UNCLASSIFIED

BRIEFING NOTE

EXPORT CONTROL ISSUES

STRATEGIC OBJECTIVES

- Obtain an assessment of the respective Ottawa 5 (O5) countries on using the export control regime to limit cyber proliferation.

- Share Canada's assessment of the use of the export control regime to limit cyber proliferation.

BACKGROUND

The principal objective of export controls is to ensure that exports of certain goods and technology are consistent with a country's foreign and defence policies. In Canada, export controls seek to ensure that Canadian exports:

- do not cause harm to Canada and its allies;
- do not undermine national or international security;
- do not contribute to national or regional conflicts or instability;
- do not contribute to the development of nuclear, biological or chemical weapons of mass destruction, or of their delivery systems;
- are not used to commit human rights violations; and
- are consistent with existing economic sanctions' provisions.

Items in Canada that are subject to export control restrictions are listed in the Export Control List. The List includes items such as munitions, dual use technologies (e.g. nuclear technology) and chemical and biological agents. Most items on the Export Control List derive from Canada's commitments to like-minded countries which participate in multilateral export control regimes or from Canada's obligations as a signatory to multilateral or bilateral international agreements. The export of other types of goods and certain activities may also be subject to United Nations trade sanctions or arms embargoes against particular countries or regions.

The Department of Foreign Affairs and International Trade leads on export control issues, with the support of a number of other organizations such as the Department of National Defence, Natural Resources Canada and Public Safety Canada.

CURRENT STATUS

Certain cryptographic and advanced computing technologies are restricted under the list. In general, and absent trade sanctions, computer tools that could be used for cyber espionage or cyber attack are not subject to export controls in Canada or in any of the Five Eyes countries. Companies in O5 countries are free to trade in these goods so long as the trading partner is not subject to existing trade sanctions, such as Iran.

CONSIDERATIONS

O5 countries may want to add restrictions to trading in computer vulnerabilities and tools to their export control lists for two reasons:

1. Doing so limits the proliferation of advanced cyber tools that could be used against the Five Eyes for intelligence or offensive purposes; and

2. Doing so may also make it more difficult on those countries looking to filter Internet content and monitor dissidents.

There is a growing market for the trade of hardware and software vulnerabilities and the tools used to exploit them. Intelligence agencies, organized crime groups, and individual computer security experts discover vulnerabilities and either exploit them for their own purposes or sell them to the highest bidder. These could be used against the Five Eyes. Media reports indicate that zero-day exploits, a tool that exploits a previously unknown vulnerability, can sell for six figures. Leading companies in this market include VUPEN (France) and Gamma International (United Kingdom).

There are burgeoning international efforts to restrict the sale of these technologies. However, they are primarily aimed at preventing human rights abuses given that cyber espionage tools and Internet monitoring technologies can be used to restrict free expression. In October 2012, the European Parliament endorsed amendments to the current European Union export control regime of dual-use items and technology to prevent European technologies from being used in ways which violate human rights. Similarly, the United States Congress is considering legal measures to prevent American companies from abetting foreign governments' capacity to restrict citizens from freely expressing their opinions or sharing information online.

In Canada, Netsweeper, a company from Guelph, Ontario, provides web monitoring and content filtering services. Human rights organizations and civil society groups have criticized it in the past for providing tools and services to countries with poor human rights records.

Adding cyber tools to the export control list in Canada

The idea of restricting the export of advanced cyber tools has not been fully explored in Canada and would require consultation within and outside government. Some of these tools have legitimate uses, such as helping parents control what their children can access online. Before adding any items to Canada's export control list, officials would require more details on what specific tools would be restricted and for what purpose.

TALKING POINTS

Assessment from O5 countries on export control

- What are your views on the use of export control to limit the proliferation of advanced cyber tools?
- What specific tools are you looking to limit?

Canada's assessment of export control to limit cyber proliferation

- We would be open to considering the use of export control to limit cyber proliferation.
- That said, we have not conducted a full assessment of the issue.
- There are some key questions that we have yet to answer.
    - Are we restricting these tools so that they are not used against us, to prevent human rights abuses, or both?
    - What specific tools are we looking to restrict?
- Michael, do you have anything else to add?

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: May-14-13 11:56 AM
To: Durand, Mathieu; Dyer, Lara
Cc: Chayer, Marie-Helene
Subject: FW: news story on US government role in zero-day market

Interesting article (starts about halfway down page) on computer exploits and law enforcement's role in development/purchasing/deployment.

Maciek

From: [redacted]
Sent: May-14-13 10:53 AM
To: info
Subject: news story on US government role in zero-day market

[redacted] ***Cyber Security Forum***

Here's a link to a fascinating and important Reuters news story about the US government being the biggest buyer of zero-day exploits – but not always spreading the word about known software flaws:

http://in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510?type=economicNews

The inherent conflicts of interest at play here are sobering, to put it mildly.

[redacted]

Emmett, Jamie

From:
Sent: October-16-13 10:27 PM
To:
Subject: !!! The NSA's New Risk Analysis

Please find an excellent and incredibly interesting article on NSA's infection techniques by Bruce Schneier --

"Here are the FOXACID basics: By **the time the NSA tricks a target into visiting one of those servers, it already knows exactly who that target is, who wants him eavesdropped on, and the expected value of the data it hopes to receive**. Based on that information, the server can automatically decide what exploit to serve the target, taking into account the risks associated with attacking the target, as well as the benefits of a successful attack. **According to a top-secret operational procedures manual provided by Edward Snowden**, an exploit named Validator might be the default, but the NSA has a variety of options. The documentation mentions United Rake, Peddle Cheap, Packet Wrench, and Beach Head -- all delivered from a FOXACID subsystem called Ferret Cannon. Oh how I love some of these code names. (On the other hand, EGOTISTICALGIRAFFE has to be the dumbest code name ever.)"

"**If the target is a high-value one, FOXACID might run a rare zero-day exploit that it developed or purchased. If the target is technically sophisticated**, FOXACID might decide that there's too much chance for discovery, and keeping the zero-day exploit a secret is more important. **If the target is a low-value one**, FOXACID might run an exploit that's less valuable. If the target is low-value and technically sophisticated, FOXACID might even run an already-known vulnerability."

Whoa :-

From the latest CRYPTO-GRAM issue, FYI,

--

The NSA's New Risk Analysis

As I recently reported in the Guardian, the NSA has secret servers on the Internet that hack into other computers, codename FOXACID. These servers provide an excellent demonstration of how the NSA approaches risk management, and exposes flaws in how the agency thinks about the secrecy of its own programs.

Here are the FOXACID basics: By the time the NSA tricks a target into visiting one of those servers, it already knows exactly who that target is, who wants him eavesdropped on, and the expected value of the data it hopes to receive. Based on that information, the server can automatically decide what exploit to serve the target, taking into account the risks associated with attacking the target, as well as the benefits of a successful attack. According to a top-secret operational procedures manual provided by Edward Snowden, an exploit named Validator might be the default, but the NSA has a variety of options. The documentation mentions United Rake, Peddle Cheap, Packet Wrench, and Beach Head -- all delivered from a FOXACID subsystem called Ferret

Cannon. Oh how I love some of these code names. (On the other hand, EGOTISTICALGIRAFFE has to be the dumbest code name ever.)

Snowden explained this to Guardian reporter Glenn Greenwald in Hong Kong. If the target is a high-value one, FOXACID might run a rare zero-day exploit that it developed or purchased. If the target is technically sophisticated, FOXACID might decide that there's too much chance for discovery, and keeping the zero-day exploit a secret is more important. If the target is a low-value one, FOXACID might run an exploit that's less valuable. If the target is low-value and technically sophisticated, FOXACID might even run an already-known vulnerability.

We know that the NSA receives advance warning from Microsoft of vulnerabilities that will soon be patched; there's not much of a loss if an exploit based on that vulnerability is discovered. FOXACID has tiers of exploits it can run, and uses a complicated trade-off system to determine which one to run against any particular target.

