Hacking Team: a zero-day market case study

taken from http://tsyrklevich.net/2015/07/22/hacking-team-0day-market/

This article documents Hacking Team's third-party acquisition of zero-day (0day) vulnerabilities and exploits. The recent compromise of Hacking Team's email archive offers one of the first public case studies of the market for 0days. Because of it's secretive nature, this market has been the source of endless debates on the ethics of it's participants. The archive also offers insight into the capabilities and limits of offensive-intrusion software developers. Hacking Team was seriously exploit supply constrained because they had difficulty finding suppliers that they deemed reliable and reasonably priced. Their competitors, like Gamma International and NSO Group, prominently advertised their 0day capabilities, forcing Hacking Team to be defensive with prospective customers.

Despite the lurid journalistic depictions of 0day markets, most of the emails offer a more mundane perspective. Buyers follow standard technology purchasing practices around testing, delivery, and acceptance. Warranty and requirements negotiations become necessary in purchasing a product intrinsically predicated on the existence of information asymmetry between the buyer and the seller. Requirements - like targeted software configurations - are important to negotiate ahead of time because adding support for new targets might be impossible or not worth the effort. Likewise warranty provisions for buyers are common so they can minimize risk by parceling out payments over a set timeframe and terminating payments early if the vulnerability is patched before that timeframe is complete. Payments are typically made after a 0day exploit has been delivered and tested against requirements, necessitating sellers to trust buyers to act in good faith. Similarly, buyers purchasing exploits must trust the sellers not to expose the vulnerability or share it with others if it's sold on an exclusive basis.

On a technical level, it's interesting to note the difference in price for different vulnerabilities. 0day markets allow unique qualitative comparisons for how difficult it is to exploit a given piece of software or bypass certain exploit mitigations. However, the reader should be warned that price comparisons for different exploits should be taken with a grain of salt. It's hard to compare the reliability and projected longevity of vulnerabilities or exploits offered by different developers, and moreover it's unclear how much a given exploit developer might be willing to negotiate the price of their exploit and how differently they price exclusive and non-exclusive sales.

Hacking Team's relationships with 0day vendors date back to 2009 when they were still transitioning from their information security consultancy roots to becoming a surveillance business. They excitedly purchased exploit packs from D2Sec and VUPEN, but they didn't find the high-quality client-side oriented exploits they were looking for. Their relationship with VUPEN continued to frustrate them for years. Towards the end of 2012, CitizenLab released their first report on Hacking Team's software being used to repress activists in the United Arab Emirates. However, a continuing stream of negative reports about the use of Hacking Team's software did not materially impact their relationships. In fact, by raising their profile these reports served to actually bring Hacking Team direct business. In 2013 Hacking Team's CEO stated that they had a problem finding sources of new exploits and urgently needed to find new vendors and develop in-house talent. That same year they made multiple new contacts, including Netragard, Vitaliy Toropov, Vulnerabilities Brokerage International, and Rosario Valotta. Though Hacking Team's internal capabilities did not significantly improve, they continued to develop fruitful new relationships. In 2014 they began a close partnership with Qavar Security.

The rest of the article is a loosely ordered recollection of Hacking Team's relationships and correspondences with various 0day providers.

Vitaliy Toropov

Vitaliy Toropov is a Russian freelance exploit developer. He approached Hacking Team in October of 2013 and offered to sell them exploits for various browser components.

Business model: Vitaliy is a freelancer that sells his own exploits and is not incorporated. He has reported dozens of bugs, primarily in browser components, to iDefense's Vulnerability Contributor Program and HP's Zero Day Initiative since 2011. It's unclear how many 0day exploits he has sold outside of public reporting programs, but a steep dropoff in his reports towards the end of 2013 might indicate the beginning of his undisclosed sales. Though he sold to Hacking Team directly, there are a number of indications that he also sold exploits through Netragard's Exploit Acquisition Program: the description for CANDLESTICK-BARNES is identical to Vitaliy's description of his Flash exploits to Hacking Team.

