FIDELIS CYBERSECURITY™

Takedowns:

Case studies and what we can be doing better

John Bambenek, Threat Research Team

Botconf ‘15

Intro

- 16 years in cybercrime, member of threat research team for Fidelis Cybersecurity based in US.
- Generally work with federal authorities in “friendly” countries on global criminal enterprises.
- Part-time faculty at University of Illinois at Urbana-Champaign in Comptuer Science.
- Produce open-source intelligence on organized crime online.
  - http://osint.bambenekconsulting.com/feeds

Sharing restrictions

- Everything here can be considered TLP:GREEN, slides and video will be online anyway.

- There is, however, some information TLP:AMBER or higher that goes into my conclusions, we can discuss offline if you like (maybe).

Problem Statement

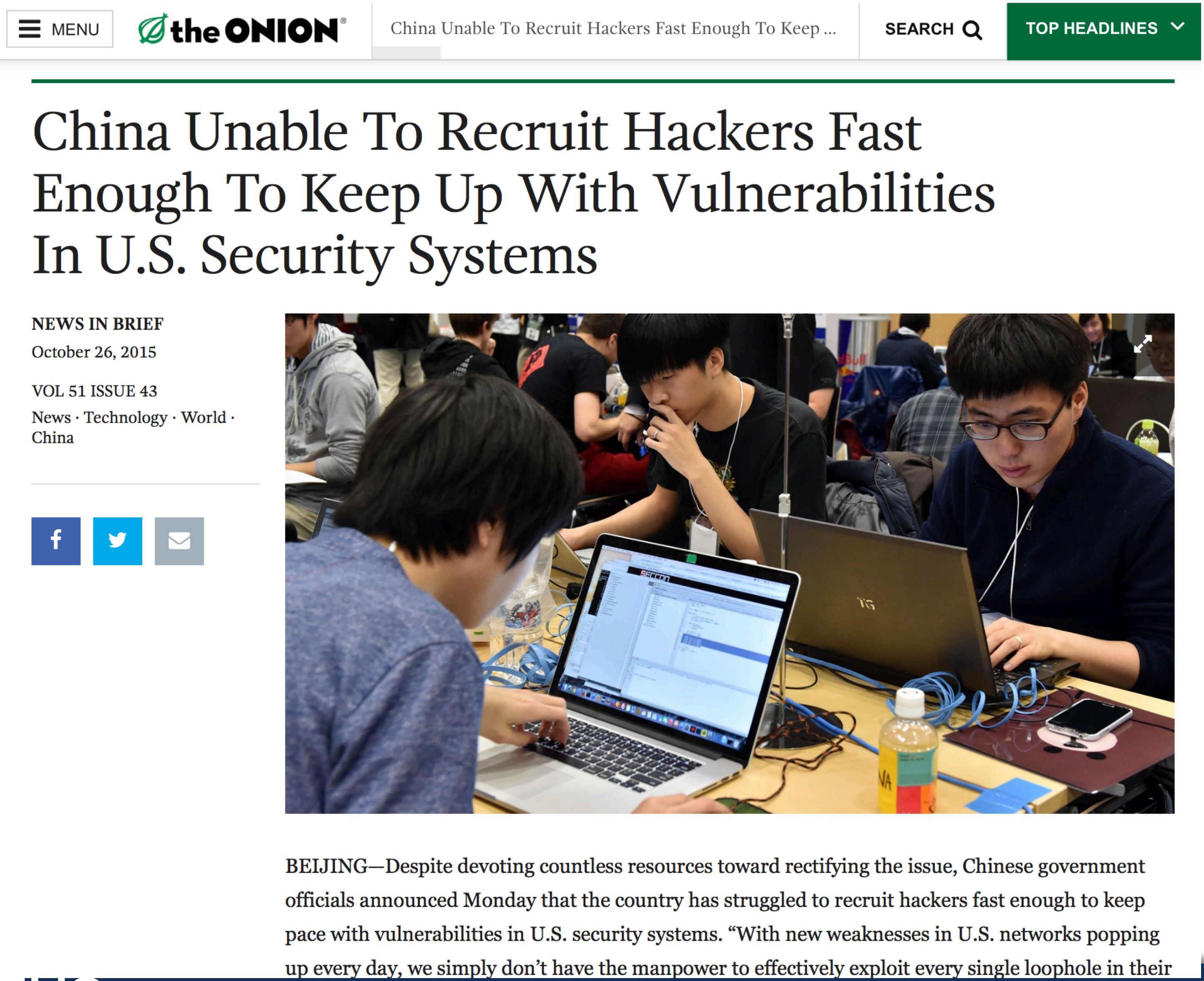
- Right now we are on the losing end of an arms race
    - The adversaries produce more malware than we can possibly analyze.
    - We have to operate in the open while they operate in secret.
    - Their core business is exploitation, security for us is a cost center.
    - We operate in a global economy without an effective means of global law enforcement.