This cost-benefit analysis doesn't end at successful exploitation. According to Snowden, the TAO -- that's Tailored Access Operations -- operators running the FOXACID system have a detailed flowchart, with tons of rules about when to stop. If something doesn't work, stop. If they detect a PSP, a personal security product, stop. If anything goes weird, stop. This is how the NSA avoids detection, and also how it takes mid-level computer operators and turn them into what they call "cyberwarriors." It's not that they're skilled hackers, it's that the procedures do the work for them.

And they're super cautious about what they do.

While the NSA excels at performing this cost-benefit analysis at the tactical level, it's far less competent at doing the same thing at the policy level. The organization seems to be good enough at assessing the risk of discovery -- for example, if the target of an intelligence-gathering effort discovers that effort -- but to have completely ignored the risks of those efforts becoming front-page news.

It's not just in the U.S., where newspapers are heavy with reports of the NSA spying on every Verizon customer, spying on domestic e-mail users, and secretly working to cripple commercial cryptography systems, but also around the world, most notably in Brazil, Belgium, and the European Union. All of these operations have caused significant blowback -- for the NSA, for the U.S., and for the Internet as a whole.

The NSA spent decades operating in almost complete secrecy, but those days are over. As the corporate world learned years ago, secrets are hard to keep in the information age, and openness is a safer strategy. The tendency to classify everything means that the NSA won't be able to sort what really needs to remain secret from everything else. The younger generation is more used to radical transparency than secrecy, and is less invested in the national security state. And whistleblowing is the civil disobedience of our time.

At this point, the NSA has to assume that all of its operations will become public, probably sooner than it would like. It has to start taking that into account when weighing the costs and benefits of those operations. And it now has to be just as cautious about new eavesdropping operations as it is about using FOXACID exploits attacks against users.

This essay previously appeared in the Atlantic.
http://www.theatlantic.com/technology/archive/2013/10/how-the-nsa-thinks-about-secrecy-and-risk/280258/ orhttp://tinyurl.com/nnmq8sm

NSA purchasing zero-day exploits:
http://www.zdnet.com/nsa-purchased-zero-day-exploits-from-french-security-firm-vupen-7000020825/ orhttp://tinyurl.com/of39n4a

NSA getting advance warning from Microsoft:
http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html orhttp://tinyurl.com/mvaew4f

TAO:
http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group orhttp://tinyurl.com/kcvk8hk

NSA abuses:
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order or http://tinyurl.com/qaynuex
http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security or http://tinyurl.com/m47p5dc
http://www.cbsnews.com/8301-202_162-57600928/report-nsa-spied-on-brazilian-mexican-presidents/ orhttp://tinyurl.com/lqqmauh
http://www.spiegel.de/international/europe/belgian-prime-minister-angry-at-claims-of-british-spying-a-923583.html orhttp://tinyurl.com/olfswq6
http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html or http://tinyurl.com/k64yqc3

Secrets are hard to keep:
http://www.reuters.com/article/2010/11/28/us-wikileaks-lessons-idUSTRE6AR38520101128 or http://tinyurl.com/q6crh7p
http://www.npr.org/templates/story/story.php?storyId=190756384

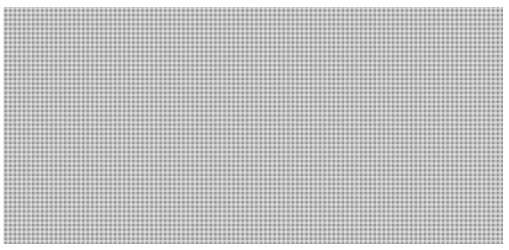
On openness as a strategy:
http://blog.ted.com/2013/01/24/why-radical-openness-is-unnerving-reshaping-and-necessary-a-qa-with-ted-ebook-authors-don-tapscott-and-anthony-d-williams/ or http://tinyurl.com/a4q5bsn

Overclassification:
http://www.nytimes.com/2013/08/04/sunday-review/a-washington-riddle-what-is-top-secret.html orhttp://tinyurl.com/kfay3cb

Generational issues in secrecy:
https://www.schneier.com/essay-449.html

Whistleblowing as civil disobedience:
http://www.zephoria.org/thoughts/archives/2013/07/19/edward-snowden-whistleblower.html orhttp://tinyurl.com/jwbcgom

--



Emmett, Jamie

From:
Sent: December-07-13 11:01 PM
To:
Subject: 0-day exploits: a few hypotheses

EXCELLENT posting by Thanks

Enjoy the reading and have a great weekend.

FYI,

--

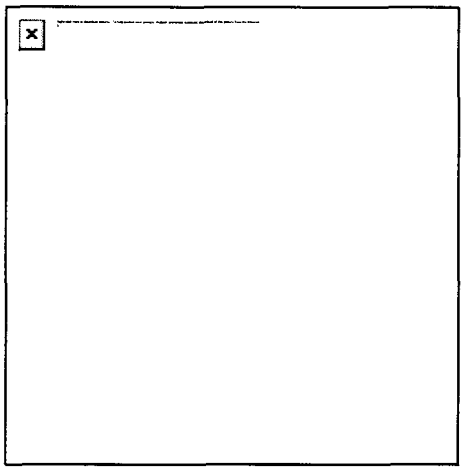
Begin forwarded message:

From:
Subject: Congetture sul numero di zeroday
Date: December 7, 2013 at 10:02:39 AM GMT+1
To: --

http://krebsonsecurity.com/2013/12/how-many-zero-days-hit-you-today/

How Many Zero-Days Hit You Today?

On any given day, nation-states and criminal hackers have access to an entire arsenal of zero-day vulnerabilities – undocumented and unpatched software flaws that can be used to silently slip past most organizations' digital defenses, new research suggests. That sobering conclusion comes amid mounting evidence that thieves and cyberspies are ramping up spending to acquire and stockpile these digital armaments.

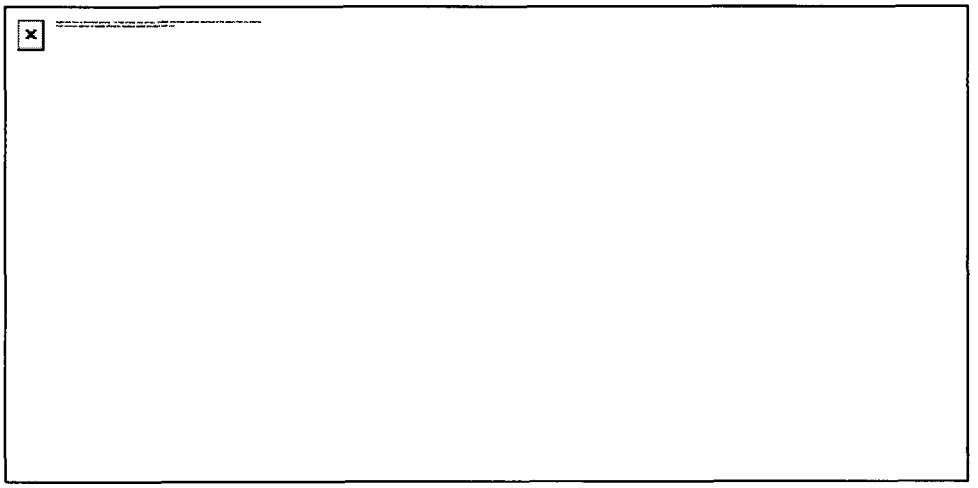


Security experts have long suspected that governments and cybercriminals alike are stockpiling zero-day bugs: After all, the thinking goes, if the goal is to exploit these weaknesses in future offensive online attacks, you'd better have more than a few tricks up your sleeve because it's never clear whether or when those bugs will be independently discovered by researchers or fixed by the vendor. Those suspicions were confirmed very publicly in 2010 with the discovery of Stuxnet, a weapon apparently designed to delay Iran's nuclear ambitions and one that relied upon *at least four zero-day vulnerabilities.*

Documents recently leaked by **National Security Agency** whistleblower Edward Snowden indicate that the NSA spent more than $25 million this year alone to acquire software vulnerabilities from vendors. But just how many software exploits does that buy, and what does that say about the number of zero-day flaws in private circulation on any given day?