Pricing: Vitaliy sold multiple Flash exploits to Hacking Team on a non-exclusive basis for a relatively cheap $35-45K. He priced exploits sold on an exclusive basis at about three times as much as on a non-exclusive basis, indicating that his non-exclusive exploits are likely frequently resold. Other vendors did not seem to offer such steep discounts for non-exclusive exploit sales, for example Vulnerabilities Brokerage International only offered a 20% discount for one non-exclusive exploit for Firefox. However, it's difficult to gauge the relative resale popularity of exploits for Firefox and Flash.

Acceptance testing: For their first purchase, Hacking Team had a three-day evaluation period during which a Flash 0day could be tested to make sure it reliably worked against the advertised targets. Hacking Team originally proposed to fly Vitaliy to Milan to be present for the testing; however, he assumed good faith on their part and allowed them to test the exploit remotely. They continued this arrangement for their future sales.

Payment structure: The payment terms for Vitaliy's first two exploits followed approximately a 50%/25%/25% split. He would be paid 50% upfront, and then 25% for the next two months, assuming the vulnerability was not patched. Before he sold his third exploit he intended to change his payment model so that he would be paid 100% up-front and provide a replacement exploit if his sale was patched within two months. But because of miscommunication and Hacking Team's wariness to embrace a new payment scheme that did not ensure a warranty, his payments were split.

Exploits: Vitaliy's initial portfolio, which he presented to Hacking Team towards the end of 2013, consisted of three Flash RCEs (2 UaFs, 1 32-bit only integer overflow), two Safari RCEs (one only affected older versions of OS X/iOS), and a Silverlight RCE. Hacking Team asked whether Vitaliy had any privilege escalations or sandbox escapes didn't present any for the duration of their relationship. Hacking Team exclusively purchased Flash exploits from Vitaliy. The following table lays out a timeline of his sales:

Date	Name	CVE	Price and Payment Structure	Notes
10/28/13	FP1	2015-0349	$45k $20k/ $15k/$10k monthly	This use-after-free was the first exploit Hacking Team purchased from Vitaliy. It targeted Flash on both OS X and Windows and they were very happy with the quality, mentioning that it supported continuation of execution and executed quickly, in

Date	Name	CVE	Price and Payment Structure	Notes
				contrast to the quality they were used to from VUPEN. It was patched in April 2015.
1/2/14	FP2	2015-5119	$40k $20k/ $10k/$10k monthly	This exploit was another use-after free targeting both OS X and Windows. In fact, the vulnerability trigger was so similar to FP1 that it triggered the discussion noted here. This bug was undiscovered until the Hacking Team archive was leaked.
4/16/15	FP3	?	$39k 60%/20%/20% monthly	After FP1 was patched, Hacking Team wanted to purchase a second exploit to have on hand in case another one of their exploits was patched. Vitaliy's catalog at the time included three vulnerabilities, and they chose FP3. Vitaliy wanted to change the payment structure to be paid 100% upfront but the discussion fell through Within a month of the exploit being sold, the vulnerability was patched.
5/13/15	FP4	2015-5122	Free!	Because FP3 was patched within the warranty period, Vitaliy provided a free exploit replacement. This bug was undiscovered until the Hacking Team archive was leaked.

Adobe security: There was an amusing exchange between Vitaliy and Hacking Team after Vitaliy sold them two exploits with very similar vulnerability triggers. Hacking Team was concerned that when one bug got patched, Adobe would also fix the other, and that both of their purchases would be lost. However, Vitaliy claimed that Adobe's security response was very poor and that in his experience they never found similar bugs. Indeed, Adobe fixed one of the bugs (CVE-2015-0349) in April but did not find the second one (CVE-2015-5119) until Hacking Team's e-mail archive was released.

