

RE: 0-day exploit..do i hear \$1000?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-10/0142.html>

From: Don Weber (Don@AirLink.com)

Date: 10/18/01

From: "Don Weber" <Don@AirLink.com>

To: "RT" <roelof@sensepost.com>, <vuln-dev@securityfocus.com>, <incidents@securityfocus.com>, <pe

Subject: RE: 0-day exploit..do i hear \$1000?

Date: Thu, 18 Oct 2001 11:28:39 -0700

Message-ID: <BAEBKBIMJFMJDDHPLBHKIEMHEAAA.Don@AirLink.com>

after reading the "0-day exploit..do i hear \$1000?", I would tend to think it would be reasonable for at least the major vendors to give rewards for people finding vulnerabilities in a product, considering, those same vendors have spent lots of money alpha/bet testing the product, still not finding the same vuln's, when a vuln is found by person x, company ABC should put say 25000\$ in a trust fund which has a panel of lets say 20 judges from the security industry, then after money is confirmed deposited to fund, hacker tells company what the problem is, company writes/releases patch, panel of Judges then read the reports on do whatever testing they themselves think necessary, and as a result vote on how much of the 25k is awarded to the person that found the hole, based on what they think the repercussions could have been if company had NOT been advised, this would possibly force the companies to either work harder on the product instead of release and hope for the best, and could even give those less than desirable hackers (for lack of a better term) an incentive to do a "good" thing with what they have found rather than use the Xploit for mischevious purposes, alot of them, white/black/green hats alike would much rather turn over what they have found if they blv they have a chance at 25k as opposed to responses along the lines of yeah right, that's dangerous we'll look into it, or oh, great thanks, and of course the cases where hacker x notifies company a company a entirely disregards the notification, and finally hacker x releases teh vuln to bugtraq or the like then vendor a flames hacker x for doijng so, claiming they either wasn't notified or given enough time. of course the reward program wouldn't have to be limited to only large companies, and the amount of any reward should have some impact on the finances of the company, and possibly some relationship to the total revenue which that product brought to the company over some period of time, there are a number of possibilities that could be used in determining the amount of the reward fund.

just my 0.02

hope this got into the right thread

Don

SecurityFocus Penetration: RE: 0-day exploit..do i hear \$1000?

-----Original Message-----

From: RT [mailto:roelof@sensepost.com]

Sent: Thursday, October 18, 2001 9:45 AM

To: vuln-dev@securityfocus.com; incidents@securityfocus.com;
pen-test@securityfocus.com

Subject: 0-day exploit..do i hear \$1000?

Moderators: Pass if you will. I think this seriously impacts the whole industry.

This email was written after I contacted a prominent "exploit collector" and asked for the new SSH exploit. He asked me "how much are you willing to pay, I selling 'sploits now". I said "You wanna WHAAT?". Afterwards I thought about it, and here are some comments/predictions as to what is happening in the industry.

At present a vulnerability is usually disclosed in the following way:

- * L33t Hacker finds problem in vendor ABC's product
- * L33t Hacker writes to ABC
- * ABC takes some time, builds a patch write an advisory and give credit to L33t Hacker
- * ABC release advisory to bugtraq, SF, packetstorm etc.
- * Security firm 123 implement patches for brain dead clients.
- * L4t3 Hacker writes exploit for problem
- * Exploit is seen on hack.co.za, packetstorm etc.
- * Assessment/Pen-test firm 456 test for the problem.

Obviously things does not always goes this way. L33t Hacker might write an exploit from the start. Exploit writers are usually after fame, wanting to see their names in lights on a MS advisory. In the above mentioned process the one people/firms that makes money from the bug are Security Firms 123 and 456. The L33t Hacker gets fame, not fortune. Hacker L4t3 also gets some fame – in some cases even more than L33t.

Then someday, Hacker L33t and L4t3 decides that they are not in it for fame, but for money. So, they open a security firm (many examples e.g. L0pht, Max Vision, RFP, many more). The problem now is keeping the exploits flowing while having to write reports, sit in meetings, wear a tie, doing budgets, and speaking to brain dead clients. So, in many cases, it does not work out. Hackers usually don't have a lot of patience with brain dead clients, hates writing report, and can't even balance their own budgets. They see that they only spend 10% of their time writing 0-day exploits...while that was the reason they signed up. Ask any "ethical hacker" – its tricky making

RE: 0-day exploit..do i hear \$1000?

SecurityFocus Penetration: RE: 0-day exploit..do i hear \$1000?

money
and keeping the brain occupied.

So, while Security Company 123, 456 and 789 are making money, hackers L33t
and

L4t3 are unemployed and frustrated by the fact that others are reaping the
rewards of their 0-day exploits that took 3 months to code. These two
contact

Hackers r3L4t3 and r3l3a5h and they form the "cyber underground
association",

and they sell 0-day exploits. They start off by selling exploit directly to
the

client and it goes like this:

- * CUA find a problem in vendor ABC's product
- * CUA codes the exploit
- * CUA let the word spread that they selling it
- * 10 script kiddies buy the exploit at \$100
- * Script kiddie l0s3r puts it on his website
- * Security firm 123 and vendor ABC get it, build patch (and the usual)
- * Script kiddie l0s3r's site gets DDOS-ed by CUA

CUA made \$1000 from the exploit. Security firm 123 made \$25 000 from it.