These are some of the questions posed by **Stefan Frei,** research director for Austin, Texas-based NSS Labs. Frei pored over reports from and about some of those private vendors — including boutique exploit providers like Endgame Systems, Exodus Intelligence, Netragard,ReVuln and VUPEN – and concluded that jointly *these firms alone have the capacity to sell more than 100 zero-day exploits per year.*

According to Frei, if we accept that the average zero-day exploit persists for about 312 days before it is detected (an estimate made by researchers at **Symantec Research Labs**), this means that these firms probably *provide access to at least 85 zero-day exploits on any given day of the year.* These companies all say they reserve the right to restrict which organizations, individuals and nation states may purchase their products, but they all expressly *do not* share information about exploits and flaws with the affected software vendors.



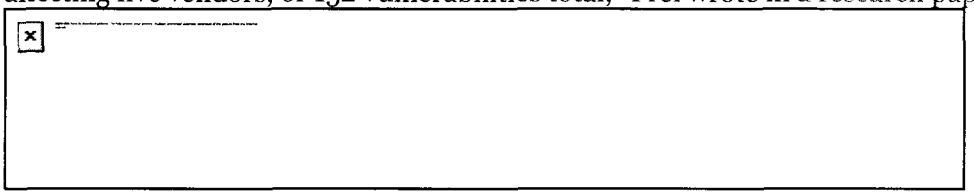
Frei's minimum estimate of exploits offered by boutique exploit providers each year.

KNOWN UNKNOWNS

That approach stands apart from the likes of **HP TippingPoint**'s Zero-Day Initiative (ZDI) and **Verisign**'s iDefense Vulnerability Contributor Program (VCP), which pay researchers in exchange for the rights to their vulnerability research. Both ZDI and iDefense also manage the communication with the affected vendors, ship stopgap protection for the vulnerabilities to their customers, and otherwise keep mum on the flaws until the vendor ships an update to fix the bugs.

Frei also took stock of the software vulnerabilities collected by these two companies, and found that between 2010 and 2012, the ZDI and VCP programs together published 1,026 flaws, of which 425 (44 percent) targeted flaws in **Microsoft**, **Apple**, **Oracle**, **Sun** and **Adobe**products. The average time from purchase to publication was 187 days.

"On any given day during these three years, the VCP and ZDI programs possessed 58 unpublished vulnerabilities affecting five vendors, or 152 vulnerabilities total," Frei wrote in a research paper released today.



Frei notes that the VCP and ZDI programs use the information they purchase only for the purpose of building better protection for their customers, and since they share the information with the software vendors in order to develop and release patches, the overall risk is comparatively low. Also, the vulnerabilities collected and reported by VCP and ZDI are not technically zero-days, since one important quality of a zero-day is that it is used in-the-wild to attack targets before the responsible vendor can ship a patch to fix the problem.

In any case, Frei says his analysis clearly demonstrates that critical vulnerability information is available in significant quantities for private groups, for extended periods and at a relatively low cost.

"So everybody knows there are zero days, but when we talk to C-Level executives, very often we find that these guys don't have a clue, because they tell us, 'Yeah, but we've never been compromised'," Frei said in an interview. "And we always ask them, 'How do you know?'"

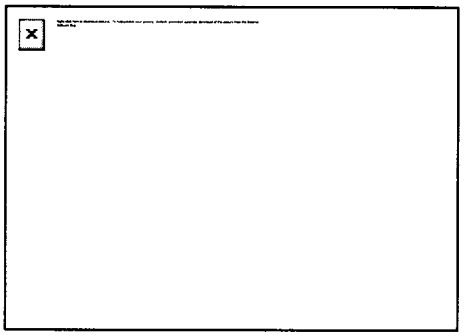
Frei said that in light of the present zero-day reality, he has three pieces of advice for C-Level executives:

- Assume you are compromised, and that you will get compromised again.
- Prevention is limited; invest in breach detection so that you can quickly find and act on any compromises.
- Make sure you have a process for properly responding to compromises when they do happen.

ANALYSIS

Although's Frei's study is a very rough approximation of the zero-day scene today, it is almost certainly a conservative estimate: It makes no attempt to divine the number of zero-day vulnerabilities developed by commercial security consultancies, which employ teams of high-skilled reverse engineers who can be hired to discover flaws in software products.

s.19(1)
s.20(1)(b)



Nor does it examine the zero-days that are purchased and traded in the cybercriminal underground, where vulnerability brokers and exploit kit developers have been knownto pay tens of thousands of dollars for zero-day exploits in widely-used software. I'll have some of my own research to present on this latter category in the coming week. Stay tuned. **Update, Dec. 6, 1:30 p.m. ET:**Check out this story on the arrest of the man thought to be behind the Blackhole Exploit Kit. He allegedly worked with a partner who had a $450,000 budget for buying browser exploits.

Original story:

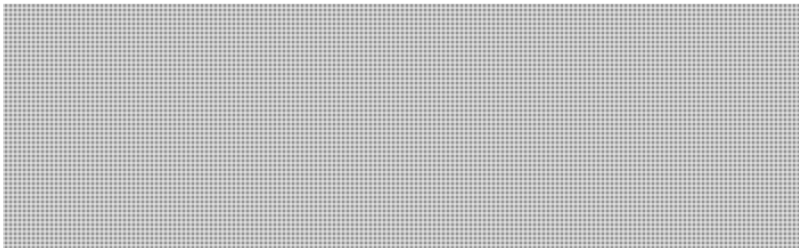
But Frei's research got me to thinking again about an idea for a more open and collaborative approach to discovering software vulnerabilities that has remained stubbornly stuck in my craw for ages. Certainly, many companies have chosen to offer "bug bounty" programs — rewards for researchers who report zero-day discoveries. To my mind, this is good and as it should be, but most of the companies offering these bounties — Google, Mozilla, and Facebook are among the more notable — operate in the cloud and are not responsible for the desktop software products most often targeted by high-profile zero-days.

After long resisting the idea of bug bounties, Microsoft also quite recently began a program to pay researchers who discover novel ways of defeating its security defenses. But instead of waiting for the rest of the industry to respond in kind and reinventing the idea of bug bounties one vendor at a time, is there a role for a more global and vendor-independent service or process for incentivizing the discovery, reporting and fixing of zero-day flaws?

Most of the ideas I've heard so far involve funding such a system by imposing fines on software vendors, an idea which seems cathartic and possibly justified, but probably counterproductive. I'm sincerely convinced that a truly global and remunerative bug bounty system is possible and maybe even inevitable as more of our lives, health and wealth become wrapped up in technology. But there is one sticking point that I simply cannot get past: How to avoid having the thing backdoored or otherwise subverted by one or more nation-state actors?

I welcome a discussion on this topic. Please sound off in the comments below.

--



Emmett, Jamie

From: [redacted]
Sent: December-16-13 10:35 PM
To: [redacted]
Subject: Dell Invests in 'Zero-day' Security Startup Invincea

"AUSTIN — **Dell Inc. is co-leading a $16 million investment in security startup Invincea Inc.** It already bundles the company's software on computers and tablets sold to businesses. **Invincea makes software that contains "zero-day attacks" — threats that exploit a previously unknown vulnerability in applications** — to prevent them from spreading to other computer software, said Jim Lussier, managing director of Dell Ventures."

VERY interesting article from today's WSJ/CIO Journal, FYI,
[redacted]

CIO Journal.
December 16, 2013, 6:58 AM ET

Dell Invests in 'Zero-day' Security Startup Invincea

By Clint Boulton

Reporter

AUSTIN — Dell Inc. is co-leading a $16 million investment in security startup Invincea Inc. It already bundles the company's software on computers and tablets sold to businesses. Invincea makes software that contains "zero-day attacks" — threats that exploit a previously unknown vulnerability in applications — to prevent them from spreading to other computer software, said Jim Lussier, managing director of Dell Ventures.

"You just can't keep up," with the security threats, Mr. Lussier said in an interview at Dell's customer conference here Friday. "It's a really big problem."