Netragard

Run by Adriel Desautels, Netragard is an information security consultancy and exploit broker that acts as the middleman between buyers and sellers. Hacking Team first made contact with Netragard in July 2011, but they did not establish a working relationship until October 2013. Adriel Desautels claims to have been brokering exploits since 1999. He shut down the Exploit Acquisition Program following the Hacking Team compromise.

Customer base: Netragard's Exploit Acquisition Program claimed to be only for US-based buyers; however, Hacking Team used Alex Velasco's CICOM USA as their US-based proxy with Netragard's knowledge and consent. After Hacking Team's relationship with CICOM USA soured, Adriel dealt directly with Hacking Team and in March of 2015 wrote, "We've been quietly changing our internal customer policies and have been working more with international buyers ... We do understand who your customers are both afar and in the US and are comfortable working with you directly." Despite this, e-mails from February 2015 discussing Luxembourg's (code name CONDOR) desire to buy exploits explicitly state that Netragard would not sell outside the US, indicating that they would not serve Hacking Team's international customers directly, but might be willing to work with Hacking Team as the intermediary.

Buyer contract: The buyer contract signed between Netragard and Hacking Team's US-based representative is available here. It lays out the standard legal boilerplate as well as some interesting terms about payment structure (§2), delivery and acceptance (§3), warranty (§5), indemnity (§8), and non-solicitation (§7). Exploits sold for less than or equal to $40k are payable at once after a month, otherwise they're split 50%/25%/25%. Payments are pro-rated if the vulnerability is patched before payments are complete. Interestingly, the contract includes a one-year non-solicitation period for Netragard's exploit developers after the contract has expired, though Netragard is not obliged to share their identities.

Catalogs: Submissions to the Exploit Acquisition Program were e-mailed out to Netragard's clients, the following is a list of exploits sourced from their catalog:

Date	Exploit notes
03/11/14	• SPEEDSTORM 3 ($215k exclusive): Flash across all browsers and Win7, 8, or 8.1 w/ sandbox escape. Modified version of HIGHWOOD used to bypass sandbox (sandbox bypass alone has sold for $120k non-exclusive.) Found via manual audit, 'reaching through fuzzing should be impossible'
04/23/14	• NEONNIPPLE: Office 2007, Word + Excel, required ActiveX control, required user interaction (going to Edit menu) • MUPPET-GRANT: IE 11 UaF, only accessible via Word via SMB/WebDAV • PEEDSTORM-KONROY: Flash bug w/ sandbox escape, targets XP/7, no Win8 or Chrome support (~80% reliability), uses modified MOHNS to bypass sandbox. Found via manual audit, 'reaching through fuzzing should be impossible' • Marshmallow: Win7 LPE • CANDLESTICK-BARNES: Flash, Win + OSX, 7-year old UaF (Likely written by Vitaliy Toropov, the description closely matches the one here.) • STARLIGHT-MULHERN: Adobe Reader XI + sandbox escape, mem disclosure + corruption, modified HIGHWOOD used to bypass sandbox (doesn't use JS or Flash)
05/28/14	• NARCOPLEX: Ammyy Admin v3.3 and 3.4, client-side bug • STIKA ($80k, non-exclusive): Netgear RCE, exploitable via CSRF
06/06/14	• HIGHWOOD-MONHS ($90 non-exclusive): Win XP through 8 LPE • STARLIGHT-MULHERN ($90k non-exclusive): Mentioned before
08/20/14	• BACKPAIN-FUN ($100k): Multi-OS Flash SOP bypass
09/24/14	• DIGIEBOLA ($50k): Flash auth bypass, 'allows Flash apps on any website to access and modify Local Shared Objects belonging to any website' allows changing mic/camera settings for any website
03/01/15	• codebyte-001: Flash Win7/8 RCE
03/03/15	• REDSHIFT ($105k): Win 7/8 Flash RCE + sandbox bypass w/ SMEP/PXN bypass & Win 8.1 CFG bypass (!) and continuation of

