A State of Dynamic Risk

Containment & Victory in a World of APTs

Branden R. Williams, CISSP, CISM
CTO – Marketing, RSA

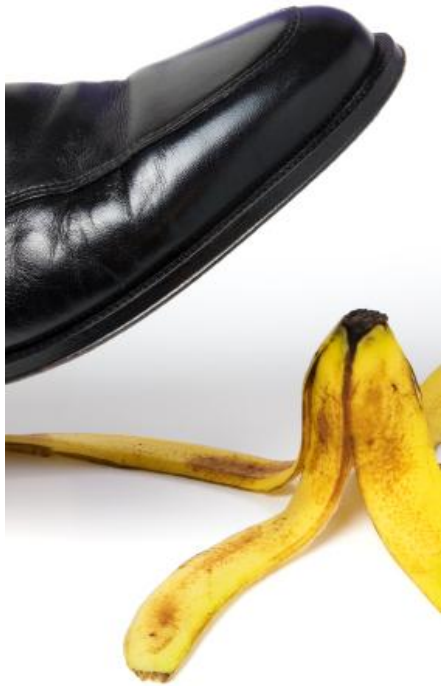
Today

- Dynamic Risk Defined
- Traditional Infosec
- Players in Cybercrime
- How they Operate
- What Next?
- Questions

What is Dynamic Risk?

Static Risk

Fixed in time and space, known

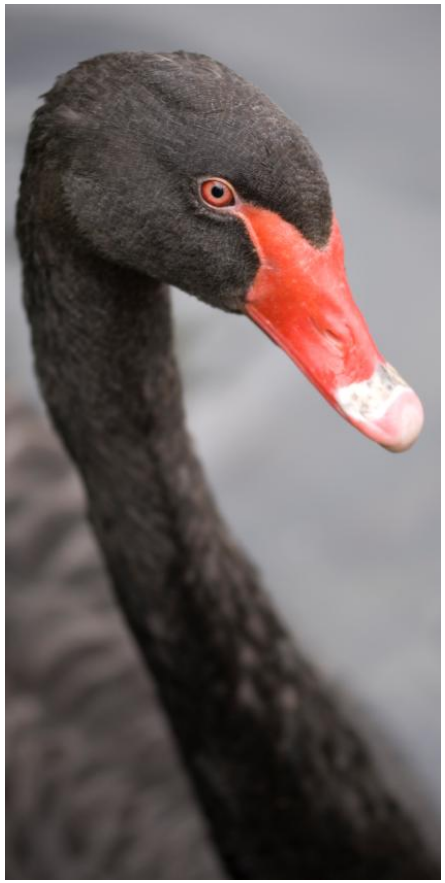


- You can insure against it
- The risk profile remains the same
- Event probability may or may not change
- Environment/Ecosystem stable

- Examples:
  - Homeowner's Insurance
  - Hole-in-One Prize
  - Volcano Insurance in Texas

Dynamic Risk

Varies without predictability, unknown



- Uninsurable (typically)
- Environment changes in an unpredictable way
- Event probability may or may not change

- Examples:
  - Fads
  - The creation of a new weather phenomenon
  - Cyber security

Objectives of Infosec

- Keep the Goods In
- Keep the Bad Guys Out

Traditional Infosec

- Deploy a firewall
- Use anti-virus
- Put public-facing assets in zones
- Run a vulnerability scanner every so often
- Fight for basic resources

- REACT TO BAD STUFF

Static v. Dynamic Risk

How does dynamic risk change our jobs?

- Today's opponent is intelligent
- Therefore, if you build a wall, the opponent will…
  - Go around it
  - Go over it
  - Go under it
- The right way to deal with the situation is to build walls (don't let anyone tell you that's a bad idea)
- It's a bad idea to rely on the wall as the primary or only means of defense
- Rely on dynamic, adapting technologies and seek architectural breakthroughs (whose boundaries you know)

Who are the players?

"You know, you can do this just as easily online."