Co-led by Aeris Capital, the series C funding round is the latest investment made by Dell Ventures' $300 million Strategic Innovation Venture Fund, which the company announced here Thursday. Dell sees the fund as a strategic pillar of its reinvention as a private company. The fund will back startups developing new technologies in storage, cloud, analytics, mobility and security, and hopes to generate significant returns.

Invincea is Dell's latest bet. "If by working with us the company were to double… we get to participate in the upside that we helped to create," Mr. Lussier said.

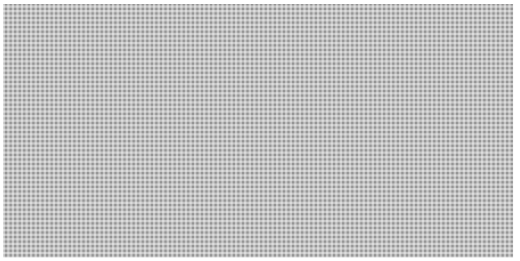
Traditional antivirus approaches involve detecting a virus and developing a patch to prevent it from spreading, said Mr. Lussier. But security threats are becoming more sophisticated and the very nature of zero-day attacks means no patches are available. When installed on computers, Invincea's FreeSpace software detects zero-day viruses in applications such as Microsoft Corp.'sMSFT +0.51% Office, Adobe Systems Inc.'sADBE -3.52% PDF Reader, and Web browsers, isolates the malware, and moves it to a virtual container to prevent it from spreading, Mr. Lussier said. Invincea targets spear-phishing, an email scam in which a sender pretends to be someone else to access sensitive data; drive-by download exploits, in which users unwittingly infect their computers by clicking on Web links or downloading apps infected with the virus; and watering hole attacks, in which perpetrators hack legitimate websites to spread malware to users.

Invincea, which said in a statement it will use the funding to expand in Europe, has roughly 10,000 customers across energy, high-tech, financial services, healthcare, retail and other sectors. Fairfax, Va.-based Invincea's roots lie in the federal government. While working as a program manager for cybersecurity systems for the Defense Advanced Research Projects Agency, founder and CEO Anup Ghosh developed Invincea's core technology as a virtual Web browsing solution. He commercialized the software as FreeSpace in 2009, according to the company's website.

Dell in June 2013 began bundling Invincea's software on its Latitude, OptiPlex and Precision tablets and PCs. Mr. Lussier said the bundle, good for one year from the time of purchase, will make its way onto 20 million computers over the next year.

Dell's innovation fund is ramping up. The company funded flash storage provider Skyera Inc. and cloud services specialist Mirantis Inc., earlier this year. Mr. Lussier said Dell has funded other startups, though he declined to name them to preserve "strategic" advantages in the market.

--



Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: December-19-13 3:51 PM
To: Dyer, Lara
Subject: RE: US task force on electronic surveillance releases report

Lara,

Below are the key points of the report on NSA practices released yesterday. In summary, the report proposes significant changes (46 in total) to the existing metadata collection powers. Critics of the NSA are calling the recommendations "strong", "ground-breaking", and "bold", and the recommendations are indeed far-ranging.

I have highlighted in bold those recommendations that directly or indirectly impact Canada (i.e. they reference what the US should do with allies, or, if the US adopts this, there may be an impact domestically).

Maciek

---

15 Key Findings and Recommendations of the President's Review Group on Intelligence and Communications Technology

1. The US Government must protect two different forms of security: national security, and the rights of citizens to be secure in their persons.

2. **Government should not be permitted to collect and store indefinitely metadata; the government should transition immediately to a system where such metadata is held by TSPs or a private third party.**

3. All requests to access this metadata (in fact, any request for personal information) should have some level of judicial authorization (i.e. separate judicial orders for each target).

4. **Government should commission a study assessing the distinction between metadata and other types of data.**

5. Detailed information about the parameters of each type of lawful access power should be made available to Congress annually.

6. **TSPs should have the authority to issue lawful access request statistics, including number of requests, rejections, types of information provided, etc. The Government should also disclose this data.**

7. Programs of the magnitude of PRISM should only be kept from the American public if it serves a compelling governmental interest and its release would substantially impair the program's efficacy.

8. **Non-US persons whose information is intercepted should be afforded the same privacy considerations as US citizens under the Privacy Act 1974, as is done by DHS.**

9. **Electronic surveillance must be used only to protect the national security of the US and its allies; it must not be used for illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries.**

10. **The US should support international norms and agreements that declare that governments should not use surveillance to steal industry secrets, manipulate financial systems, or require equipment point of presence in situ.**

11. Sensitive intelligence requirements (e.g. intercepting foreign head of state) should be set by the President and his/her security advisors, not the intelligence agencies, and be guided by specific considerations, such as the risk if discovered, alternative means of collecting the info, etc.

12. **The US and close allies should explore arrangements regarding intelligence collection practices with respect to each others' citizens. These arrangements should involve share NS objectives, close and honest relationships between senior officials, and operational cooperation.**

13. The independent Privacy and Civil Liberties Oversight Board should be strengthened to oversee the foreign intelligence activities of all intelligence agencies (would serve as recipient for whistleblower complaints, perform audits, and provide assessments of technology initiatives).

14. The NSA should stop undermining encryption, and no longer subvert or make vulnerable any generally available commercial software, and use "zero day" vulnerabilities (vulnerabilities discovered by the NSA but not shared with developers, giving them "zero days" to patch the vulnerability) sparingly and only on the basis of interagency agreement.

15. **The US should streamline the Mutual Legal Assistance Treaty process for sharing/receiving electronic communications with/from international partners.**

From: Dyer, Lara
Sent: December-19-13 1:22 PM
To: Hawrylak, Maciek
Subject: FW: US task force on electronic surveillance releases report

Please action. Tks.

From: MacDonald, Michael
Sent: December-19-13 12:16 PM
To: Dyer, Lara
Subject: RE: US task force on electronic surveillance releases report

Pls prepare me a quick overview summary of key points. thx

From: Dyer, Lara
Sent: December-19-13 10:27 AM
To: MacDonald, Michael
Subject: FW: US task force on electronic surveillance releases report

FYI

From: Hawrylak, Maciek
Sent: December-19-13 10:26 AM
To: Plunkett, Shawn; Emmett, Jamie; McKinnon, Korey; Thompson, Julie
Cc: Dyer, Lara
Subject: US task force on electronic surveillance releases report

FYI, the task force appointed by President Obama to investigate the practices of the NSA released its report yesterday.

An NY Times article reviewing the contents is here, while their editorial board came out against mass surveillance programs here.

Maciek

Emmett, Jamie

From: [redacted]
Sent: January-14-14 9:50 PM
To: [redacted]
Subject: Companies eye lucrative zero-days market

Please find another very interesting article on the 0-day market.

From today's FT, FYI,
[redacted]

January 14, 2014 2:54 pm

Companies eye lucrative zero-days market

By Chris Bryant in Frankfurt

Vupen, a French start-up that recently opened an office in Maryland, home also to the National Security Agency's headquarters, is one of a growing number of companies selling hacking tools, known as "zero days", to the intelligence community.

According to documents obtained via a freedom of information request in September by Muckrock, an open government news organisation, the NSA is one such customer. Chaouki Bekrar, Vupen chief executive, did not confirm this but told the Financial Times that his company "works exclusively with allied [Nato] countries" and it complies with the "most restrictive international regulations on technology exports".

He added: "Vupen is a start-up, other US companies such as Lockheed Martin, ManTech, Raytheon, and Harris are much bigger players in the computer network operations or computer network attack business."

ManTech, Harris and Lockheed Martin declined to comment. Raytheon's marketing materials boast that it is the "number one company in finding zero-day vulnerabilities". Raytheon declined to comment on how government or military customers use its research.

This is a potentially lucrative business, with the value of a zero day depending on how widely the software is used, whether the zero day is exclusive to the buyer and whether it can help penetrate a mobile device.

