DECIPHER

Security news that informs and inspires

Aug 30, 2021

LAWYERS, BUGS

By Dennis Fisher

Share

For as long as there have been computers, there have been bugs. That's damn near 100 years and an uncountable number of bugs, some big, some small, some with wings, some that lived for decades. If they were discovered at all, most of those bugs were probably found by the developers themselves or another technical user and then fixed without much fuss. It wasn't until much later that some bugs became security concerns and developers and researchers began thinking about them in terms of their potential effects on the confidentiality, integrity, and availability of a system. Finding and fixing bugs was gradually becoming both more difficult and more important. In 1983, Hunter & Ready was so confident in the quality of its new VRTX real-time operating system that the company offered to reward anyone who found a bug in it with a Volkswagen Beetle. "But don't feel bad if a year from now there isn't a bug in your driveway.

There isn't one in your operating system either," the magazine ad said. It was a clever idea but it didn't inspire many imitators. Not until 1995 when a startup called Netscape Communications offered cash and Netscape merchandise to people who reported security bugs in the new beta release of its Navigator 2.0 browser.

And so, the bug bounty was born. Or at least conceived.

It would be another nine years before the idea truly took off when Mozilla unveiled its Security Bug Bounty Program, which paid the astounding sum of $500 for reports of critical security bugs in its applications. In the 17 years since Mozilla started its program, software providers, hardware companies, social media platforms, cloud providers, and even the Pentagon have taken the idea of a bug bounty and modified, reshaped, and remixed it. Today, bounties from public programs can reach six figures and there is a significant community of professional bug hunters who make their living from those bounties. Once dismissed as a novelty, bug bounties are now de rigeur. This is the story of the hackers who turned a niche idea into a worldwide industry. This is the first in a three-part series.

Note: All job titles and posiions reflect the person's role at the time of the events.

Lucas Adamski (director of security engineering, Mozilla): The strength of any security system, to me, is simply a function of how many smart, motivated people have looked at it over a period of time. That's it. It's got nothing to do with who wrote it, in my opinion, almost. It's almost about who has actually tried to break it, and that's what results in a strong system. So bounties were a way of saying, "Okay, we can only have so many people we hire." Mozilla originally was founded with not really intent to hire anybody. It was meant to be contributors. So the bounty program was just so we'd be getting contributors on the security side. I think the controversial side about it is, okay, why are we paying them because we weren't paying any other contributors other than full-time. If we do a security value program, why don't we just do a feature value program? Anybody who fixes a bug or creates a feature is also going to get paid. That was a big culture discussion. I think there were some distinctions. First of all, there already is a market for these work products, black market. It's not like people are generally getting paid to fix bugs or generate features randomly unsolicited. There's no market for, oh, I have a feature to flip a bit in something. Nobody's going to pay you randomly for that code you wrote, but there is definitely a market for the bug, an underground market for it.

Pedram Amini (founding member of iDefense Vulnerability Contributor Program and Zero Day Initiative): I went to Tulane and I didn't go to any classes my freshman year. All I did was stay up and hack the network because there was just so much stuff to play with. You could spend all day and night just discovering what was out there and what is this system? Let me go play with it. And I would find things. And when I would go to report it, because I did that every time the school was so supportive, they could have easily kicked me out the first time I brought something up. Instead, not only were they supportive, but they encouraged me. But one of the things they would always say is you remind us of this guy, Dave Endler. Who the is this guy? Every time I go to tell somebody about something, someone new on campus, they're telling me

Every time I go to tell somebody about something, someone new on campus, they're telling me about the name of this person. So fast forward to my senior year. And at this point I've made a couple of publishings on Bugtraq and Full Disclosure, which was the way that you publish anything back then. And so, because I had a few postings, iDefense who was Dave Endler and Sunil James and Mike Sutton, they came up with the idea of an open bug bounty. Let's buy vulnerabilities from people and report it to the vendor and we'll have pre access to it, part of our information feed that goes to our customer base. So to get it started, they scoured Bugtraq and Full Disclosure and they enumerated the folks that had published a few advisories and they sent outreach to them announcing this program that they were starting.