The “Community’ of Attackers

Criminals

Petty criminals

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

Nation States

PII, government, defense industrial base, IP rich organizations

Non-state actors

Terrorists

PII, Government, critical infrastructure

Anti-establishment vigilantes

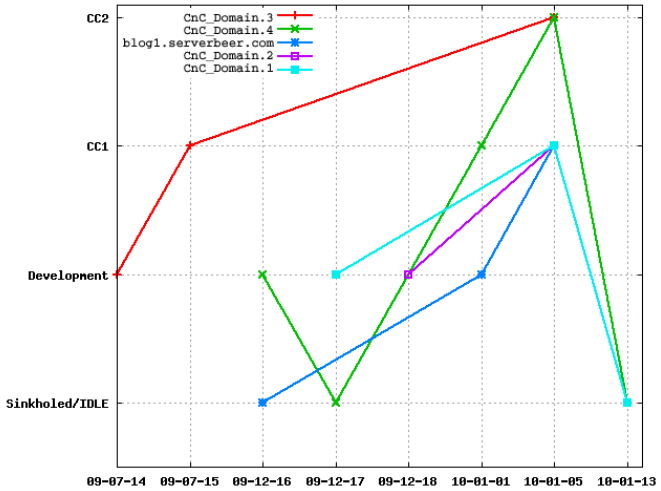
“Hacktivists” Targets of opportunity

How do they operate?

Stealth

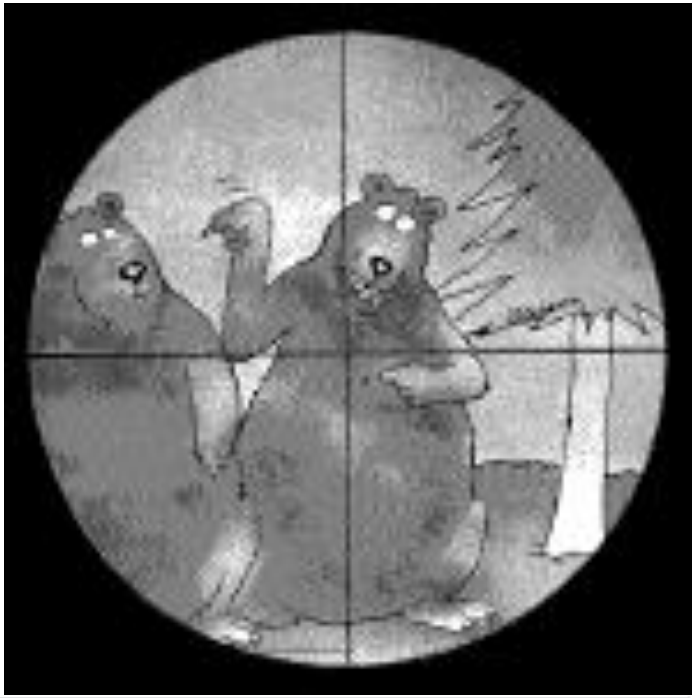
Stay invisible to victim operators on host ALAP

- No regular traffic or computation on infected host
- No predictable traffic or computation on infected host
- Intricate CnC topology to make detection of CnC traffic hard (still the weakest link though)
- Use domain name agility rather than DDNS
- Fast Flux
- Temporary Deregistration



Persistence

- When an exploit fails, try another later
  - Do until exploit succeeds ... one will
- When an exploit succeeds, consolidate
  - Multiple additional vectors
  - Establish Backdoors
- When attack succeeds, come back later



The Human Element (Case Study)

- Attackers today use more than one attack front
- Technical tools (walls) don't protect you
- Breach Example:
  - Included combination of social engineering, zero-day exploitation, and privilege escalation
  - Began with spear phishing attack via social media
  - Exploits zero-day via another app (Embedded exploits)
  - Targets administrators

AV Defense (wall) is Questionable…

Anti-Virus Engine	No. of Variants detected by AV Engines Out of 547	Detection Rate % of the total variants
NOD32	245	44.8%
GData	242	44.2%
Panda	231	42.2%
BitDefender	230	42.0%
Kaspersky	223	40.8%
McAfee	211	38.6%
McAfee-GW-Edition	208	38.0%
Ikarus	207	37.8%
AntiVir	199	36.4%
Sophos	197	36.0%
Microsoft	190	34.7%
AVG	188	34.4%
DrWeb	183	33.5%
Avast5	177	32.4%
TrendMicro-HouseCall	158	28.9%
TrendMicro	152	27.8%
F-Secure	150	27.4%
Symantec	150	27.4%
Fortinet	145	26.5%
Prevx	89	16.3%

Zero-day Powered

- Aurora
  - 05/02/2009 FakeAVTrojan1-a mcsmc.org thcway.info
  - 08/18/2009 FakeAVTrojan1-b mcsmc.org thcway.info
  - 10/20/2009 FakeAVTrojan1-c mcsmc.org miecros.info
  - 10/22/2009 FakeAVTrojan1-d mcsmc.org mnprfix.cn micronetsys.org
  - 11/26/2009 FakeAVTrojan1-e mcsmc.org filoups.info
  - …
  - 01/12/2009 Trojan.Hydraq
- How do 0-Day's become exposed? (use after free, shallow copy, out of spec API usage)
- Could have been much more precise:
  - vTable substitution
  - Function substitution
  - Stack substitution
  - Object substitution

```
bstrName = SysAllocString(OLESTR("cat"));
hr = pObj->GetDispID(bstrName, 0, &dispid);
hr = pObj-> InvokeEx(dispid,
LOCALE_USER_DEFAULT, DISPATCH_PROPERTYGET,
&dispparamsNoArgs, &var, NULL, NULL);
```

