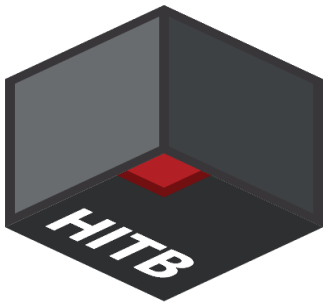


HITB+ CyberWeek

Abu Dhabi, UAE: 12-17 October 2019

Building High-performance Security Research Teams

Tips for the smallest to the biggest corporations

Rodrigo Rubira Branco (@BSDaemon)

Chief Security Researcher

INTEL STrategic Offensive Research & Mitigations (STORM) Team

rodrigo *noSPAM* kernelhacking.com

“Be curious. Read widely. Try new things. I think a lot of what people call intelligence boils down to curiosity.” - **Aaron Swartz**

Disclaimers

- I don't speak for my employer. All the opinions and information here are my responsibility
- I'm sorry in advance for the excessive usage of generalizations!
- No specific profession or field is better or necessarily harder or more challenging than any other
  - I am passionate for security research and that is the focus of this talk, so lessons might apply to other areas but I'm not implying that is so

“As long as you keep the team unified, you shall succeed”

– **Master Splinter**

Objectives

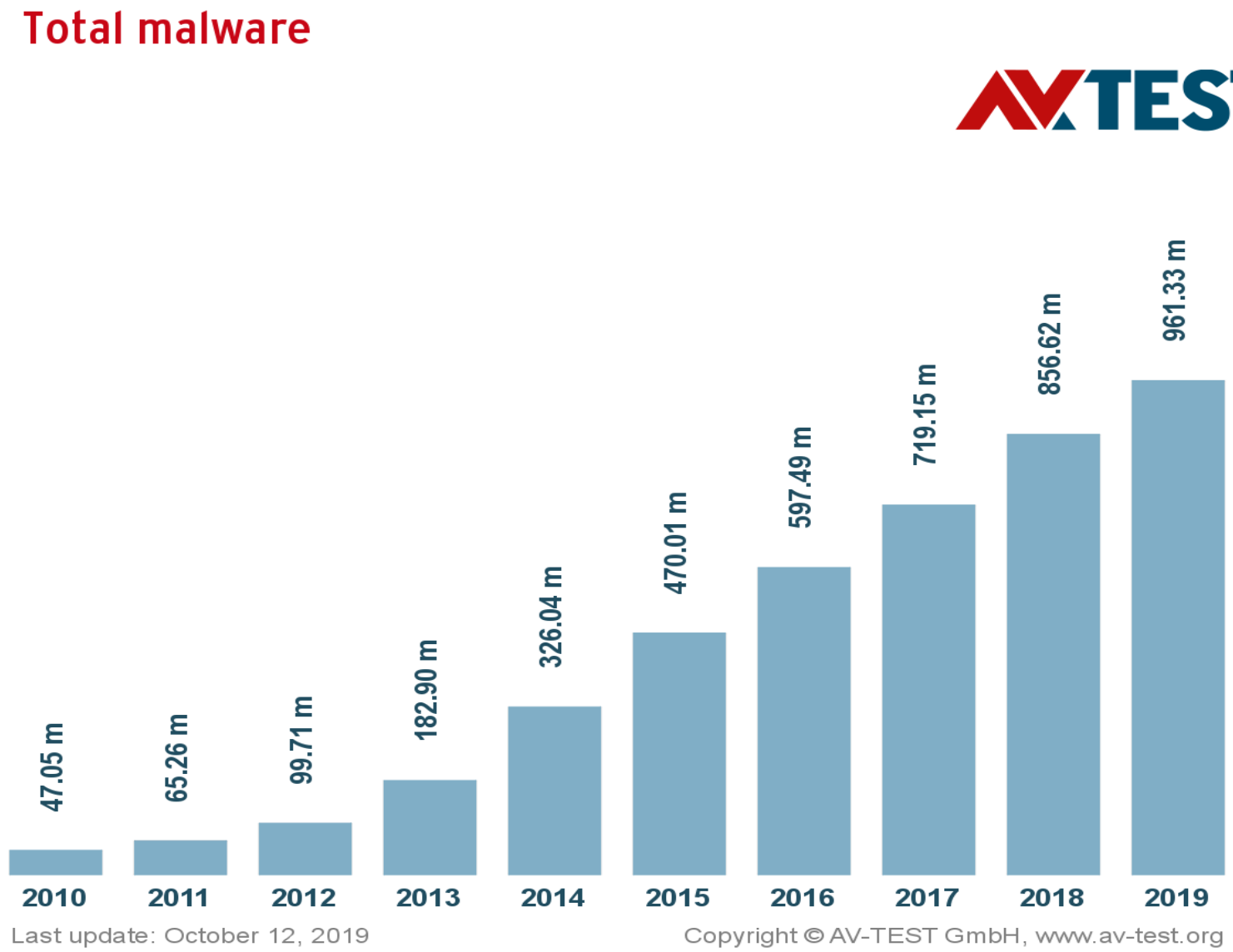
- There exists a lot of information on building efficient teams