And so I get this email and it's got Dave's name on it who I've been hearing about for years. And I wrote him back. I'm like, this is neat. Who do you guys have on your end actually validating these things because I love the idea. I'd love to be involved. He's like, "Actually nobody. I'll be in town next week, visiting buddies, why don't we meet and see if something can be worked out?" So when I graduated school, after this meeting, my first job was with iDefense as the first person to sit there and validate these things on our end.

Aaron Portnoy (security researcher at Zero Day Initiative): I began working at the ZDI as an intern in 2006, the year after it had formed and prior to Pwn2Own. My main responsibility was verifying incoming zero-day submissions from our pool of external researchers. The process could be quite time consuming as it required installing and setting up software, debugging the issue, reverse engineering the root cause, verifying exploitability, and finally suggesting appropriate compensation.

Pedram Amini: And let me tell you, there was trolling, they were giving us just some things you didn't even want to validate. But the company has put budget there and we're like, let's just do it. Let's show people that we're paying them. Let's publish advisories at some point, this will change. And sure enough, it did.

Aaron Portnoy: As the youngest member of the team I tended to work through my analysis queue more quickly than others, motivated both by my love of reversing but also the ever-present pressure from the submitting researcher who was awaiting a determination. This was why I ended up being the team member chosen to be on-site and adjudicate the Pwn2Own contest when we launched it in 2007. In the following years I was promoted to manager of the ZDI and inherited the responsibility to craft future contests and rules, which I did for the following 6 occurrences.

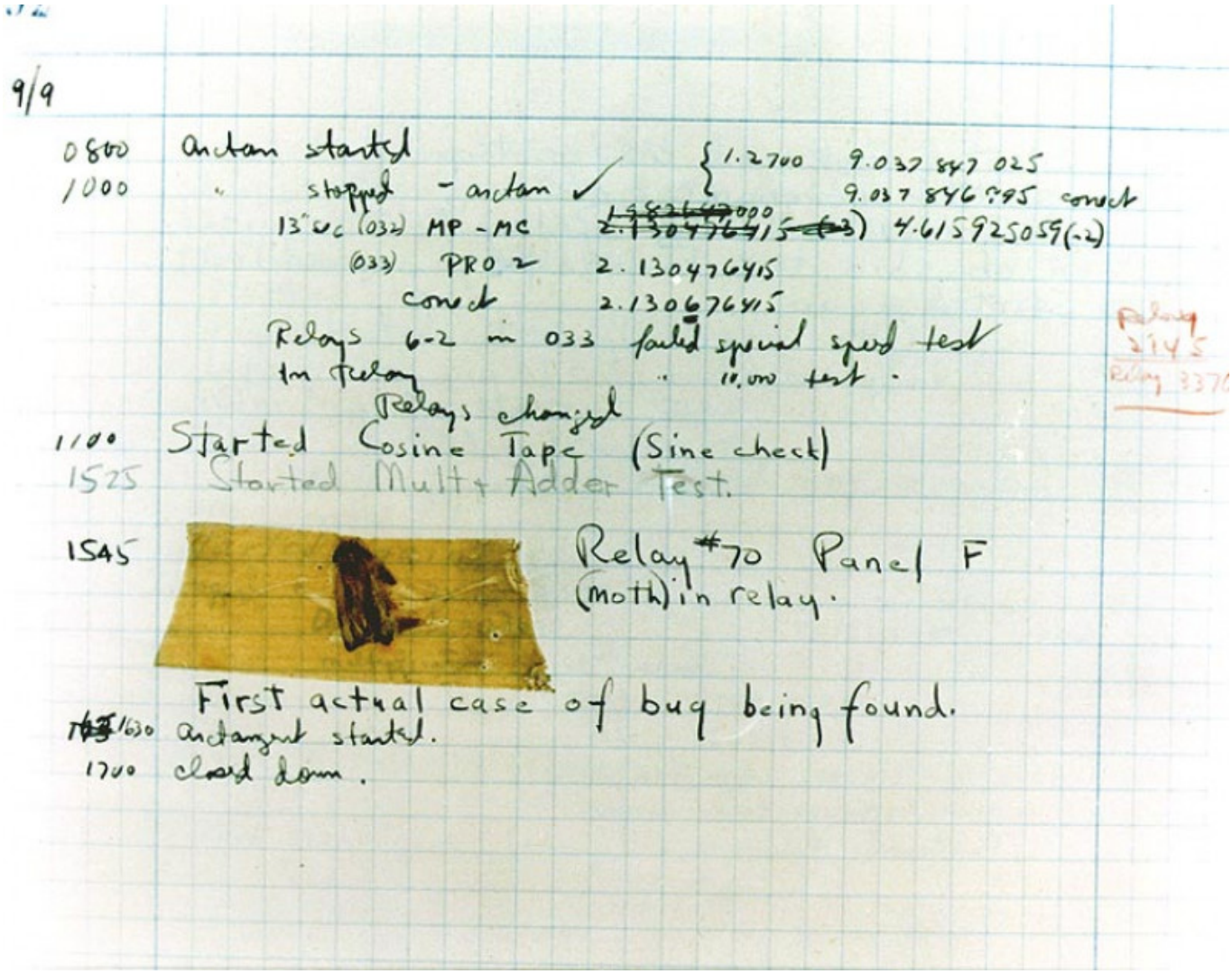
Pedram Amini: I had hired Aaron when he was 16 years old. He had come into the office. One of the sales guys came into my room like, "Hey, there's a dude here. He wants to do some technical work." And he mentioned the word OllyDbg, which at the time was a debugger that was kind of new age. And when I heard that, I'm like, let me see what this guy can do. So went in, met this young kid, I had to talk with his mom. And she said, "I don't want him working so young." I'm like, believe me, I'm a dinosaur.