Challenge: Cleanup

Necessary for integrity and compliance

- Did you get it all? (Cleaning)
- Do you adequately understand how it happened? (Forensics)
- Will the exploits work again? (Remediation)
- Is damage understood and contained? (Risk Model and Reduction)

APTs are nasty because…

- Little opportunity for correlation
  - Focused, so no community sourced warning based on correlation across victims
  - Zero-day heavy, so ineffective behavioral pattern or footprint signature correlation
  - Complex and resilient CnC -> hard to correlate on attack source
  - CnC Operators change as botnets are transferred by section or by victim.
  - Low and Slow, so no temporal correlation. Signal to noise ration is low. Touch to compromise ration 1.4.
- APT Malware Analysis:
  - Average File Size: 121.85 KB
  - Only 10% of APT backdoors were packed
  - Packing is not as common in Standard APT malware
  - Packing is common in advanced APT Malware and used by more advanced APT groups

APT Names and Malware

- Most Common APT Filenames:
  - svchost.exe (most common)
  - iexplore.exe
  - iprinp.dll
  - winzf32.dll
- APT Malware avoids anomaly detection through:
  - Outbound HTTP connections
  - Process injection
  - Service persistence

What now?

Time to shore the foundation

- Be perimeter aware, but information focused
- Understand the context of events and not just the meat of the events
- Point solutions don’t make for a secure ecosystem
- Buy security built in, not bolted on
- Understand the business to best protect it and its stakeholders

Perimeter v. Information (transaction) centric

- The perimeter is going away
  - We all know it and have heard it
  - We all sense there's something right about this
- It's better to say that it's shrinking
- Ultimately, it's about the data and its value to you, competitors, and if lost
- Result: Become perimeter aware and information and transaction centric

http://www.primrosecottageholidays.co.uk/custom/kent_dover_castle.jpg

Attack Focus v. Context

- So you want to get away with a murder…
  - Locard's exchange principle: with contact between two items, there will be an exchange (this is why we have CSI labs)
  - You have two options
    - Clean up all traces (duct tape / spandex / etc
    - Spread around a lot of false trace evidence
- We see a huge amount of "noise"
  - Background noise covers tracks
- Result: Focus on the context of the events and the intelligence surrounding attacks, not the attacks themselves

Some personal items of Mr Sherlock Holmes

No Eight Ball!

Point Products v. Ecosystem

- Security events occur on seams
- Complexity detracts from a systems approach
- It makes sense to pursue…
  - Smoother hand-offs
  - Better coordination
  - Less complexity
  - More interoperability
- Consider also the people and processes!
- Sometimes the best product doesn't work best
- Result: The harmony among people, products, and tools and an "ecosystem" approach, over time, is what will make the most difference in securing companies

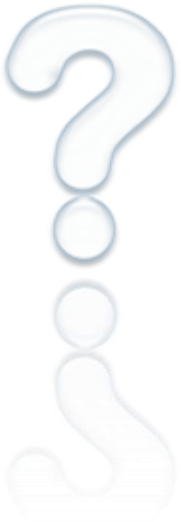
Built-In v. Bolted-On

- “Not another agent?!?”
- Bolt-On follows legacy IT principals (make it work) and only works for expediency in the short term
- Over-time, technologies have to become more transparent
- We can’t be spending our time focusing on the tool – we need to focus on the task
- Result: Focus on transparency and building security into the infrastructure—to bolster intelligence, adaptability, ecosystems and so on.

Business v. Technology Focus

- Security is a BUSINESS problem
  - Information is monetized
  - Business processes depend on information technology
- There is always another point of view (Raconteurs)
  - Lots of ways to accomplish secure operations
  - Understanding the business operations helps to devise an appropriate plan to secure them
- Technology-focused security is the tail wagging the dog
- Result: Business aware security allows the build to grow securely!

Q&A



Branden R. Williams, CISSP, CISM

Branden.williams@rsa.com

CTO – Marketing

Blog: brandenwilliams.com

Office: +1 (214) 432-5446

THANK YOU