- Hopefully I will present what is lesser known (or what does not necessarily apply to overall leadership)

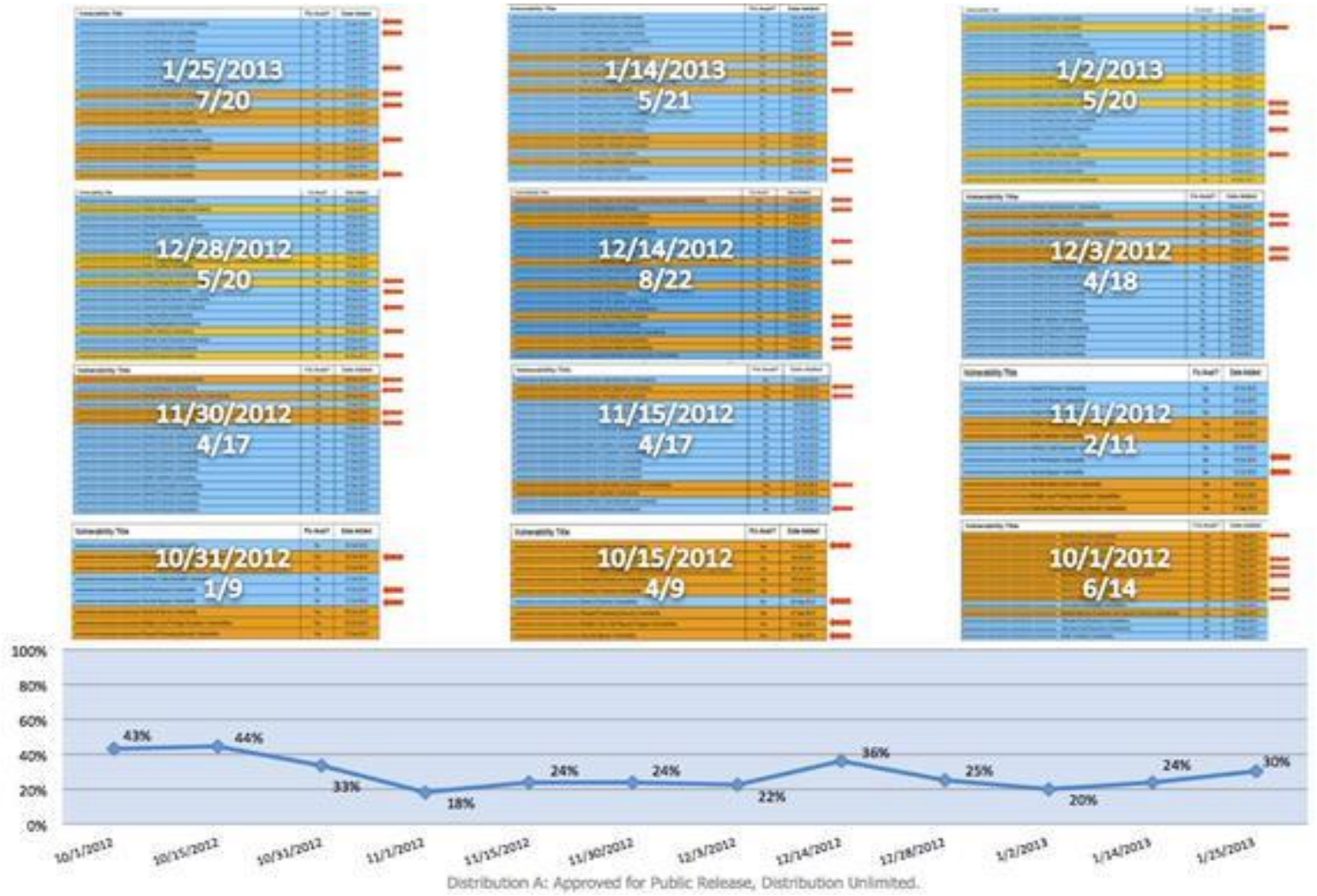
Security nowadays

- Buggy programs deployed on critical servers
- Rapidly-evolving threats, attackers and tools (exploitation frameworks)