Dragos Ruiu (founder of CanSecWest conference): It was my idea. What happened was, there was a gentleman from the UK and he gave us a presentation on Apple vulnerabilities. And he had a real unfortunate history because he had had a run-in as a kid with law enforcement. And he got basically a slap on the wrist, he was a brilliant guy, he was just poking around boundaries of laws in those days. But he was very, very nervous. I, as usual, trying to do the good thing, send Apple a copy of the presentation. So Apple responded after I sent them the presentation with the cease and desist letter from their lawyer to him. And he's like, "Eh." I was just pissed. And this was right around the time when the common refrain was, "Apples don't get hacked. They're secure." Because Windows was just shit in those days. It was like, you breathe wrong and you'll get a blue screen. And so I said, "Okay, well forget this." I was going to get a MacBook, I'm going to put it in a room, and the first person to hack it gets to keep it. And I was like, "I'm going to invite a bunch of reporters here to watch this because Apple screwed me out of a great presentation, dropping a whole bunch of important security information. I'm going to replace this with this spectacle."

Dino Dai Zovi (security researcher, co-winner of the first Pwn2Own contest): So when I was doing it, the stuff online just said, "Get the free laptop," but when I was sitting in my apartment, I was like, "I'm just doing this for the credit," and kind of just to show off really. But because my friend Shane (Macaulay) was actually in Vancouver, I was like, "Yeah, you get the laptop. I just bought a MacBook Pro, I don't need one that's identical specs. I don't care." But I was finding my exploit, you're just running it on the keyboard. Just to make sure I'm clear about that, because I'm in this to show off. Absolutely what I'm in it for. Because I was 27 or something. So I did that. But then the next day, when they said, "Oh yeah, it worked, the exploit worked, blah, blah, blah." I'm like, "Awesome." And they're like, "Oh, by the way, ZDI wants to offer $10,000 for the details of the bug. You want to talk to them?" I'm like, "Sure."

Dragos Ruiu: So right around that time, it was kind of an accident, someone came in and said, "Hey, so what are you going to do with that exploit that somebody's going to use for the MacBook? Can we buy it from you? Can we put up a cash prize for that?" And then, I don't remember, maybe that was 5K, and then I believe it was Aaron and company, said, "You know that 5K, can we make that a 10K prize?" So this started a little bit of a bidding war. And so that was the very first one.

"Oh, by the way, ZDI wants to offer $10,000 for the details of the bug. You want to talk to them?" I'm like, "Sure."



The first recorded computer bug, found in the Mark II at Harvard University in 1947, by a team that included Grace Hopper, a pioneering mathematician and programmer who later rose to the rank of rear admiral in the U.S. Navy.