Date	Exploit notes
	execution
03/05/15	• jkw1 ($25k): Oracle RAC/CRS pre-auth root RCE, requires 1521 (SQLNet) connection, not mem corruption, logic flaw + input validation
03/27/15	• HastyLizard: QNAP NAS RCE, exploitable via CSRF, logic flaw
04/07/15	• TOAD: Win7/8, 2008/2012 server office 2013 SP1/2010 SP2/2007 SP3 client side. Requires WebDAV/SMB load, dll hijacking
04/21/15	• edubp06: Windows Media Center client-side
04/21/15	• CODEMONKEY: Changes local OS X password
04/24/15	• edubp08: Win7/8, 2008/2012 server OLE client-side, exploitable via Office/Wordpad, required user interaction
04/24/15	• edubp09: Win7/8 Word ActiveX IE/Office Web Components (w/o Office?) client-side
04/30/15	• edubp10 ($80k): Win7/8 IE11 RCE, requires click on page or running renderer via MS Word. Bug chain using 5-7 bugs. Good description of some bugs in the chain, might be possible to reverse engineer. Even more details.
05/19/15	• edubp12: Microsoft Paint accessed via SMB/WebDAV, requires user to hit Save As, useless bug

Purchasing history: In June of 2014, Hacking Team expressed an interest in purchasing STARLIGHT-MULHERN, an Adobe Reader XI client-side with optional sandbox bypass (HIGHWOOD) integrated. The original stated price was $100k, but it was eventually purchased for $80.5k. It appears that this was without the HIGHWOOD sandbox bypass since another email indicates that HIGHWOOD sells non-exclusively for closer to $90-$120k, but it's unclear whether this is the case from the emails archive.

During the testing of the exploit, Hacking Team discovered that the exploit did not work on Windows 8.1/x64. After some discussion with Netragard, Hacking Team was reminded that Windows 8.1 support was not in the original exploit specification. The developer offered to develop a new capability against Windows 8.1 for an additional $30k, a discount over the standalone price of such a technique. It does not appear that Hacking Team took the developer up on that offer. This vulnerability was patched in May of 2015.

Hacking Team briefly considered purchasing REDSHIFT for Luxembourg (code name FALCON); however, they decided to purchase another exploit from Vitaliy, presumably because it was less than half the proposed cost and also supported OS X.

iOS exploit pricing: Adriel stated he was supply-constrained for iOS RCE exploits because exploit developers frequently had their own connections to sell them, and that he believed that such exploits were overpriced. An exclusive exploit sale could cost as much as half a million dollars, but Adriel said he had sold them non-exclusively in the past and the price would be more palatable.

Qavar

In April of 2014, Hacking Team attended the SyScan conference in Singapore with the intention of recruiting new exploit developers. They believed that 0day vendors like VUPEN purchased most of their exploits, and simply passed on higher costs. By contacting researchers directly, they could get lower prices and more easily direct their research towards Hacking Team's priorities. They succeeded in making contact with several researchers interested in working with them, including Eugene Ching. Eugene demonstrated a proof-of-concept that impressed their offensive security team. Eugene expressed an interest in leaving his position at D-crypt's Xerodaylab and founding a company. Hacking Team was interested in purchasing their output.

By August of 2014, Eugene had founded his new company, Qavar Security Ltd, and entered a consulting agreement with Hacking Team. Their contract specified that the purpose of his work was “improving the analysis of vulnerabilities in order to better [...] RCS.” The contract term was for a year, and specified compensation of $80K SGD (~$60k USD.) The contract also specified a three-year non-compete and non-solicitation. Eugene began productionizing his Windows local privilege escalation PoC to work within Chrome and Internet Explorer's sandboxes. For that exploit, Eugene needed a kernel infoleak to bypass KASLR from within Chrome's restrictive sandbox and he was quoted $20k SGD by a Singaporean contact for such an infoleak. It's unclear if he purchased it or developed his own. A back-up (original email) of this exploit dated from January 2015 targeted 64-bit Windows 8.1 and included an info leak.