- Lack of training for developers, lack of resources and people to fix problems and create safe code
- **That's why we are here today, right?**

Why are we here?



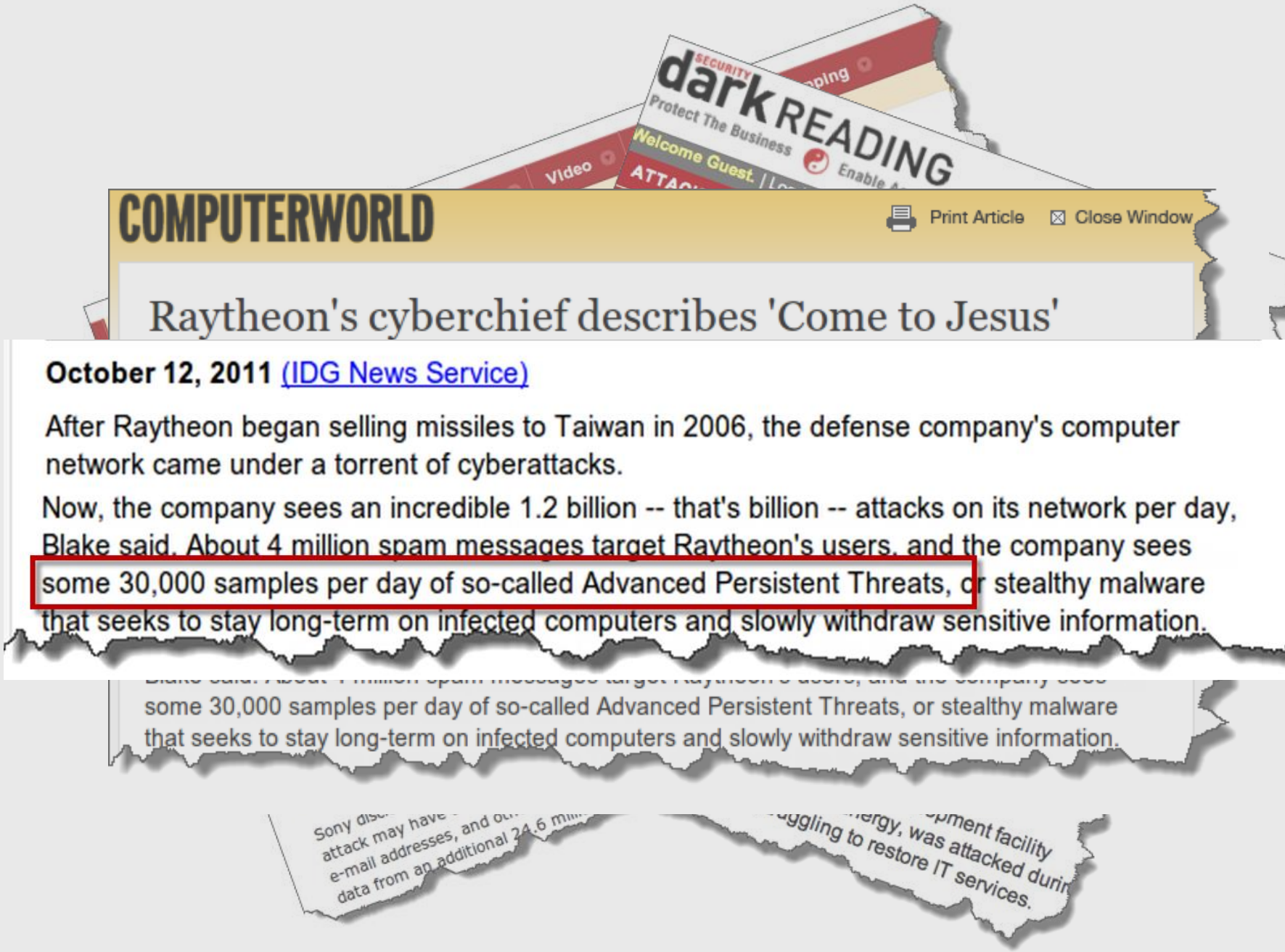
1/3 of Government Systems Vulns are in Security Software



