

## No more free bugs NLNOG-day 2015



### This talk

### To shed some light on a shady side of the internet

- Some background on Odays
- What does the Oday market look like? •
- How is this relevant to us? •
- So now what?

## About

### **Christiaan Ottow**

**CTO of Pine Digital Security** 

christiaan.ottow@pine.nl

@cottow





### What we do



### **Security services**

Performing penetration tests, code audits and consulting/training



### **Managed hosting**

Managed secure hosting services for customers (AS12854)



### Secure development

**Developing software** for customers with a high security or privacy demand

### Zero Day (Oday) vulnerability: a vulnerability that has not been publicly disclosed



Source: Stefan Frei, "The Known Unknowns" [1]

### 2013

Program	Program	Total	Targeted	Time To
	Inception	Purchases	Vendors	Disclosure
iDefense VCP	2002	969	195	133 days
TippingPoint ZDI	2005	1,423	92	174 days

Source: Stefan Frei, "The Known Unknowns" [1]

### **ZDI**, 2015

- Over 2000 disclosed vulnerabilities •
  - That's ± 600 in the last 18 months •
- 2010: > 30% took > 365 days to patch
  - 180-day automatic disclosure implemented •
- 2013: only 6 vendors > 180 days, 5 > 120 days •
- 2014: 120 day automatic-disclosure implemented

Source: ZDI@10: 10 fascinating facts about 10 years of bug hunting [10]

### **Odays live 312 days on average in the wild before disclosure**

Source: Bilge et al, "Before we knew it" [12]

## **Suppliers**

- VUPEN VBI • Raytheon Netragard • • Northrop Grumman ReVuln • • **Endgame Systems** • • •
- **Exodus Intelligence** •

### **Mitnick Security**

### Zerodium

### Growth



Source: Cisco IBSG [8]

NSA 'hacking unit' infiltrates computers around the world - report

 NSA: Tailored Access Operations a 'unique national asset' Former NSA chief calls Edward Snowden a 'traitor'



f y @ in g+ & 215 shares 0 comments

The Home Office has denied that recent changes made secretively to antihacking laws have "increased" or "expanded" GCHQ's powers. That's despite the fact the spy agency is using the amendment to legalise the same hacking

Certry Images

A top-secret National Security Agency hacking unit infiltrates computers around the world and breaks into the toughest data targets, ac documents quoted in a magazine report on Sunday.

'Politie mag terughacken en Skype afluisteren'

Gepubliceerd: 02 mei 2013 06:34 Laatste update: 02 mei 2013 09:29

De politie krijgt als het aan minister Ivo Opstelten (Veiligheid en Justitie) ligt veel meer bevoegdheden om hackers en cybercriminelen aan te pakken.

LLL

# GCHQ just 'changed the rules' on hacking

iii f ¥ 8+

### **Growth drivers**

- Number of targets
- **Government interest** •
- ROI per target
- Skill required



## Hacking Team

"What you need is a way to bypass encryption, collect relevant data out of any device, and keep monitoring your targets wherever they are, even outside your monitoring domain.

**Remote Control System does exactly that.**"

Source: <u>http://www.hackingteam.it/images/stories/galileo.pdf</u>

## Hacking Team

- Surveillance software
  - Audio recording (phone, Skype, ...) •
  - Keystroke logging •
  - GPS tracking
- Impressive list of customers, including oppressive regimes •
  - Bahrein, Kazakhstan, Azerbaijan [10] •
- Breached in July 2015, 400GB dumped (inc. mail spools, source code, contracts)

## **Suppliers**

- VUPEN
- Vulnerabilities Brokerage International (VBI) •
- Netragard •
- Vitaliy Toropov •



## Pricing

### The grugq, 2012

ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

Source: Andy Greenberg in Forbes, 2012 [3]

## Pricing

### Hacking Team, 2015

- Adobe Reader + sandbox escape: \$100k list price (\$80.5k final) •
  - Sandbox escape non-exclusive: \$90k \$100k •
  - Netragard •
- Three Flash Player Odays: \$39k \$45k
  - Vitaliy Toropov •

## Catalogs

Date	Exploit notes
03/11/14	<ul> <li>SPEEDSTORM 3 (\$215k exclusive): Flash across all browsers</li> </ul>
	escape. Modified version of HIGHWOOD used to bypass sar
	sold for \$120k non-exclusive.) Found via manual audit, 'reac
	impossible
<u>04/23/14</u>	<ul> <li>NEONNIPPLE: Office 2007, Word + Excel, required ActiveX c</li> </ul>
	(going to Edit menu)
	<ul> <li>MUPPET-GRANT: IE 11 UaF, only accessible via Word via SM</li> </ul>
	<ul> <li>PEEDSTORM-KONROY: Flash bug w/ sandbox escape, targ</li> </ul>
	support (~80% reliability), uses modified MOHNS to bypass s
	'reaching through fuzzing should be impossible'
	Marshmallow: Win7 LPE
	<ul> <li>CANDLESTICK-BARNES: Flash, Win + OSX, 7-year old UaF (I</li> </ul>
	description closely matches the one here.)
	<ul> <li>STARLIGHT-MULHERN: Adobe Reader XI + sandbox escape</li> </ul>
	modified HIGHWOOD used to bypass sandbox (doesn't use
05/28/14	<ul> <li>NARCOPLEX: Ammyy Admin v3.3 and 3.4, client-side bug</li> </ul>
	<ul> <li>STIKA (\$80k, non-exclusive): Netgear RCE, exploitable via C</li> </ul>

rs and Win7, 8, or 8.1 w/ sandbox andbox (sandbox bypass alone has ching through fuzzing should be

control, required user interaction

MB/WebDAV gets XP/7, no Win8 or Chrome sandbox. Found via manual audit,

(Likely written by Vitaliy Toropov, the

e, mem disclosure + corruption, e JS or Flash)

CSRF





Source: https://twitter.com/Zerodium/status/644107653745016832

### **Business model**

- Acceptance testing •
- **Replacement if patched** •
- Support on implementation •
- Phased payments •

### Actors



### So what?

- Odays are much like weapons •
- Only, they are almost exclusively interesting for offensive • purposes
- Who benefits from having them and who benefits from fixing • them?