After several months of development, in April of 2015 Eugene was ready to deliver his exploit targeting 32- and 64-bit versions of Windows up to 8.1 to Hacking Team. Eugene was given a $30k SGD (~$20k USD) bonus for this deliverable. Eugene offered to sell a VLC exploit; however, the trigger used a playlist which wouldn't normally be opened with VLC, so he began to develop another VLC exploit targeting videos.

Interestingly, Eugene's responsibility with the Singaporean Army, presumably for his mandatory service, is to test and fix 0day exploits that they purchase.

VUPEN

VUPEN Security is an international exploit developer and broker. Its relationship with Hacking Team dates back to at least 2009 when the original contract negotiation was for both Hacking Team’s information security consultancy and government surveillance businesses. VUPEN provides 0day, but they also provide an archive of exploits and proof-of-concepts for older vulnerabilities and these older exploits made up the bulk of Hacking Team's purchases.

Distrust: Hacking Team's early experiences with VUPEN were frustrating, they received exploits that only targeted uncommon, old, or very specific software configurations. Though they negotiated cross-promotion clauses in their 2011 contract their relationship did not significantly improve. Hacking Team complained that, despite VUPEN's high-profile presentations and exploits for Pwn20wn, they did not get any of those high-caliber exploits and they had to reassure customers who demanded similar capabilities. They were wary of VUPEN's intimate relationship with their competitor, Gamma International, and set out to find new 0day vendors. Hacking Team claimed to know the specifics of an agreement between VUPEN and their competitor Gamma - that gave Gamma access to a constantly restocked set of 0days. VUPEN claimed that high-quality exploits cost approximately $100k each, and that it wasn't worth selling them to Hacking Team's customers for $50k.

They discussed renegotiating their contract, but both parties had reasons for distrust. Moreover, Hacking Team had been stung by using generic payloads from VUPEN's exploits. A Kaspersky report that claimed to have been monitoring a payload used by Hacking Team actually traced a staging payload used in some of VUPEN's exploits; it had actually implicated multiple actors, including Hacking Team. Hacking Team's CTO claimed that VUPEN "burned" their (presumably unsold) vulnerabilities after a set period of time to move the exploit market; putting their deployments in jeopardy.

Mobile: VUPEN offered several different remote code execution and local privilege escalation exploits for Android; however, not all of them were 0day and Hacking Team deemed that the prices were too high to purchase. Though there was interest in purchasing exploits for iOS, VUPEN said they were limited to certain customers, presumably high-paying government agencies.

Vulnerabilities Brokerage International

Run by Dustin Trammel, also known as I)ruid, VBI is an exploit broker. The first indications of the relationship between Hacking Team and VBI date back from August of 2013, but there is no evidence of how or when their relationship was established. It does not appear that Hacking Team purchased any exploits from VBI; however, they did begin negotiations for some exploits.

Exploit portfolios: VBI regularly sent portfolio updates to its customers. Though they were encrypted, Hacking Team's habit of forwarding encrypted messages unencrypted means that many of them are accessible. Several of these forwards included a PDF with VBI's entire exploit portfolio as I discussed in another post. The following is a table of their cleartext portfolio updates:

Date	Notes
08/19/13	ASUS BIOS device driver LPE, Firefox RCE added
10/14/13	PDF, McAfee EPO no longer brokered (purchased by VBI), Windows LPE added
10/28/13	PDF, PHP remote sold
11/25/13	2 McAfee EPO LPEs added
02/24/14	PDF, "Apple iOS Remote Forced Access-Point Association"/"Apple iOS Remote Forced Firmware Update Avoidance" no longer available, OpenPAM (used on BSDs) LPE added
03/31/14	PDF, Adobe Reader client-side (w/o sandbox escape), Windows LPE added
10/06/14	PDF, Solaris SunSSHD RCE, OS X LPE added