Source: Tweet by @dotMudge

Asia Pacific Threats? (APT)

- Ops, it is not the Chinese anymore…
- Are all compromises advanced?


dark READING
Protect The Business
Welcome Guest.
Video
COMPUTERWORLD
Print Article
Close Window
Raytheon's cyberchief describes 'Come to Jesus'
October 12, 2011 (IDG News Service)
After Raytheon began selling missiles to Taiwan in 2006, the defense company's computer network came under a torrent of cyberattacks.
Now, the company sees an incredible 1.2 billion -- that's billion -- attacks on its network per day, Blake said. About 4 million spam messages target Raytheon's users, and the company sees some 30,000 samples per day of so-called Advanced Persistent Threats, or stealthy malware that seeks to stay long-term on infected computers and slowly withdraw sensitive information.
some 30,000 samples per day of so-called Advanced Persistent Threats, or stealthy malware that seeks to stay long-term on infected computers and slowly withdraw sensitive information.
attack may have
e-mail addresses, and
data from an additional
facility
was attacked
to restore IT services.

100% security is economically unfeasible

- **Crime and Punishment: An Economic Approach - Gary S. Becker**
- Since there are no guarantees, why should anyone care? Or prioritize?
- “Why should I buy from vendor X?”
  - “Because everybody is doing so”

What is security, for real?

- Some argue that a system is secure when it is behaving in the way it is designed to

- I believe that is not exactly the case
  - Some functional issues are security issues
  - Some security issues might be just functional issues
  - **But, many security issues are just the change of the assumptions a system operates on, or the composition of multiple perfectly behaving systems**

Composition and Assumptions

The two biggest sins?

- Assumptions are really what people ‘believe’ about a system
  - A security researcher must be able to challenge the assumptions
  - Make sure they are correct
- The composition of assumptions (present in different functionalities) work against researchers, since they change the truism of assumptions
  - So security researchers **must learn fast** (faster than usual)
  - And I argue that researchers **have to know more** about the system than the engineers who developed it (and that sometimes worked on it for 15 years)

Composition and Assumptions

- The 15 year knowledge is still invaluable (due to history, how decisions were made)
  - That is why it is important to partner with the design teams
- But the assumptions might have changed due to the composition that happened over time

And what security research is?

- re·search (/ˈrēˌsərCH,rəˈsərCH/)
- *noun*
  - the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions.
- *verb*
  - investigate systematically.

And what security research is?

- While security research has a lot of engineering challenges, it is mostly investigative (and as such, it must have open-ended questions and expect possibly new conclusions)

- Security research has a lot of failures (approaches that do not work, ideas that do not pan-out)

Comparing to Chess

- Besides the intellectual comparison [1]
  - Chess ‘teams’ are essentially an individual’s work that is added up to a team result/score
  - A research team’s work is most often individual ‘human<->computer’ time (in which the different pieces complement each other for the final result)

[1] “A Praise for Hackers”, Zero Nights 2015. Link: http://2015.zeronights.org/assets/files/00-Branko.pdf

Importance of Mistakes in Research

- *"Some part of a mistake is always correct"*
  - *Savielly Tartakover*

- *"an accumulation of small advantages leads to a supreme advantage."*
  - *Wilhelm Steinitz*

So, why build a research team?