Charlie Miller (security researcher, four-time Pwn2Own winner): On one of the Pwn2Owns, I had two Safari exploits, I think. Back then, the way Pwn2Own worked was, and still, probably to this day, it's not super well organized, it's run by a bunch of hacker dudes so you never know exactly what you're going to get. It takes me a long time to write an exploit. So I would see Pwn2Own is in a month or two. So I was like, "I'm going to find two Safari exploits and then I'll win the thing twice and I'll get twice the money as last year. That sounds like a good deal." Then, a week before Pwn2Own, they announced the rules and you can only win one. So I won and then I had

this other exploit, right. I was like, "Well, what am I going to do with this thing?"

I can't use it in a contest and I could just report it to Apple, I guess, but I didn't really see the point in doing that. I mean, obviously the point is it makes everyone more secure. But for me, personally, there wasn't much to get out of that. I guess I could have given it to ZDI or something, but I guess, but there weren't really any options to do that. I wasn't going to give it to a bad guy. So basically I just didn't do anything. I just did nothing. Then the next year Pwn2Own came on again and I was like, "Oh, I wonder if that exploit still works?" I tried it and it did so then I won the next year with the same exploit from the year before. So the bad news is, for a year, there was this exploit that existed and, presumably, I'm not the only one who could have found it. Some other people might've had that same exact exploit. So people were vulnerable for a year.

Pedram Amini: One of the things we saw at both VCP and ZDI is we had a decent statistical sampling of researchers and vulnerabilities around the world. Obviously not anywhere near the whole ecosystem, but even with that good enough view, we found a lot of overlap. In one case, I remember three different researchers from three different parts of the planet had found the same bug in three different ways and submitted to us around the same time. So we knew for fact that overlapping research is happening and it's happening with frequency. So that justifies the value of all this too because somebody's weapon might become moot because someone else altruistically through the program reported it and it went to the vendor and it got fixed.

Aaron Portnoy: As a fairly young researcher responsible for what became a highly visible contest, I can say it was definitely a diplomatic challenge and learning experience for me. The very first year was an experiment and most people who first heard of Pwn2Own thought of it as a gimmick for marketing purposes. However, once the first news cycle hit and the breadth of coverage spread to mainstream outlets, the affected vendors started to take serious notice. As the years progressed many of the recurring vendors would even schedule their patch cycles to kill bugs immediately before the contest was held, hoping to invalidate potential negative outcomes. The more the contest grew, the more I had to work on establishing relationships with all the parties involved--from the researchers, to the vendors, to the press. As you could imagine, the larger the contest became, the more pressure the vendor representatives were getting from their legal and marketing teams. For example, in the early days of Pwn2Own our team would take the exploits for analysis and deliver them to the affected vendors after the event. This created a period of time where vendors were out of the loop but still had to respond to the massive amount of press coverage. That process evolved over the years and culminated in a "war room" whereby the disclosure happened on-site immediately after a successful demonstration, which is certainly a more collaborative solution and allowed us to foster a trusting relationship with vendors.

Dragos Ruiu: And ironically, this is the funny bit, in those days our biggest supporter was Microsoft, who was really sending a lot of guys. That was when they were just getting into gear. And so they were really, really being supportive of the security industry. So in a way, it was Microsoft money that bought that (Apple) laptop.

Charlie Miller: So the downside of not having these kinds of bug bounty programs is you get this sort of situation where people are not incentivized to report bugs. Then people like me don't and then I get to win a contest a year later because of it. So it all worked out in the end, that bug got fixed.

"Pretty quickly, people were calling us extortionists."

Charlie Miller after winning Pwn2Own 2009, top, and Pwn2Own challenge coins, bottom.

Aaron Portnoy: When Chaouki (Bekrar, CEO of VUPEN) showed up, he brought the all-star team of six guys you don't know about. And he gamed the contest in a way that our rules weren't really accounting for. The whole state of everything got to a point where you couldn't have one guy do everything. You couldn't have one guy find the bug, exploit the bug, get past the mitigations... so they need a team. And once it gets to a team level, it's basically like the Olympics at that point. In hindsight, the motivation of the contest was initially simply to host a spectacle event for offensive security researchers for bragging rights. As we realized how much impact it ended up having, it became clear that simply the yearly demonstration of what was possible in a real-world scenario was an important awareness campaign--not just inside information security, but more importantly to the Internet community as a whole. As researchers ourselves, we knew what was possible because we dealt with zero-day vulnerabilities on a daily basis. It wasn't until Pwn2Own where those outside infosec were exposed to the fact that the devices they most trust are one motivated reverse engineer away from being compromised. Additionally, with the increasing awareness of the offensive-focused exploit market, Pwn2Own was able to offer an alternative outlet for research that did not include operations against unwitting targets.