Relationship timeline: Hacking Team's began to negotiate a purchase from VBI in December of 2013. The exploit, VBI-13-013, was for a Windows local privilege escalation that could be used to bypass application sandboxes. It was to be sold on an exclusive basis for $95k (with commission), negotiated down from the original price of $150k. The purchase included a two-week long testing and validation period and the payment structure was such that Hacking Team would pay 50% up front, including four payments of 12.5% of the total amount over the next four months. Despite the extended negotiation, there are indications that Hacking Team did not eventually purchase this exploit. First, communications about the exploit fell off before testing began and did not seem to pick back up, and second, though the sale was to be exclusive, it was listed as still available in later updates.

Hacking Team expressed interested in a pair of exploits, VBI-14-004 and VBI-14-005, targeting Adobe Reader and the Windows kernel for a sandbox escape, until they learned they cost approximately $200k combined.

Lastly, Hacking Team began to negotiate purchasing VBI-14-008, an exploit for Firefox, in December of 2014. They primarily wanted to repurpose it to target Tor Browser (which is built on top of Firefox Extended Support Release) but were also interested in greater browser coverage and avoiding exposing a privilege escalation. The exploit was priced at $105k for exclusive use, and $84k for non-exclusive use before any negotiation. In the end the discussion dragged out for too long and it was sold to another party.

Rosario Valotta

Rosario is an Italian security researcher with specializations in browser security and fuzzing. His relationship with Hacking Team dates back to at least May of 2013 when he was fuzzing browsers on the side for them. He focused primarily on test case generation as he was not experienced at writing productionized exploits. During this time he primarily focused on fuzzing SVG, XSLT, and XPath. He was paid $3.5k EUR per month, until he ended his contract in January of 2014 because of family issues. He approached Hacking Team several times after the termination of his contract, offering to sell them a fuzzed Internet Explorer test case and exclusive rights to the Fileja fuzzer before its released at Syscan360.

Fuzzer results: Though Rosario's fuzzers found numerous crashing test cases, like most fuzzer outputs few of them appeared exploitable. One of the first crashes that looked exploitable was an IE10 memory corruption that was patched within a week of its discovery. Soon after, Rosario found a Firefox crash that looked exploitable but only appeared to occur under memory pressure. Despite months of analysis, Hacking Team was unable to turn this into a working exploit. It was discovered in October of 2013 and VUPEN used the same bug to win Pwn2Own in May of 2014.

Lastly, in February of 2015 after his contract ended, Rosario offered Hacking Team a crashing IE11 test case but it appears they were unable to exploit it despite months of effort. It does not appear that Hacking Team purchased it from Rosario despite their effort, and the vulnerability was patched as MS15-065 after the Hacking Team archive was released.

The following is a non-exhaustive list of e-mails with crashing test cases attached for various browsers: 1 2 3 4 5 6 7

COSEINC

COSEINC is a Singapore-based information security consultancy and 0day vendor. COSEINC founder, Thomas Lim, also ran and organized the SyScan security conference before it was sold to Qihoo 360. Hacking Team inquired about purchasing exploits from COSEINC as early as 2013; however, they did not appear to be interested in the IE9 exploit offered at the time. Thomas Lim offered to sell Hacking Team several bugs after their attendance at SyScan 2014; however, he did not want to discuss the sale over the phone or within Singapore (an OPSEC mindset that Hacking Team ridiculed.) After negotiating a third-party country to meet in, Hacking Team received (note: working attachments here) a list of exploits Thomas was willing to sell. Two were for old, patched bugs, and the third, an IE low-to-medium integrity privilege level escalation, was exorbitantly priced at $500k SGD ($360k USD). These offers give the appearance that COSEINC was primarily interested in offloading old or overpriced bugs to Hacking Team.

Miscellaneous

- Ability Ltd

Ability Ltd is an Israeli corporation focusing on interception and decryption tools. Ability's founder, Anatoly Hurgin, approached Hacking Team in January of 2013 to discuss reselling RCS to a customer to whom he could not resell NSO's surveillance software because of NSO's political commitments. He returned in December of 2014 to offer Hacking Team an OS X-specific Flash exploit with an OS X sandbox escape; however, Hacking Team deemed it to be too expensive. No record was found of the stated price.