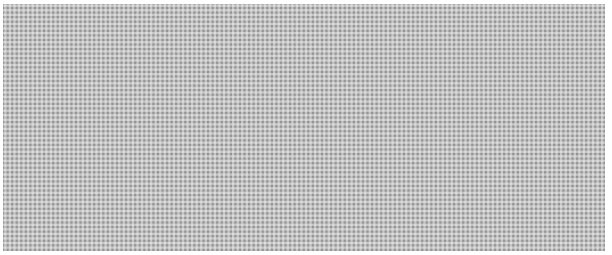
"There is no typical price. It can range from the low tens of thousands to the high hundreds of thousands," says Adriel Desautels, chief executive of Netragard, a zero-day broker that exclusively sells to US-based entities.

Governments must continually replenish their zero-day supplies because if a software vendor issues an update, a zero day can become useless.

"Even if you have the best arsenal of exploits right now, in six months to a year they won't exist any more. This fuels constant demand for fresh exploits," explains Mikko Hypponen, chief research officer at F-Secure, the Finland-based computer security company.

Pierre Roberge, founder of Arc4dia, a Quebec-based IT security company that recently left the business of selling zero days to intelligence agencies and police in order to focus on defensive IT works, said: "I really wanted to help law enforcement . . . But there's a pendulum and now it seems it has swung too much in the other direction. When you see what's been in the press [about state surveillance], you're like holy cow . . ."

--



s.19(1)
s.20(1)(b)

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: January-30-14 11:23 AM
To: Dyer, Lara
Subject: RE: PLEASE ADVISE: Q-234 - consultation

For this question, all agencies should be in a position to answer affirmatively or negatively, since it simply asks if they have these tools. The agencies may, however, wish to decline to answer.

Maciek

From: Dyer, Lara
Sent: January-28-14 4:42 PM
To: Hawrylak, Maciek
Subject: Fw: PLEASE ADVISE: Q-234 - consultation

Same, pls + tks.

From: Jacquard, Christina
Sent: Tuesday, January 28, 2014 04:40 PM
To: Dyer, Lara
Cc: Johnston, Shannon; Haeck, Kimberly; Kingsley, Michèle
Subject: FW: PLEASE ADVISE: Q-234 - consultation

Good afternoon Lara,

We received a second similar request.

Please see the below email and advise if ITTP would be in a position to respond to parts and/or lead in the coordination of responses.

Please respond to DGO by 10 am tomorrow morning. NIL response is required.

Many thanks,

Christina Jacquard
Administrative Assistant / Adjointe administrative
National Security Operations / Opérations de la Sécurité nationale
Public Safety Canada / Sécurité public Canada
Tel: (613) 990-2733

From: Dupuis, Chantal
Sent: Tuesday, January 28, 2014 4:32 PM
To: Hammerschmidt, Peter; Matz, Mark; Kingsley, Michèle
Cc: Viau, Julie; Johnston, Shannon; Jacquard, Christina; Haeck, Kimberly; Lamontagne, Samuel; Johnson-Moses, Cheryl; Anestis, Melanie; Bedor, Tia Leigh; Dupuis, Chantal
Subject: PLEASE ADVISE: Q-234 - consultation

Good afternoon,

Please see new written question Q-234 below regarding communications devices and services. We would need to determine who would be in the best position to respond to each part and/or a lead. Could you please advise (even if nil). It would be appreciated if you could get back to me by **noon tomorrow.**

With regard to tracking by government agencies of customers' usage of communications devices and services: do government agencies use their own (i) tracking products (e.g. "IMSI Catchers"), (ii) infiltration software (e.g. zero day exploits, malware such as FinFisher, etc.), (iii) interception hardware (i.e. placed within or integrated with a company's network)?

En ce qui concerne le suivi fait par les organismes gouvernementaux de l'utilisation, par les consommateurs, des services et des appareils de communication : les organismes gouvernementaux utilisent-ils leurs propres i) dispositifs de suivi (p. ex. les capteurs IMSI), ii) logiciels d'infiltration (p. ex. les exploits du jour zéro, des logiciels malveillants comme FinFisher, etc.), iii) dispositifs d'interception (p. ex. placés à l'intérieur du réseau d'une compagnie ou intégrés à ce réseau)?

Merci beaucoup, Chantal

Emmett, Jamie

From:
Sent: April-18-14 10:52 PM
To:
Subject: Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA

So there! J

Please find an interesting dispatch on 0-day vulnerabilities and the NSA.

From WIRED, FYI.,

Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA

By Kim Zetter 04.15.14 | 6:30 am

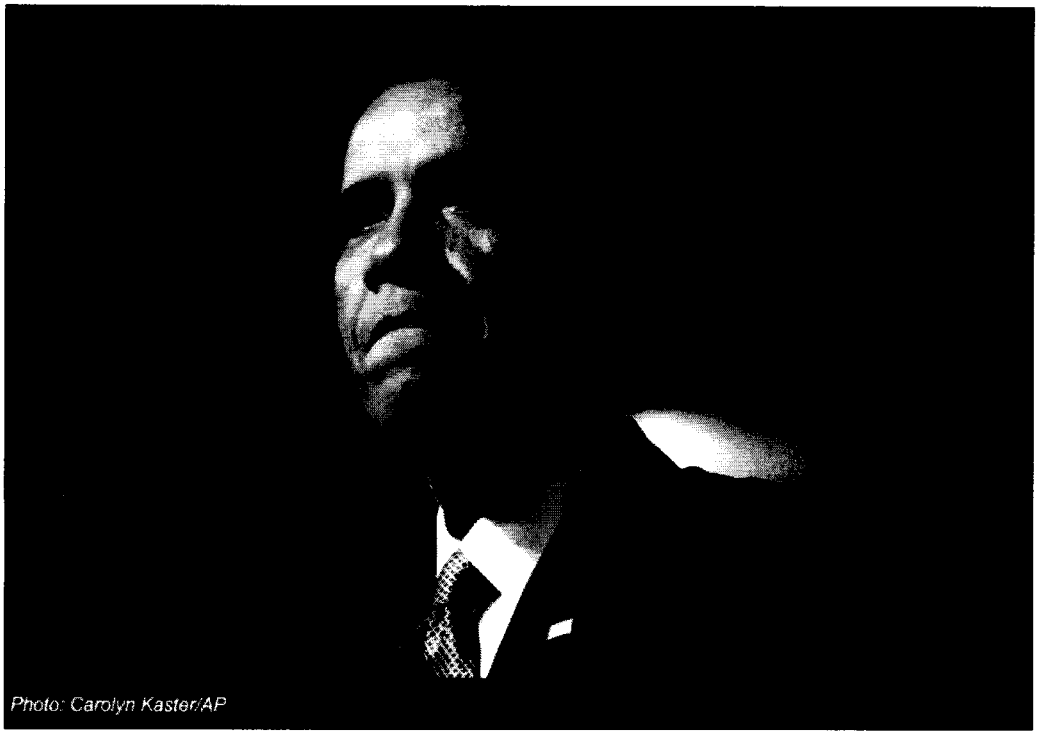


Photo: Carolyn Kaster/AP

After years of studied silence on the government's secret and controversial use of security vulnerabilities, the White House has finally acknowledged that the NSA and other agencies exploit some of the software holes they uncover, rather than disclose them to vendors to be fixed.

The acknowledgement comes in a news report indicating that President Obama decided in January that from now on any time the NSA discovers a major flaw in software, it must disclose the vulnerability to vendors and others so that it can be patched, according to the *New York Times*.

But Obama included a major loophole in his decision, which falls far short of recommendations made by a presidential review board last December: According to Obama, any flaws that have "a clear national security or law enforcement" use can be kept secret and exploited.

This, of course, gives the government wide latitude to remain silent on critical flaws like the recent Heartbleed vulnerability if the NSA, FBI, or other government agencies can justify their exploitation.

A so-called zero-day vulnerability is one that's unknown to the software vendor and for which no patch therefore exists. The U.S. has long wielded zero-day exploits for espionage and sabotage purposes, but has never publicly stated its policy on their use. Stuxnet, a digital weapon used by the U.S. and Israel to attack Iran's uranium enrichment program, used five zero-day exploits to spread.