Dragos Ruiu: So doesn't that mirror what was happening in the exploit development industry right at the time? You still have, even these days, you can still have the guy that runs it from beginning to end, does some cool shit. But these days it's always four or five, you got your fuzzer guy, you got your stack, your heap exploitation juju, magic ROP guy. You've got your guy who does the KLM thing. Everybody's got these multifunctional teams, and that's what it takes to play

these days. We've seen some two men teams, but it's two, three, four men teams that are usually the guys that are pulling it in to do this kind of stuff. It's because the scope of the exploitation now has become where it's really hard for one guy to be an expert in all of this crap.

Dino Dai Zovi: So obviously there's always kind of a black market, but that's a pretty dangerous road to go down if you don't know who you're dealing with. Basically, you should just assume that if you engage in a transaction like that, this is someone heavily engaged in cybercrime and you're an accomplice to it now. That's a terrible idea. And again, when you also realize, it was pretty obvious in 2000 that a lot of the energy behind a lot of cybercrime got connected pretty fast to Russian organized crime. They kill people. Do you want them to know who you are? Do you ever want to have a conversation anywhere near them? No. You do not.

Aaron Portnoy: I think it became very obvious that the secret 0-day market was going to appear. Every year at Pwn2Own, when the numbers went up, and the contestants went up, and then the difficulty went up. It's not hard to figure out where that's going to go.

Lucas Adamski: We were actually trying to compete with it head-on because that was a big part of the conversation too, is like, "Well, the underground market can pay ten grand, a hundred grand, maybe more for an exploit, but they're paying for something very different." They're actually paying for an exploit, and also they're paying for exclusivity. They're going to pay a lot of money, but you're going to have to weaponize it, and weaponizing stuff is a lot of work, and it's a pain in the butt. Also, you have to be a little ethically compromised maybe to do this. So we provided an alternate path.

Dino Dai Zovi: The idea (for No More Free Bugs) came from a night out in New York. And (Charlie's) like, "Hey, I'm in town, let's get a drink." And so we're having a drink at the bar and then I think Alex (Sotirov) came out too, and I can't remember exactly the order. Then Charlie told us a story about him reporting a bug or basically his presentation, and we're going to have some vulnerabilities in Android.

Charlie Miller: The way I remember it was, we were at (CanSecWest) and that conference was unique, at least as far as the ones I go to where it's only one track. So everyone is there all the time together. During one of the breaks we were sitting around outside and we started talking about this idea about how we do all this research and no one pays us. There's people who work for the companies that are doing the exact same thing as we do and they get a paycheck. So then we just had the idea that we were going to do this no more free bugs thing. I mean, it was totally spur of the moment, we just grabbed, I don't know why it was even there, but there was some old boxes. We found a marker somewhere and we made the sign. So Dino and Alex held the sign while I proselytized about it, at the mic. So that was how it went down.

Dino Dai Zovi: So basically that was just an over beers discussion. And then months later at CanSecWest, maybe even six months later, I can't remember, they have lightning talks at the end, and Charlie's like, "Hey guys, I want to do a talk about No More Free Bugs," and we're like,