- DSquare Security

DSquare Security sells CANVAS exploit packs targetted towards penetration testers. Hacking Team purchased the Exploitation pack in 2009, but quickly realized that the penetration testing focus did not suit their business.

- Keen Team

Keen Team, a Chinese security group, met Hacking Team at SyScan 2014 and Hacking Team expressed an interest in purchasing exploits from them. Though Hacking Team initiated a conversation with them, no record was found of Keen Team offering to sell them any.

- LEO Impact Security

In a particularly amusing episode, Hacking Team came into contact with Manish Kumar of LEO Impact Security and appears to have purchased a fake Microsoft Office exploit in spite of his questionable credentials. Unfortunately, I could not find a record of how much they paid.

- Security Brokers

Security Brokers, an Italian company founded by Raoul Chiesa, brokers 0day exploits. Hacking Team did not contact them because they believed it was sketchy and the Hacking Team CEO called Raoul his 'ex-friend' because he had worked with a competitor.

Conclusions

Security takeaways: The exposure of pricing and vulnerability information gives the information security community a valuable trove of data to find undiscovered vulnerabilities and corroborate our intuitions about the effectiveness of security controls. Though some common software, like browsers and operating system kernels, is far too large and complex to allow one to find the specific vulnerabilities described by 0day vendors, this does not hold for all of the vulnerabilities they advertised. For example, the extensive portfolios advertised by Vulnerabilities Brokerage International include some vulnerabilities with narrow-enough scopes to allow auditors to search for them, e.g. SunSSHD remote roots or an OpenPAM local privilege escalation.

After combing through the Hacking Team archive, there are two points that stuck out to me on the topic of corroborating commonly held security intuitions. Firstly: the rumors about high-priced 0days for iOS have been bolstered by the numbers quoted by vendors and the exclusivity with which they consider them. (This is not surprising given the widely-spread rumors about iOS 0day-exploit chains fetching over a quarter million dollars each, but it's reassuring knowing that their exclusivity puts them out of range of second-rate surveillance contractors like Hacking Team.) Secondly: given Java's notoriously poor security track record and the subsequent initiatives by browser vendors to disable Java or relegate it to click-to-play status, it's encouraging to see that there were no click-to-play bypasses offered to Hacking Team. They might well exist, but they don't appear to be common; this offers a convenient path forward for browser vendors to enact a widespread shutdown of Adobe Flash next.

Notoriety and Wassenaar: Notoriety has come with limited consequences for Hacking Team. Some of their customers are wary of being targeted for inclusion in tell-all reports that might bring political consequences. The inclusion of 'intrusion software' in the recently proposed changes to the Wassenaar Arrangement is a direct consequence of the backlash against surveillance companies like Hacking Team and Gamma International selling their products to repressive regimes. However, the overall picture for Hacking Team hasn't considerably changed despite the negative publicity and the implementation of the new changes to the Wassenaar Arrangement in the EU. Italy granted Hacking Team carte blanche for exporting their products, sales have continued to increase, and their 0day vendors have not deserted them. Given America's long history of supporting repressive allies in the Middle East and elsewhere, I am skeptical that the implementation of the proposed BIS rules would actually prevent the transfer of such technology to repressive governments. Efforts to shame and regulate Hacking Team have been unsuccessful so far; governments efforts to improve worldwide security would be more effective at thwarting Hacking Team and their ilk than Wassenaar.

Correction 7/22/15: I've restated the Keen Team section to make it clear that Hacking Team solicited them, not the other way around.

Update 7/23/15: Clarified Hacking Team's second-rate 0day market access, expanded wording about healthy skepticism about stated exploit prices, added ReVuln to misc. section

Published on 22 Jul 2015