- Companies highly benefit from security research
  - Better understanding
  - Real-life awareness
  - Solving complex problems with lower budgets
- Having security researchers isn't only for security vendors
  - A researcher is capable of solving complex tasks, such as analyzing huge amounts of logs
  - A researcher can provide real understanding of the threats in an organization, 'translate' the marketing materials to the real-world benefit it provides

"Tonight you have learned the final and greatest truth of the Ninja: that ultimate mastering comes not from the body, but from the mind. **Together**, there is nothing your four minds cannot accomplish. **Help each other**, draw upon one another, and always remember the **power that binds you**."

– **Master Splinter**

Offensive and Defensive Research are both Important

- **Offensive research** is important to keep the state-of-the-art knowledge and understanding of offensive strategies

- **Defensive research** is extremely important to be sustainable (just fixing bugs is not enough as a durable strategy that deals with modern development growth and software dependency)

Offensive x Defensive Research

- The problem is how we see security research in general as well
  - Offensive is cool
  - Defensive is boring, useless

Offensive x Defensive Research

"Investments in defense should benefit from the investments in offense (be guided by it) [1]. In the mitigations space, implementation details make all the difference and proper architectural definitions are not enough." [2]

[1] Ben Hawkes. "Project Zero – Make 0day Hard". CanSecWest 2015.
[2] BSDaemon. "Keynote Inside the Machine". Offensive Con 2018.

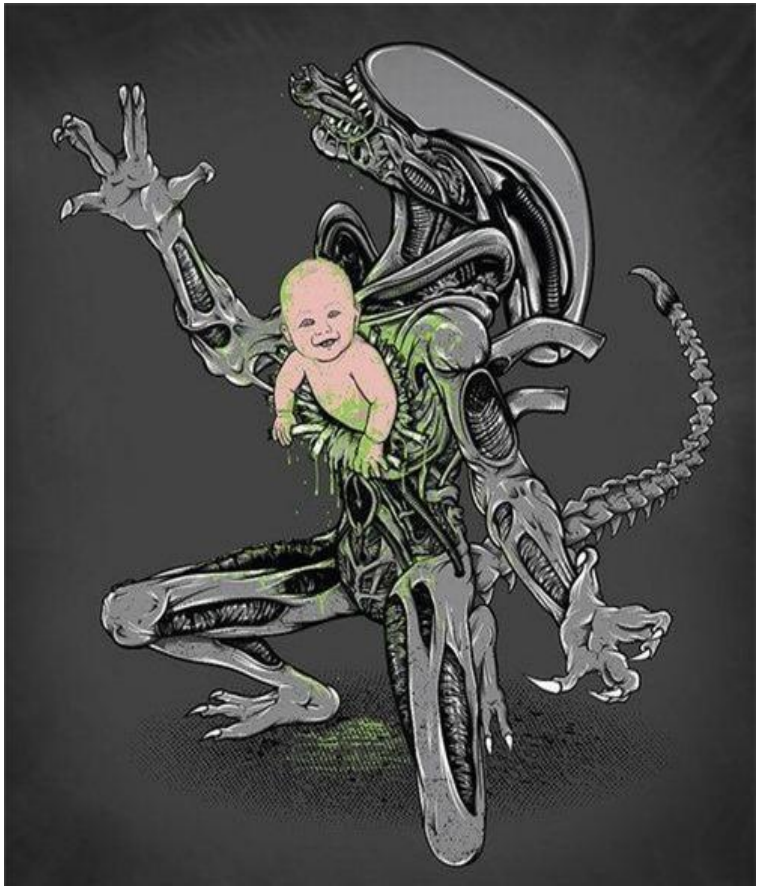
What can we improve?

- We researchers are culpable:
  - Every time we demonstrate a bypass of something, we forget to mention the many times that something is actually useful
  - We also forget to mention what is the actual state of the art for the given technology we are bypassing, and which mistakes were made in the specific implementation we are targeting ☺

What comprises a team?

- Every highly efficient research team needs at least:
  - Experience (Knowledge/Skills)
  - Dedication
  - Passion
  - Vision (and leadership principles)
  - An ‘extremist’ (the person that keeps the team aligned with the vision)

So a team is born!



Asymmetry

“The amount of energy necessary to refute bull**** is an order of magnitude bigger than to produce it.”