Last December, the President's Review Group on Intelligence and Communications Technologies declared that only in rare instances should the U.S. government authorize the use of zero-day exploits for "high priority intelligence collection." The review board, which was convened in response to reports of widespread NSA surveillance revealed in the Edward Snowden documents, also said that decisions about the use of zero-day attacks should only be made "following senior, interagency review involving all appropriate departments."

"In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection," the review board wrote in its lengthy report (.pdf). "Eliminating the vulnerabilities — 'patching' them — strengthens the security of US Government, critical infrastructure, and other computer systems."

When the government does decide to use a zero-day hole for national security purposes, they noted, that decision should have an expiration date.

"We recommend that, when an urgent and significant national security priority can be addressed by the use of a Zero Day, an agency of the US Government may be authorized to use temporarily a Zero Day instead of immediately fixing the underlying vulnerability," they wrote. "Before approving use of the Zero Day rather than patching a vulnerability, there should be a senior-level, interagency approval process that employs a risk management approach."

But Obama appeared to ignore these recommendations when the report was released. A month later, when he announced a list of reforms based on the review board's report, the issue of zero days went unaddressed.

Last week, however, after the Heartbleed vulnerability was exposed, and questions arose about whether the NSA had known about the vulnerability and kept silent about it, the White House and NSA emphatically denied that the spy agency had known about the flaw or exploited it before this year.

Following a now-disputed report from Bloomberg that the NSA had been exploiting the Heartbleed flaw for two years, the Office of the Director of National Intelligence issued a statement denying that the NSA had known about the vulnerability before it was publicly disclosed.

"If the Federal government, including the intelligence community, had discovered this vulnerability prior to last week, it would have been disclosed to the community responsible for OpenSSL," the statement said.

Intelligence authorities also revealed that in response to the presidential review board's recommendations in December, the White House had recently reviewed and "reinvigorated an interagency process for deciding when to share" information about zero day vulnerabilities with vendors and others so that the security holes could be patched.

"When Federal agencies discover a new vulnerability in commercial and open source software … it is in the national interest to responsibly disclose the vulnerability rather than to hold it for an investigative or intelligence purpose," the statement said.

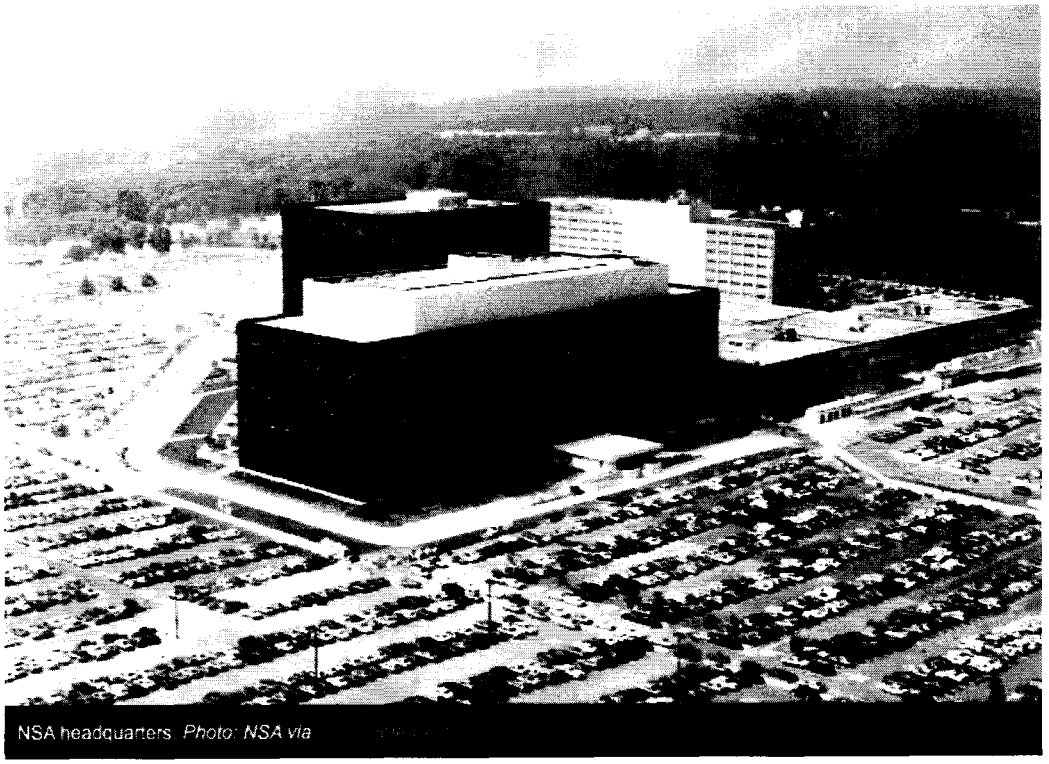
The government process for deciding on whether or not to use a zero-day exploit is called the Vulnerabilities Equities Process, and the statement said that unless there is "a clear national security or law enforcement need," the equities process is now "biased toward responsibly disclosing such vulnerabilities."

This implies, of course, that the bias was aimed in favor of something else until now.

"If this is a change in policy, it kind of explicitly confirms that beforehand that was not the policy," says Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic Council and a former officer in the Air Force's cyber division.

The government's use of zero-day exploits has exploded over the last decade, feeding a lucrative market for defense contractors and others who uncover critical flaws in the software used in cell phones, computers, routers, and industrial control systems and sell information about these vulnerabilities to the government.

But the government's use of zero days for exploitation purposes has long contradicted Obama's stated policy claims that the security of the internet is a high priority for his administration.



NSA headquarters. *Photo: NSA via*

The NSA's offense-oriented operations in the digital realm would also seem to directly oppose the agency's own mission in the defensive realm. While the NSA's Tailored Access Operations division is busy using zero days to hack into systems, the spy agency's Information Assurance Directorate is supposed to secure military and national security systems, which are vulnerable to the same kinds of attacks the NSA conducts against foreign systems. The NSA is also supposed to assist the DHS in helping to secure critical infrastructures in the private sector, a duty that is compromised if the NSA is keeping silent about vulnerabilities in industrial control systems and other critical systems in order to exploit them.

The government has used its equities process to analyze its use of zero-day exploits for the better part of a decade. That process is patterned after the approach used by the military and intelligence community in times of war to decide when information gleaned through intelligence should be exploited for military gain or kept secret to preserve intelligence capabilities.

The equities process for zero days has until now largely been focused on critical infrastructure systems — for example, the industrial control systems that manage power plants, water systems, electric grids — with the aim of giving government agencies the opportunity to state when disclosing a vulnerability to the vendor might interfere with their own ability to exploit the vulnerability. When vulnerabilities have been found in more general computing systems that could have an impact on U.S. military and other critical government systems, sources say the government has engaged in a form of limited disclosure — working on ways to mitigate the risk to critical government systems while still keeping the vulnerability secret so that it can be exploited in enemy systems.

But the first hint that the government's policy in this area was beginning to lean more toward disclosure than exploitation appeared in March during the confirmation hearing for Vice Admiral Michael Rogers to replace Gen. Keith Alexander as head of the NSA and the U.S. Cyber Command. In testimony to the Senate Armed Services Committee (.pdf), Rogers was asked about the government's policies and processes for handling the discovery and disclosure of zero days.

Rogers said that within the NSA "there is a mature and efficient equities resolution process for handling '0-day' vulnerabilities discovered in any commercial product or system (not just software) utilized by the U.S. and its allies."

The policy and process, he said, ensures that "all vulnerabilities discovered by NSA in the conduct of its lawful missions are documented, subject to full analysis, and acted upon promptly." He noted that the NSA is "now working with the White House to put into place an interagency process for adjudication of 0-day vulnerabilities."

He also said that "the balance must be tipped toward mitigating any serious risks posed to the U.S. and allied networks" and that he intended to "sustain the emphasis on risk mitigation and defense" over offensive use of zero days.