TL;DR

Bad News: We’re doomed

Good News: Unlimited job security for me

TL;DR



China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

NEWS IN BRIEF

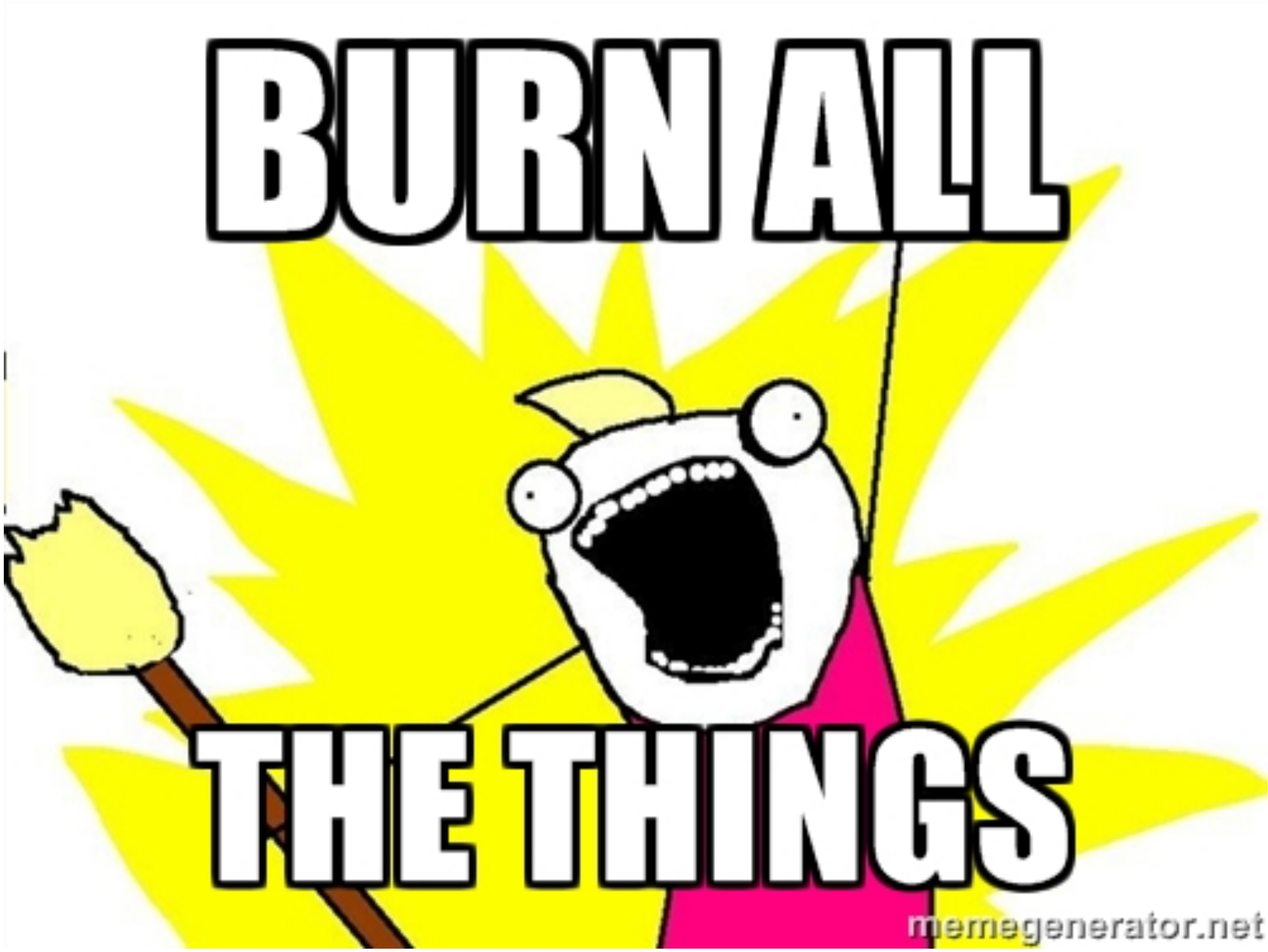
October 26, 2015

VOL 51 ISSUE 43

News · Technology · World · China

BEIJING—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. “With new weaknesses in U.S. networks popping up every day, we simply don’t have the manpower to effectively exploit every single loophole in their

My approach to takedowns



What is a takedown?

- Treated as a distinct and special action in security.
- Seizing a few domains?
- Getting a hosting company to clean up their network?
- Marketing ploy?
- My definition: an operation to significantly disrupt an adversarial actor’s capability to continue in their efforts and designed to achieve a particular objective.

Why do a takedown?

- Most everyone here works for a security company, we can build products to prevent infections and mitigate for our customers. That’s what we are paid to do.

- But most of the people who are in most need of protection do not or can not pay for our products.

The takedown debate?

- Attackers will adapt…
- Takedowns are ineffective…
- Do more harm than good…
- Should law enforcement always be involved…

Takedowns as disruption

- Everything we do is disruptive to attacker objectives and to varying degrees they adapt to all of it.
  - AV Detections
  - Firewall Rules
  - Blacklists
  - DGA list example

- Takedowns are just farther on the other side of disruptive activities we can do but certainly not the most extreme end of it.

Ineffective?

- After every takedown the “best” outcome is some other crime family took its place. In many cases, the actor reconstituted themselves, sometimes within hours.

- Occasionally there has been collateral damage.

- There have been success stories: Conficker, Zeus/Cryptolocker, Ramnit, Dridex (to an extent)

Do more harm than good…

- Besides adaption, there may be collateral damage.