Some

networks are comprised by the kids, security firms/vendors takes the heat;

an

assessment was done on the network a week ago and it was certified as
"safe".

The whole IT security industry takes a knock. Everyone lose. CUA gets
together,

have a meeting, decides on new strategy. It goes like this:

- * CUA finds a problem in vendor ABC's product (no guessing who ABC is)
- * CUA codes the exploit
- * CUA contact "Exploit dealer @m1c\$" – a well connected person in script
kiddie
country.
- * @m1c\$ sells the exploit only to selected few – at \$500 a pop. He sells 10
copies.
- * @m1c\$ makes \$2500, CUA makes \$2500.
- * One of that selected few was in fact working for Security firm 456.
- * Knowing that CUA is killing the trade, and wanting the fame, 456 employee
rebrands the exploit to say 456-inc. and sends it off to Bugtraq (or puts it
on
their webpage)
- * Everyone gets the code on SF
- * 456-inc. gets DDOS-ed.

The other 9 selected few are typically people that will spend \$500 on an
exploit, knowing that they can compromise a network that have \$5000 worth of
credit cards or the likes. They are thus your black hat dudes – the criminal

RE: 0-day exploit..do i hear \$1000?

SecurityFocus Penetration: RE: 0-day exploit..do i hear \$1000?

type. The industry takes a knock – again, and in a bigger way. Security firm 123 and 789, not willing to pay for the code are booted out of several contracts, as their client's networks were compromised.

CUA has another meeting. Somehow they are not seeing the \$10000s that they expected. They make a new plan – bigger and better than before. They will bypass the dealer and only sell to people they know. It goes like this:

- * CUA finds yet another bug in ABC's software, codes exploit
- * CUA sells exploit to 25 selected people at \$1000 a pop.
- * Exploit is actually sold to many foreign agencies and a few terrorist
- * Exploit is also sold to n0h@ck, an undercover FBI agent.
- * CUA is taken to court and convicted under the 2002 Terrorist Bill thingy
- * End of CUA
- * Oh and the FBI gets DDOS-ed

Think about it for a while. At \$1000 an exploit, who are you going to attract?

People that will pay that amount of money must surely be in a situation that will make it worth their while. Dealing with these people will be dangerous for sure.

Non-disclosure will spark paying for exploits. Paying for exploits would be the same as paying for arms. Paying for exploits would make them illegal in no time. It would very much hurt the industry – the whole security industry – from the software vendor to the security vendor to the "ethical hackers", and all the way, the client/end user or firm will be taking the fall. Even the exploit writers will have a hard time. They are never going to make real money from their "product", will live in fear for their customers, and will take constant heat from their law enforcement agencies. A bigger challenge is to write the code AND make money in an honest way, AND keeping sane in the process, and I believe it can be done. The more underground the industry goes, the more heat it will take from government and law enforcement. The more open the industry is, the more transparent it is, the more acceptable it would become. And now I hear people saying – full disclosure is the reason behind script kiddies, the reason behind worms that cost us millions. Well lets quickly think about just that.

The Nimda worm did damages ranging in the millions of dollars (or so the bright beanies says). Just about every vulnerable server was attacked and compromised

RE: 0-day exploit..do i hear \$1000?

SecurityFocus Penetration: RE: 0-day exploit..do i hear \$1000?

by the worm, they say. Just think of all the man hours it took just to fix the problem they say. Think about the loss of productivity etc. OK. Its true. But this is also true – in the months before Nimda, SensePost (Pen-testing firm I work for) could take just about any corporate when doing an assessment. Easily. Way easy. Boredom actually set in. About 33% of all servers (those that were not the official websites or prominent sites) encountered were vulnerable. Gaping hole. Getting into the inner network way easy. No firewall could stop the attack. An open door to any attacker wanting to do damage in the network. And attackers and cyber criminals did just that. Has anyone EVER asked what the cost of the IIS double decode or Unicode bug was in dollars? No. Prolly because it cannot be easily calculated. How many networks were compromised, credit cards stolen, transactions altered etc. because of the bug? How much money / credibility was lost due to the bug? And how much would it cost to fix the bug on every machine – machines that administrators do not even know exist facing the Internet. For a large firm with multiple class B addresses – to find the machines? And to patch all?? And how many \$'s to co-ordinate all of that across the planet in one week. After the worm everyone seems patched. Those that are not are getting emails from just about every IDS out there – saying – hey! get with the program – patch your server with IP a.b.c.d. And here at SensePost we are elated – no more boring pen-testing – you prolly won't find a single double decode / Unicode machine out there now. Are worms that bad if they don't do local damage – I don't think so – they simply force people to sit up and react. The Nimda worm did more to secure the planet's networks in one week then any security company could do in a year. People simply don't read advisories, and never apply patches.

Makes you think eh?

Regards,
Roelof.

Roelof W Temmingh SensePost IT security
roelof@sensepost.com +27 83 448 6996
<http://www.sensepost.com> <http://www.hackrack.com>

This list is provided by the SecurityFocus Security Intelligence Alert (SIA)

RE: 0-day exploit..do i hear \$1000?

SecurityFocus Penetration: RE: 0-day exploit..do i hear \$1000?

Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** [Josh Daymont: "Re: Hacking Lotus Domino 5.0.5"](#)
- **In reply to:** [RT: "0-day exploit..do i hear \\$1000?"](#)
- **Next in thread:** [rain forest puppy: "Re: 0-day exploit..do i hear \\$1000?"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)