Rogers noted that when the NSA discovers a vulnerability, "Technical experts document the vulnerability in full classified detail, options to mitigate the vulnerability, and a proposal for how to disclose it." The default is to disclose vulnerabilities in products and systems used by the U.S. and its allies, said Rogers, who was confirmed by the Senate and took command of the NSA and US Cyber Command in March.

"When NSA decides to withhold a vulnerability for purposes of foreign intelligence, then the process of mitigating risks to US and allied systems is more complex. NSA will attempt to find other ways to mitigate the risks to national security systems and other US systems, working with stakeholders like CYBERCOM, DISA, DHS, and others, or by issuing guidance which mitigates the risk."

Healey notes that the public statements on the new policy leave a lot of questions unanswered and raise the possibility that the government has additional loopholes that go beyond the national security exception.

The statement by the Office of the Director of National Intelligence about the new bias toward disclosure, for example, specifically refers to vulnerabilities discovered by federal agencies, but doesn't mention vulnerabilities discovered and sold to the government by contractors, zero-day brokers or individual researchers, some of whom may insist in their sale agreements that the vulnerability not be disclosed.

If purchased zero days vulnerabilities don't have to be disclosed, this potentially leaves a loophole for the secret use of these vulnerabilities and also raises the possibility that the government may decide to get out of the business of finding zero days, preferring to purchase them instead.

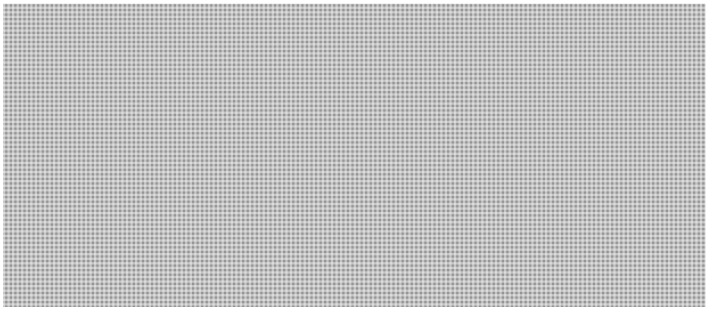
"It would be a natural bureaucratic response for the NSA to say 'why should we spend our money discovering vulnerabilities anymore if we're going to have to disclose them?'" Healey says. "You can imagine a natural reaction would be for them to stop spending money on finding vulnerabilities and use that money to buy them off the grey-market where they don't have to worry about that bias."

The government's new statement about zero days also doesn't address whether it applies only to vulnerabilities discovered in the future or to the arsenal of zero-day vulnerabilities the government already possesses.

"Do you grandfather in all of the existing vulnerabilities that are in the Tailored Access Operations catalog or are they going to go through with the new bias and review every vulnerability they have in their catalog?," Healey asks. "The military will do everything they can to not do that."

If the government does apply the new rules to its back-catalog of exploits, suddenly disclosing to vendors a backlist of zero-day vulnerabilities it has been sitting on and exploiting for years, it may well be detectable, Healey notes. The tell-tale sign to look for: a slew of new patches and vulnerability announcements from companies like Microsoft and Adobe.

--



s.19(1)
s.20(1)(b)

Thompson, Julie

From: [redacted]
Sent: Friday, July 18, 2014 10:23 PM
To: [redacted]
Subject: The consolidating 0-day exploits business, PART I (was: Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers)

Please find an interesting article on Google and its 0-days exploits research activity.

"**When 17-year-old George Hotz became the world's first hacker to crack AT&T's lock on the iPhone in 2007**, the companies officially ignored him while scrambling to fix the bugs his work exposed. **When he later reverse engineered the Playstation 3, Sony sued him and settled only after he agreed to never hack another Sony product. When Hotz dismantled the defenses of Google's Chrome operating system earlier this year, by contrast, the company paid him a $150,000 reward for helping fix the flaws he'd uncovered. Two months later Chris Evans, a Google security engineer, followed up by email with an offer: How would Hotz like to join an elite team of full-time hackers paid to hunt security vulnerabilities in every popular piece of software that touches the internet?**"

"**Today Google plans to publicly reveal that team, known as Project Zero, a group of top Google security researchers with the sole mission of tracking down and neutering the most insidious security flaws in the world's software.**"

[redacted]

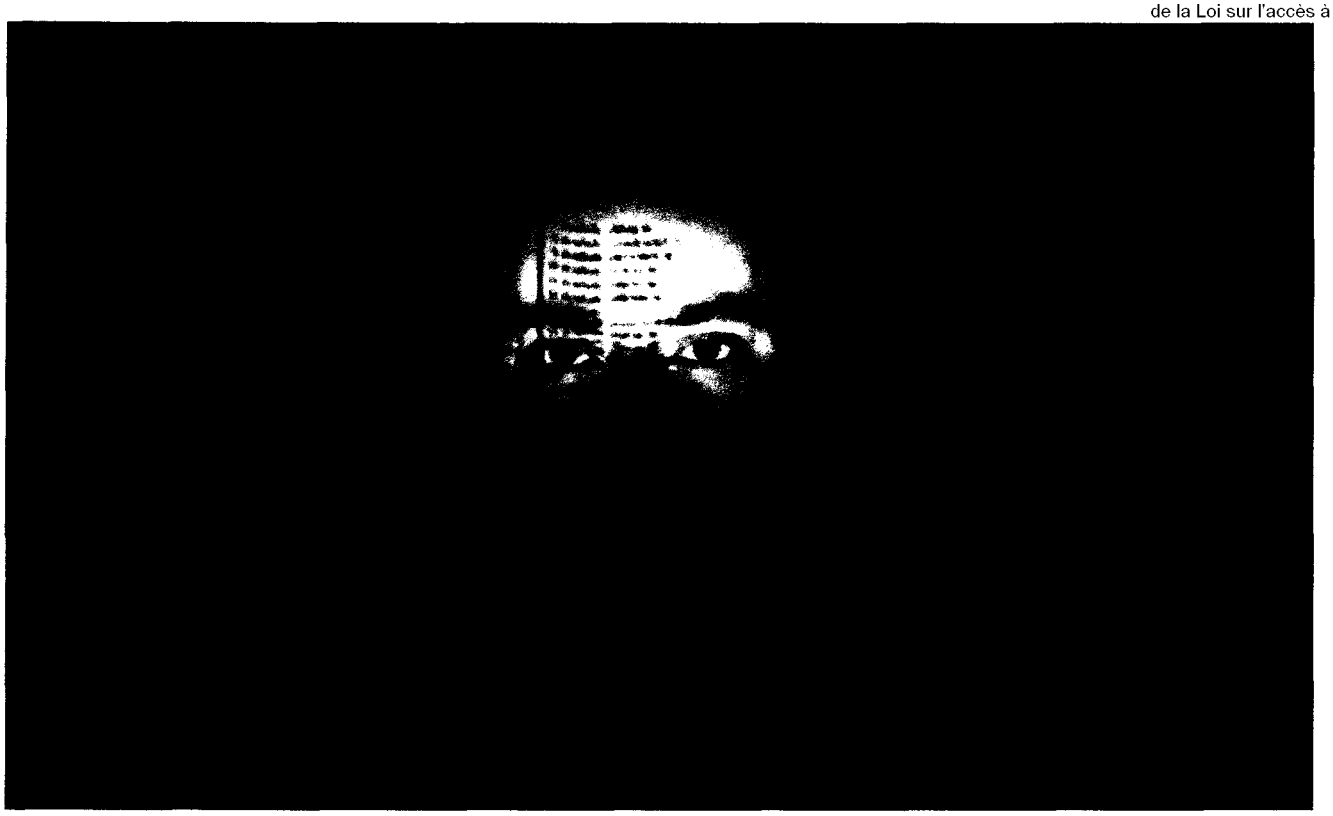
From WIRED, also available at http://www.wired.com/2014/07/google-project-zero/ .

Have a great day!

FYI,
[redacted]

Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers

By Andy Greenberg | 07.15.14 | 6:30 am |



Hacking wunderkind George Hotz's latest gig: An intern on Google's elite hacking team.