Alberto Brandolini

Security Myth #1: The 'EXPERT'

- **The Market for Lemons: Quality Uncertainty and the Market Mechanism – George Akerlof**

- Asymetric knowledge
  - Complex subject
  - Industry defines its own standards
  - Politics define 'auditing' (e.g., SOX)

The new speed?

- *"Half the variations which are calculated in a tournament game turn out to be completely superfluous. Unfortunately, no one knows in advance which half"*
  - *Jan Tinman*

- Many somehow nowadays expect results before the 'sit-and-work time'

"The path that leads to what we truly desire is long and difficult, but only by following that path do we achieve our goal."

- Master Splinter

Passion

“Do what you love and you’ll never work a day in your life”

Passion (Patched)

Do what you love and you'll ~~never work a day in your life~~ work super f****** hard all the time with no separation or any boundaries and also take everything extremely personally

@adamjk

So watch for…

- Burn-out
- Overall stress
  - Specially with the speed of others
- Folks do take things personally, after all, they love what they do…
  - Solve problems without removing their passion

The importance of a TEAM

“Today's German Language lesson: "TEAM" is a German abbreviation for "Toll, Ein Anderer Machts". (engl. "Great, someone else does it")”

FX

The importance of a TEAM

While it is obviously a joke, it reminds us that we need to be careful with group decisions (when everyone believe everyone else is doing something)

The importance of a TEAM

“Be like a volleyball team and not like a soccer one”

Bernardo Rocha de Rezende (Bernardinho)

suggestion in his book (“Transforming Sweat into Gold”)

The importance of a TEAM

"If you are like a soccer team, at least do not be like a 'varzea' one (non-professional league in Brazil)"

@BSDaemon

Complex Problems – A Team matter?

"Those proposing mitigations must understand the problem. Such understanding can be gained through experience writing real exploits (with real limitations and complexities) or by teaming up with someone with that experience." [1]

[1] BSDaemon. "Keynote Inside the Machine". Offensive Con 2018.

Disclaimer: Being able to write exploits do not imply liking to do it (I do know developers that work in very good mitigations that do not like to write exploits, but have the full understanding and ability to do so)

The importance of a Vision

and guiding principles

- Google's Project Zero Vision [1]
  - "Make 0day hard"

- Intel STORM Vision
  - "A research team that has **highly motivated individuals** and freedom to find **interesting (to the individual)** security-related topics to work on; that will work harder, deliver more, and **achieve, surpass, and drive the state of the art** faster than any other team with any other motivational factor."

[1] Ben Hawkes. "Google Project Zero". Black Hat USA 2019. Link: "https://i.blackhat.com/USA-19/Thursday/us-19-Hawkes-Project-Zero-Five-Years-Of-Make-0day-Hard.pdf"

The importance of a Vision

- Once in a chess competition, grandmasters were analyzing a position -> They mostly agreed a given side had advantage (let's say white)

- Capablanca was passing by and was asked to give an opinion: he said black had a clear advantage (!)

- When told to demonstrate it, instead of doing moves, he just changed the entire position to something new -> To the surprise of the grandmasters, there was nothing white could do to avoid the game to get into that position
    - NOTE: I've not added a reference because I couldn't find one, maybe I mixed names of the grandmaster. If you have a reference on that, please send it my way ☺

Importance of Leadership

"Chess, like any creative activity, can exist only through the combined efforts of those who have creative talent, and those who have the ability to organize their creative work."

– Mikhail Botvinnik

Trust in a Team

- Trust is at first given, not deserved
  - Team Principles keep the trust and help solving problems
- It is the way that humans are, that's why social engineering works!
- This is also what generates the problem, because security is something counter-natural, and people see hackers as paranoids
  - **Trust should not be transitive either**
  - **Be prepared to deal with team members that will *not* give trust first! Learn how to develop that trust.**

Hiring

- I believe previously released research is a great source to understand an individuals motivation/passion/skills
- 1:1s are a good way for folks to see individual fit (we usually do group interviews for technical discussions)
- Interview challenges are a way to quickly remove bias (some individuals might not be as social as others and be nervous when answering questions in an interview)

Are CTF results a good criteria for Hiring?