- Important to enumerate all paths of communication of C2s to victim.
- Important to run through outcomes of removing adversarial infrastructure to the victims.
  - Conficker
  - Ransomware

Should law enforcement be involved?

- Define involved…
- Arrests are better than takedowns, I will usually defer to law enforcement if there is active interest.
- “Agency” issues.
- What if there is no active LE interest? Or what about “unfriendly” jurisdictions?

Should LE be involved?

- How to get LE involved revolves around one question?

- Sometimes only way to get the necessary data is to do a partial takedown/sinkholing operation.

Deconfliction

- My personal approach before taking private/civil action is to reach out to LE to find who has an open case/if there is an open case.
  - Some but decreasing difficulty of doing this with non-US LE.

- I will work on any LE takedown operation if I can help in any way.

Marketing Ploys?

- An issue in the information security industry in general and the threat intelligence industry in specific is that in the absence of someone defining operational requirements, marketing departments define those requirements.

- Stop this.

Takedown objectives

- Takedowns for the sake of a take down will generally always fail.

- A takedown is not necessarily the ideal outcome. An arrest is.

- Other outcomes may lend themselves to not taking something down (economic / reputation attacks against adversary, more on this soon)

Case study: No-IP

- Many malware campaigns use Vitalwerks (No-IP) for dynamic DNS.
- MSFT, in essence, took over No-IP DNS via civil court order in attempt to block only the “known malicious” no-ip hostnames.
- Hilarity did not ensue.

Case study: No-IP

- Microsoft was unable to fully manage No-IPs DNS and massive outages occurred.

- Was, in theory, supposed to target only a small percentage of No-IP hosts.

- Ultimately major brand damage occurred and Microsoft settled matter with No-IP privately.