When 17-year-old George Hotz became the world's first hacker to crack AT&T's lock on the iPhone in 2007, the companies officially ignored him while scrambling to fix the bugs his work exposed. When he later reverse engineered the Playstation 3, Sony sued him and settled only after he agreed to never hack another Sony product.

When Hotz dismantled the defenses of Google's Chrome operating system earlier this year, by contrast, the company paid him a $150,000 reward for helping fix the flaws he'd uncovered. Two months later Chris Evans, a Google security engineer, followed up by email with an offer: How would Hotz like to join an elite team of full-time hackers paid to hunt security vulnerabilities in every popular piece of software that touches the internet?

Today Google plans to publicly reveal that team, known as Project Zero, a group of top Google security researchers with the sole mission of tracking down and neutering the most insidious security flaws in the world's software. Those secret hackable bugs, known in the security industry as "zero-day" vulnerabilities, are exploited by criminals, state-sponsored hackers and intelligence agencies in their spying operations. By tasking its researchers to drag them into the light, Google hopes to get those spy-friendly flaws fixed. And Project Zero's hackers won't be exposing bugs only in Google's products. They'll be given free rein to attack any software whose zero-days can be dug up and demonstrated with the aim of pressuring other companies to better protect Google's users.

Google security engineer Chris Evans, who is recruiting top talent for Project Zero .

"People deserve to use the internet without fear that vulnerabilities out there can ruin their privacy with a single website visit," says Evans, a British-born researcher who formerly led Google's Chrome security team and will now helm Project Zero. (His business cards read "Troublemaker.") "We're going to try to focus on the supply of these high value vulnerabilities and eliminate them."

Project Zero has already recruited the seeds of a hacker dream team from within Google: New Zealander Ben Hawkes has been credited with discovering dozens of bugs in software like Adobe Flash and Microsoft Office apps in 2013 alone. Tavis Ormandy, an English researcher who has a reputation as one of the industry's most prolific bug hunters most recently focused on showing how antivirus software can include zero-day flaws that actually make users less secure. American hacker prodigy George Hotz, who hacked Google's Chrome OS defenses to win its Pwnium hacking competition last March, will be the team's intern. And Switzerland-based Brit Ian Beer created an air of mystery around Google's secret security group in recent months when he was credited under the "Project Zero" name for six bug finds in Apple's iOS, OSX and Safari.

Evans says the team is still hiring. It will soon have more than ten full-time researchers under his management; Most will be based out of an office in its Mountain View headquarters, using flaw-hunting tools that range from pure hacker intuition to automated software that throws random data at target software for hours on end to find which files cause potentially dangerous crashes.

Google Vs. The Spooks

And what does Google get out of paying top-notch salaries to fix flaws in other companies' code? Evans insists Project Zero is "primarily altruistic." But the initiative–which offers an enticing level of freedom to work on hard security problems with few restrictions–may also serve as a recruiting tool that brings top talent into Google's fold, where they may later move on to other teams. And as with other Google projects, the company also argues that what benefits the internet benefits Google: Safe, happy users click on more ads. "If we increase user confidence in the internet in general, then in a hard-to-measure and indirect way, that helps Google too," Evans says.

This fits with a larger trend in Mountain View; Google's counter-surveillance measures have intensified in the wake of Edward Snowden's spying revelations. When the leaks revealed that the NSA was spying on Google user information as it moved between the company's data centers, Google rushed to encrypt those links. More recently, it revealed its work on a Chrome plug-in that would encrypt users' email, and launched a campaign to name which email providers do and don't allow for default encryption when receiving messages from Gmail users.

When a zero-day vulnerability gives spies the power to completely control target users' computers, however, no encryption can protect them. Intelligence agency customers pay private zero-day brokers hundreds of thousands of dollars for certain exploits with that sort of stealthy intrusion in mind. And the White House, even as it has called for NSA reform, has sanctioned the agency's use of zero-day exploits for some surveillance applications.

All of that makes Project Zero the logical next step in Google's anti-spying efforts, says Chris Soghoian, a privacy-focused technologist at the ACLU who has closely followed the zero-day vulnerability issue. He points to the now-famous "fuck these guys" blog post by a Google security engineer addressing the NSA's spying practices. "Google's security team is angry about surveillance," Soghoian says, "and they're trying to do something about it."

Like other companies, Google has for years paid "bug bounties"–rewards for friendly hackers who tell the company about flaws in its code. But hunting vulnerabilities in its own software hasn't been enough: The security of Google programs like its Chrome browser often depend on third-party code like Adobe's Flash or elements of the underlying Windows, Mac, or Linux operating systems. In March, Evans compiled and tweeted a spreadsheet, for instance, of all eighteen Flash bugs that have been exploited by hackers over the last four years. Their targets included Syrian citizens, human rights activists, and the defense and aerospace industry.

Colliding Bugs

The idea behind Project Zero, according to former Google security researcher Morgan Marquis-Boire, can be traced back to a late-night meeting he had with Evans in a bar in Zurich's Niederdorf neighborhood in 2010. Around 4am, the conversation turned to the problem of software outside of Google's control whose bugs endanger Google's users. "It's a major source of frustration for people writing a secure product to depend on third party code," says Marquis-Boire. "Motivated attackers go for the weakest spot. It's all well and good to ride a motorcycle in a helmet, but it won't protect you if you're wearing a kimono."

Hence Project Zero's ambition to apply Google's brains to scour other companies' products. When Project Zero's hacker-hunters find a bug, they say they'll alert the company responsible for a fix and give it between 60 and 90 days to issue a patch before publicly revealing the flaw on the Google Project Zero blog. In cases where the bug is being actively exploited by hackers, Google says it will move much faster, pressuring the vulnerable software's creator to fix the problem or find a workaround in as little as seven days. "It's not acceptable to put people at risk by taking too long or not fixing bugs indefinitely," says Evans.

Project Zero bug hunter Ben Hawkes.

Whether Project Zero can actually eradicate bugs in such a wide collection of programs remains an open question. But to make a serious impact, the group doesn't need to find and squash all zero-days, says Project Zero hacker Ben Hawkes. Instead, it only needs to kill bugs faster than they're created in new code. And Project Zero will choose its targets strategically to maximize so-called "bug collisions," the cases in which a bug it finds is the same as one being secretly exploited by spies.

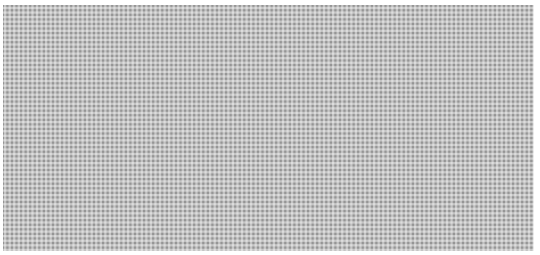
In fact, modern hacker exploits often chain together a series of hackable flaws to defeat a computer's defenses. Kill one of those bugs and the entire exploit fails. That means Project Zero may be able to nix entire collections of exploits by finding and patching flaws in a small part of an operating system, like the "sandbox" that's meant to limit an application's access to the rest of the computer. "On certain attack surfaces, we're optimistic we can fix the bugs faster than they're being introduced," Hawkes says. "If you funnel your research into these limited areas, you increase the chances of bug collisions."

More than ever, in other words, every bug discovery could deny attackers an intrusion tool. "I'm confident we can step on some toes," Hawkes says.

Case in point: When George Hotz revealed his Chrome OS exploit in Google's hacking competition last March to win the contest's six-figure prize, another competition's contestants had simultaneously come up with the same hack. Evans says he also learned of two other private research efforts that had independently found the same flaw—a four-way bug collision. Instances like that are a hopeful sign that the number of undiscovered zero-day vulnerabilities may be shrinking, and that a team like Project Zero can starve spies of the bugs their intrusions require.

"We're really going to make a dent in this problem," Evans says. "Now is a very good time to make a bet on putting a stop to zero-days."

--



s.19(1)
s.20(1)(b)