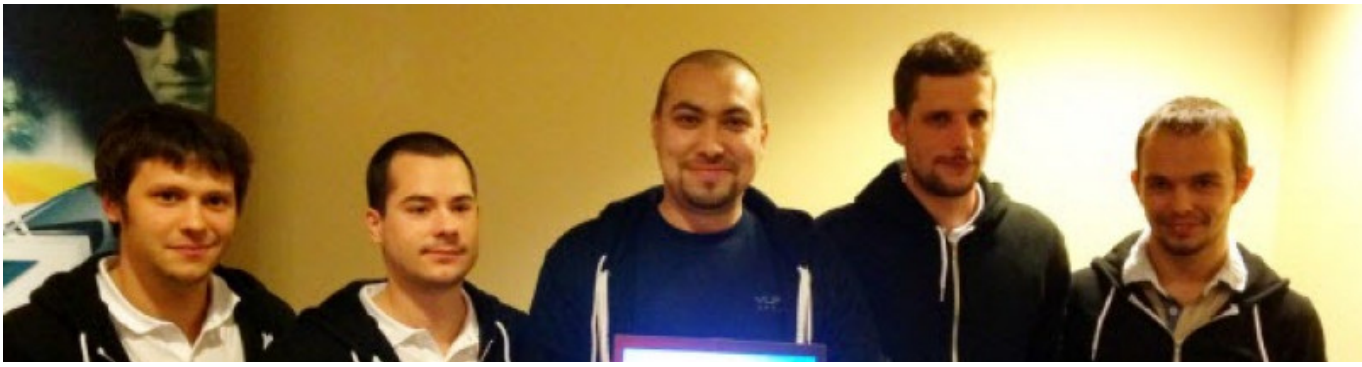
"Cool." I think it was Charlie's idea, of, "Let's make a sign." And so Charlie and I are using markers on this cardboard saying, "No More Free Bugs." And we were laughing at the mental image of a cardboard sign, like, "Will hack for food." And then it got some legs and I was like, "All right, I'm going to write a blog post about this, because I think people can pretty easily take it the wrong way." And so I wanted to just put something in writing versus just a bunch of stuff, because pretty quickly, people were calling us extortionists.

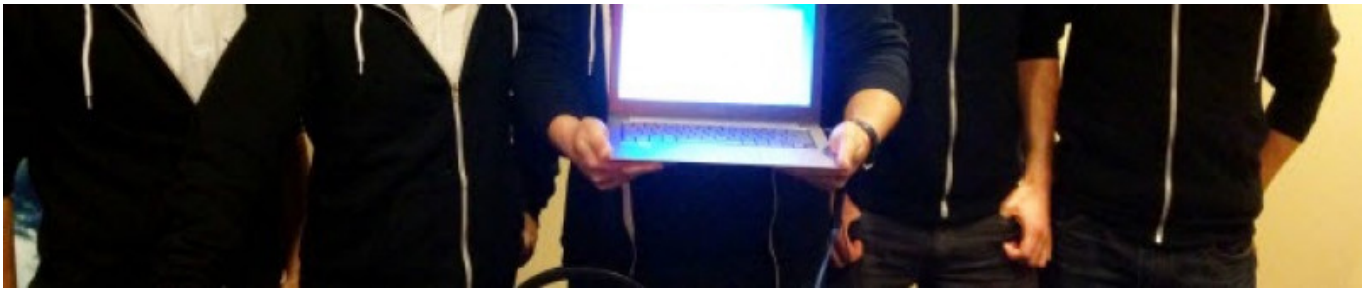
Charlie Miller: A lot of people I talked to really did stop reporting bugs. Then, nine months later, I was having a talk with Dino or someone about it and it occurred to us that this wasn't really effective. It wasn't really doing anything that we wanted. So what happened? So in nine months we stopped reporting bugs to them. So that's a good thing. But from the company's perspective, they don't necessarily... you can't really measure the security of their products. All you can do to see, oh, there's always patches. So there's a nine month period or whatever, where they're not getting any reports. Or at least not as many. So they're not having to make so many fixes. So, in essence, it looked like their software, all of a sudden, got really secure. But that's not what happened. So it had the opposite effect. We were like, "Oh, the companies are going to be like, "Oh my God, please keep reporting bugs." But really, they were happy as hell. It was like, "Oh, sweet, stop reporting bugs. That's even better. Now we don't have to fix anything. Now it looks like our software's secure. Now we don't have to deal with these researchers." So it didn't really work, I think. It might have worked in raising public awareness that this is an issue and, hopefully, some of these young hacker types and researchers went on to become CSOs who thought that paying for this research is important. But, at the time, I don't think it really had the intended effect with the companies.

Tomorrow: Part two.

Header image Creative Commons license from Garrett Gee's Flickr stream; second image courtesy of Ryan Naraine; third image CC license from Garrett Gee; fourth image by author; fifth image courtesy of Ryan Naraine.

Bug Bounty





Chaouki Bekrar (center) and the VUPEN team.