- **“***Chess is not like life... it has rules!***”**
  - *Mark Pasternak*

- “**and so does CTFs**”
  - BSDaemon

Great, but what knowledge to prioritize in an interview?

- Mikhail Botvinnik was a three-times world champion of chess and had as pupils Anatoly Karpov, Garry Kasparov and Vladimir Kramnik

- Even after that, it was said that he listened to basic chess lessons in the radio. The reason: To always remind him of the **fundamentals**. Keep them sharp
    - NOTE: I've not added a reference because I couldn't find one, maybe I mixed names of the grandmasters. If you have a reference on that, please send it my way ☺

The Fundamentals

- The essence behind computation did not change
  - The Turing Machine model of computable problems existed even before digital computers (1936)
  - Chomsky's work on language hierarchy is from the 1950's
  - TCP/IP is from the 1980's
    - The essence of PC architecture too ☺

Measure understanding, not memorization

- *"Chess books should be used as we use glasses: to assist the sight, although some players make use of them as if they thought they conferred sight"*
  - *Jose Raul Capablanca*

- "**If you really know, you can hack**"
  - BSDaemon

Remote Teams? Flexible Hours?

- I am highly in favor of flexibility for creative work

- Flexibility can be seen in a lot of things, from remote work, hours of work to choosing the problems to work on
  - The secret is to find the proper balance
  - Finding the right problems (that are interesting, challenging and impactful – with meaning to the company) is harder in some places than others (and depending on the team's objectives)
  - Remote work requires better infra-structure for sync'ing in some styles of work, but expands the pool of talent available
  - Flexible hours seems like a must nowadays ☺

“Do not confuse the specter of your origin with your present worth”

– **Master Splinter**

The importance of diversity and mentorship

- Diversity is essential to bring new points of views and approaches
  - Read the work by Scott E. Page (University of Michigan) on the topic
  - Diversity is about education, backgrounds, minorities and many other aspects and provide a real (measurable) advantage to a team

- Mentorship is essential to evolve junior folks, to keep the passion in the team and to keep the team true to its principles

What About Metrics?

- What about them?

- Besides the usual metrics (that fit the organization and make sense for the team's vision and objectives), here is one to consider that is uncommon/untraditional
  - How many talents did your senior researchers bring to the organization in the past?

What About Metrics?

- Value deepness versus breadth for researchers
  - It is more important to really deeply understand and challenge assumptions than give opinions in a bunch of meetings
  - Sometimes a simple opinion in a meeting might have a ‘high’ impact, but is that what you need researchers for?

“We choose what holds us back and what moves us forward”

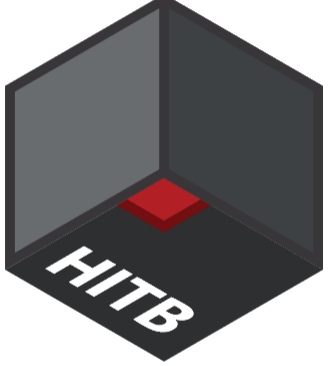
– Master Splinter

Hackers are changing the world

- Lots of hackers currently work for big corporations and/or independently
- They are working on pushing defensive technologies in hardware, operating systems and many different software
- They are also working on finding and patching security vulnerabilities

What does the future hold?

- Understand what security is really about and what are the real security aspects of a system:
  - Complexity is bad
  - Assumptions are dangerous
  - Composition of systems != the security of each element of that system
  - What is formally proven is not necessarily correct if the pre-requirements and simplifications of the computing model are not correct either (if they lose power)
  - **A security research team will impact your view and understanding on all those problems!**



HITB+ CyberWeek

Abu Dhabi, UAE: 12-17 October 2019

"Be curious. Read widely. Try new things. I think a lot of what people call intelligence boils down to curiosity." - **Aaron Swartz**

The End!! Or is it Really !?

Rodrigo Rubira Branco (BSDaemon)
Chief Security Researcher
INTEL STrategic Offensive Research & Mitigations (STORM) Team
rodrigo *noSPAM* kernelhacking.com
https://twitter.com/bsdaemon

Acknowledgements

- This material would not be possible if it was not for the excellent team that I'm proud to be part of!

- Special thanks to:
  - Marion Marschalek
  - Thais Hamasaki
  - Will Burton