### So what?

- Stopping Oday sales will not stop all spies and criminals •
- But it will stop the likes of HackingTeam •

### Now what?

"[..] Are vulnerabilities in software dense or sparse? If they are sparse, then every one you find and fix meaningfully lowers the number of avenues of attack that are extant.

If they are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it."

### **Corner the market**

- USG buys them all
- Reports all to vendors •
- USG then controls the market •

### Drain the offensive stockpile

"[..] People deserve to use the internet without fear that vulnerabilities out there can ruin their privacy with a single website visit

If we increase user confidence in the internet in general, then in a hard-to-measure and indirect way, that helps Google too"

Source: Wired interview with Chris Evans of Google Project Zero [5]

### **Tweak the levers**



Source: Katie Moussouris, "The Wolves of Vuln Street", RSA Conference 2015 [6]

---IE10 beta, no bounty

> IE11 beta, with bounty (PROJECTION S ONLY)

## Regulation

- Wassenaar, a town in Europe
- Intrusion malware •
- Intrusion exploits •
- IP surveillance

## Regulation

- The problem with dual use
- It's the internet, stupid •
- ACLU is for, EFF has reservations

### **Bugs are dense**

"[..] Which is: you don't chase and fix vulnerabilities, you design a system around fundamentally stopping routes of impact. For spender it is eradicating entire bug classes in his grsecurity project. For network engineers it is understanding each and every exfiltration path on your network and segmenting accordingly.

Containment is the name of the game. Not prevention."

### Conclusions

- A new market has emerged that is at best shady
- Involves actors from gov't, commerce and crime mixed on all • sides
- Legal battle being fought together with Crypto Wars II •
- Will have impact on what our kids' internet will look like •

### **Questions? Shoot!**

## **Bibliography**

- [1] Stefan Frei, Dec 2013, "The Known Unknowns", https://www.nsslabs.com/sites/default/files/ • public-report/files/The%20Known%20Unknowns\_1.pdf
- [2] Vlad Tsyrklevich's analysis of Hacking Team leak wrt Oday trading: https://tsyrklevich.net/ • 2015/07/22/hacking-team-0day-market/
- [3] Forbes/Andy Greenberg's profile on the grugq: http://www.forbes.com/sites/andygreenberg/ • 2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/
- [4] Dan Geer, on density and counting of vulns, "For Good Measure": http://geer.tinho.net/fgm/ • fgm.geer.1504.pdf
- [5] Interview with Chris Evans of Google Project Zero by Wired: http://www.wired.com/2014/07/ • google-project-zero/
- [6] Kate Moussouris, "Wolves of Vuln Street": https://hackerone.com/blog/the-wolves-of-vuln-• street and https://www.rsaconference.com/writable/presentations/file\_upload/ht-t08-the-wolvesof-vuln-street-the-1st-dynamic-systems-model-of-the-Oday-market\_final.pdf
- [7] Bas Alberts, rant on disclosure, "The Old Speak": https://lists.immunityinc.com/pipermail/ • dailydave/2015-August/000976.html
- [8] Cisco IBSG, # of Internet-connected devices: <u>http://www.cisco.com/web/about/ac79/docs/</u> • innov/loT\_IBSG\_0411FINAL.pdf
- [9] Dan Geer, on cornering the market, BlackHat 2014: http://geer.tinho.net/geer.blackhat. 6viii14.txt NSA's TAO group accidentally off lining Syria: http://thehackernews.com/2014/08/ nsa-accidentally-took-down-syrias.html

## **Bibliography**

- [10] ZDI figures after 10 years: <u>http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/</u> • ZDI-10-10-fascinating-facts-about-10-years-of-bug-hunting/ba-p/6770127#.VfgrprQVf8s
- [11] HackingTeam customer list: <u>https://theintercept.com/2015/07/07/leaked-documents-</u> • confirm-hacking-team-sells-spyware-repressive-countries/
- [12] Bilge et al (Symantec), "Before we knew it" on Odays in the wild, 2012:<u>https://</u> • <u>users.ece.cmu.edu/~tdumitra/public\_documents/bilge12\_zero\_day.pdf</u>
- On Odays on the dark web: https://www.deepdotweb.com/2015/04/08/therealdeal-dark-net-• market-for-code-0days-exploits/
- Market size 2012: http://www.slate.com/articles/technology/future\_tense/2013/01/ • zero\_day\_exploits\_should\_the\_hacker\_gray\_market\_be\_regulated.html
- Market size 2012: http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-• who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/
- Market size 2012: http://moritzlaw.osu.edu/students/groups/is/files/2015/06/Fidler-Second-• **Review-Changes-Made.pdf**
- Market size 2013: <u>http://www.darkreading.com/vulnerabilities---threats/hacking-the-zero-day-</u> • vulnerability-market/d/d-id/1141026
- Robert Graham, notes on Wassenaar: <u>http://blog.erratasec.com/2015/05/some-notes-about-</u> • wassenaar.html#.VfnEmbQVf8s
- Heartbleed discovery collision: <u>http://readwrite.com/2014/04/13/heartbleed-security-</u> codenomicon-discovery