- Use of alternate dynamic DNS providers began but not yet “in earnest”.

Case study: No-IP

- No cooperation with outside entities.
- No apparent risk assessment on collateral damage.
- Tried to take over third-party infrastructure without ability to manage it.

Case Study: Conficker

- Massive international private sector and LE cooperation.
- Adversarial control of botnet successfully disabled.
- 2011 arrests connected, in part, to Conficker actors.
- Still about 600,000 or so infected machines.

Cast Study: Kelihos (pick one)

- Have been about four attempts to take this down. Including one on stage at a conference.

- None have persisted beyond days (hours).

- Generally involved P2P poisoning.

Case study: Kelihos

- Objective appeared to be a takedown for the sake of a takedown.
- Research into alternative channels not thoroughly researched.
- Generally was go-it-alone.

Case study: Cryptolocker/GOZ

- My piece was the Cryptolocker part.
- 14 nations, 150 or so private sector participants.
- Appeared in August 2013, COULD have taken it down ~October.

Case study: Cryptolocker/GOZ

- Had to weigh risks of more people being infected versus ability of victims to recover files.
  - Erred on side of recovery and “we” did eventually recover the private keys and a service was published to recover encrypted files.

- Cryptolocker was tied to Gameover Zeus and we deferred action in favor of GOZ case. (Meant waiting almost 6 more months).

Case study: Cryptolocker/GOZ

- CL and GOZ dead and have not returned.
- Actor under indictment with US $3M bounty.
- Was a effort for remediation and public awareness (more by NCA than in US).
- Cooperation with private sector in .ru and .cn

Case study: Alienspy “takedown”

- Alienspy part of long family of commercial Java-based RATs (unrecom, frutas, adwind), current JSocket.
- All builders/C2s call to main domain to verify subscription status.
- Published report on details and due to lack of clarity on my part, AlienSpy.net was suspended nuking all builder/C2s worldwide.

Case Study: Alienspy

- Key lesson: being clear what can be done with data and asking people not to take action ☺

- Exposed a consequence of the actor's design choices.

- Also exposed an interesting path of attack: economic/reputation attacks.

Case study: Angler

- On Oct 6, 2015, Cisco said they took down part of Angler.

- In reality, just helped one specific hosting company to clean up all the Angler related stuff in their network.

- Minimal impact to Angler but good impact to that provider.

Case study: Xindi botnet

- Just kidding!

- ☺

How its done (civil process)?

- For DNS-based C2 channels, it’s easy.

- For hosting/service providers, mileage varies.
  - “Contractual” / AUP requests easier.
  - Civil litigation comes with “standing” issues.

- Law enforcement has better tools but there are civil means but highly complicated.

Economic/Reputation Attacks

- Key problem for the “bad” guys, the operate in a service economy just like we do. How do criminals trust other unaffiliated criminals?
- Exit strategy
- How can this be used against other threats (i.e. Kelihos)?

Dealing with “non-cooperating” jurisdictions

- Just because governments of various countries may not cooperate doesn’t mean private sector in those countries can’t work together.

- Still needs to be relevant to them or worth their while.

- Involves good old fashioned relationship management.
  - Trust lists / electronic groups good but not enough.

My Entry Requirements for a Takedown

- Willing partners
- Relevant threat
- Thorough knowledge of primary and backup means of communication
- Risk analysis of both collateral damage and deception

Wrapping it up

- Takedowns are just another form of disruption which all of us do every day.
- Key is to have an ultimate objective and picking the right tools to achieve that objective (and a takedown might not be it).
- Deconflicting with LE essential because there are better outcomes than takedowns.

Wrapping it up

- Broad cooperation is key.

- Building relationships and trust is essential. Go-it-alone not a recipe for success.

- Need to be better about informing public not just about being infected, but as a means for building security awareness.

QUESTIONS?

TO JOIN ANY OF MY EFFORTS GET IN TOUCH (RANSOMWARE, DGAS, DDOS, KELIHOS…)

JCB@PEOPLE.OPS-TRUST.NET
+1 217 493 0760