limitations. Don’t reward hyperbole</td>
</tr>
</tbody>
</table>

**Cybereason**

RSAC Conference 2018
# How to apply

<table>
<thead>
<tr>
<th>How to secure...</th>
<th>Processes</th>
<th>Management</th>
<th>Technology (as a practitioner)</th>
<th>Technology (as a vendor)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next Week</strong></td>
<td>Review common attack patterns: how your IR processes might bias against detecting innovations</td>
<td>Share second-order risk from maturity process</td>
<td>Review tools for SPF, create compensating controls</td>
<td>Identify ML weaknesses (review data set interference, analyze algorithm for weaknesses)</td>
</tr>
<tr>
<td><strong>Next Three Months</strong></td>
<td>Develop training to improve intuition, craft, mastery in IR team, Review blind spots created by playbooks</td>
<td>Review how investment decisions are led by external influence (avoid “industry-think”)</td>
<td>Discuss redundancy and blind spots with vendors (remember, vendors want to be your only provider)</td>
<td>Develop protections for ML (internal evaluation teams, adversarial ML, shifting data sets)</td>
</tr>
<tr>
<td><strong>Next Six Months</strong></td>
<td>Review blind spots created by investment decisions</td>
<td>Practitioners and Vendors partner to counter adversary influence, improving ML resilience against relevant threats</td>
<td>Improve your rate of innovation as a KPI</td>
<td></td>
</tr>
<tr>
<td><strong>... And Remember</strong></td>
<td>Beware abstraction, Ensure the next generation share “trust but verify”</td>
<td>Maturity always leads to some exploitable predictability. Find it first (reduce security debt).</td>
<td>Work with companies that understand and share their limitations. Don’t reward hyperbole</td>
<td>Understand and share your limitations. Remember, you have carbon based intelligence</td>
</tr>
</tbody>
</table>
Q&A

Thank you
APPENDIX

Analysis of risks associated with additional basic complication
Limited Resources

Complication

Limited Resources for coverage or new projects
Gaps in monitoring, hunting
Less forward leaning projects
Inferior monitoring

Predictable Impact

Multiple teams and managed services
Increase in automation in multiple locations
Increase of tools that aggregate and correlate
Blind trust in tools

Predictable Response

Adversaries have longer time between “sweeps” and bigger shadows to hide in
Coordination complications among automation stacks
Gap in hunter knowledge re “how it works” in sec. eng.

Mirror Chess Risk

<table>
<thead>
<tr>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Avg.</td>
<td>6</td>
</tr>
</tbody>
</table>

Mirror Problem

PAST
Hard to Find and Retain Talent

Complication

Hard to find and retain talent
- Senior talent (L2/L3)
- Low level (L1) talent

Predictable Impact

- Hard recruiting training cost ($, time)
- Burnout, less focus on excellence

Over reliance on playbooks
- Alone automation
- Over reliance on ML to supplement human effort
- Just take what comes off the queue

Predictable Response

- Lack of ability to “verify”
- Less mastery (XP!) dev
- Longer attacker TTL in environment
- Less knowledge of “how,” especially over time

Mirror Problem

Lack of ability to “verify”
- Less mastery (XP!) dev
- Longer attacker TTL in environment
- Less knowledge of “how,” especially over time

Mirror Chess Risk

<table>
<thead>
<tr>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg.</td>
<td>Avg.</td>
<td>4</td>
</tr>
</tbody>
</table>
Distraction by Non-Mission Priorities

Complication

Distraction by non-mission priorities
Need to spend time on compliance, hygiene for hygiene', reporting, etc.

Predictable Impact

Decrease in % of time at “sharp end” finding / stopping malicious ops
Defenders “stay in the rut”

Predictable Response

Increase automation
Increased use of ML
Tools to assist become manipulable

Mirror Problem

Lack of urgency to “verify”
Less mastery (XP!) dev
False sense of security
Longer attacker TTL in environment

Mirror Chess Risk

<table>
<thead>
<tr>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg.</td>
<td>Avg.</td>
<td>4</td>
</tr>
</tbody>
</table>

PAST
Regulatory waves bring efficiency pressure

1st Wave: Do something!
2nd Wave: Pay the price!
3rd Wave: Get specific!
4th Wave: Get ahead of the Reg!

What does it mean?
Can I get out of it?

No escape
Fines coming
Everyone’s a consultant

Details, details, details
Cost is king
Security enslaved by compliance

• Can be hard to achieve
• Risk-centric discipline
• Regulations have catalyzed but don’t dominate
Single Points of Failure

Complication
- Network and systems single points of failure
  - Often the consequence of other issues or lack of alignment with IT

Predictable Impact
- Security talent and tools reliance on homogeneity
- Multiplication of errors
- Ever growing blind spots

Predictable Response
- Segmentation efforts (this is a good thing if it can be done!)
- Deployment of “dumb” correlation, aggregation, reduction and automation

Mirror Problem
- Adversaries apply similar attack to multiple areas
- Increase in attractiveness as target
- Catastrophic, chained failure with bigger impact

Mirror Chess Risk

<table>
<thead>
<tr>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>High</td>
<td>3</td>
</tr>
</tbody>
</table>

Cybereason
Resilience normally an afterthought

**Complication**
- Post-infection processes weak
- DR/BC weak
- Lack of experience or live-fire practice in recovery

**Predictable Impact**
- Playbooks may switch to backup on first sign of failure
- Gaps in image windows too long

**Predictable Response**
- Adversaries can trigger quick resilience to force disruption and harm (DOS)
- Greater risk of ops and IP losses during image windows
- New vulnerability surface

**Mirror Problem**
- High Cost of Resilience

<table>
<thead>
<tr>
<th>Mirror Chess Risk</th>
<th>Chance</th>
<th>Impact</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>High</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>