

Drive-by Downloading – an Interview with Amichai Shulman – CTO and co-founder of Imperva

Listen to the Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit [Imperva.com](https://www.imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. Joining me today is Amichai Shulman, cofounder and CTO of Imperva. Thanks for joining us today, Amichai.

Amichai Shulman: It's great being here today, Brian.

Brian Contos: So Amichai, today we're here to talk about drive-by downloading. Could you give us a little bit of background, a high-level overview of what exactly that term means?

Amichai Shulman: A lot of our listeners may have heard the term "buzzing ground", given the huge number of attacking incidents of drive-by downloads, and the press coverage that some of those incidents have gotten. Now basically a drive-by download attack is where a website is compromised in a way that is not visually apparent to visitors, but the code delivered by the page redirects visitors to download malicious software from an attacker-controlled site.

Brian Contos: OK, so in that way it might be somewhat similar to a bot attack, where a bot might infect a machine, but then it will go out and download more malicious code, and use that to render more systems compromised. Is that correct?

Amichai Shulman: Basically drive-by download attacks are today, probably the major proliferation engines for botnets. Innocent visitors are visiting the compromised sites, some of them high profile sites. Once they visit the site, their browser is instructed to download a small piece of software from an attacker-controlled server. That software in turn downloads the entire botnet agent.

Brian Contos: I see. So to encapsulate that, the compromised site isn't actually hosting the malware, specifically. It is just containing code redirecting the user's browser to that location.

Amichai Shulman: Exactly. Most of the time, this download is actually happening behind the scenes without the visitor, an innocent victim, even noticing it. When there is some kind of [inaudible 290] there's a sense from the victim that the question is popped up by the compromised site, which is usually a trusted one, rather than by the attacker-controlled site.

Brian Contos: This would usually be to point people to download things like spyware, computer viruses, or some other type of malware. Is that generally the goal?

Drive-by Downloading with Amichai Shulman

Amichai Shulman: Yes. It's quite focused on spreading botnet agents.

Brian Contos: So essentially the more systems that they can get infect for whatever use - spam relay, distribution of malware, used collaboratively as a denial of service attack engine, any of the standard things we're used to hearing whenever we talk about botnets.

Amichai Shulman: Exactly.

Brian Contos: Let me ask you this. We know a little bit about drive-by download, but what is really the technique that is used to compromise the site that's facilitating this activity?

Amichai Shulman: That really depends on an application by application basis. Sometimes it's a sort of vulnerability that would allow the attacker to actually inject an entire HTML page into the application or add to an existing page. Sometimes it's a different vulnerability, most commonly SQL injection, that would allow the attacker to change the content within the application database, in a way that is then displayed as part of the HTML forms delivered by the application.

I think that if we look over the past year, most drive-by download attacks used SQL injection for this purpose, but we did see some incidents that used completely different vulnerabilities. Mostly these are sporadic, individual incidents rather than massive attacks.

Brian Contos: Now, is there one particular vulnerability that stands out above others? Is there really something that is a prime target for attackers to exploit when they are looking to perpetrate this type of activity?

Amichai Shulman: Well, actually no. Actually it's more about the application and how the web application is built. I think that most drive-by download attack abused an SQL injection vulnerability within the target applications. In fact, there were a number of attacks during 2008 using already existing botnets to compromise hundreds of thousands of web applications, inserting into their databases pieces of HTML that would then cause visitors to download more botnet agents, and in this way increase the size of the botnet exponentially.

These were applications that were not using Active X at all. It's not about the client, it's about the web application.

Brian Contos: OK, that's a great point. A lot of people, I think, think about the problem sometimes as an end user problem. They think about enabling Active X control, which isn't really the root of the problem as opposed to the applications being vulnerable and being exploited. It's very interesting, this robots creating other robots reminds me of an episode of Star Trek: The Next Generation. But I digress.

Something comes to mind, though. Obviously this is a prolific type of attack. There's a lot of systems vulnerable to this. What are some of the high profile cases that we've seen regarding drive-by downloading?

Amichai Shulman: We had massive incidents that were invoked by the Asprox botnet. These incidents compromised hundreds of thousands of servers. Some of them were high profile. I think one of Microsoft's sites was hit, one of the CA sites was hit, and some others. There were some individual compromised incidents that were used for drive-by download attacks. I think the latest, and probably the most famous one is Paris Hilton's site being hacked and, again, being used for drive-by download attacks. Other than that, Major League Baseball, again, not for the first time was hacked and used for drive-by download attacks.

Drive-by Downloading with Amichai Shulman

So definitely we have seen some high profile cases of drive-by download attacks.

Brian Contos: It never ceases to amaze me how often Paris Hilton is the target for a lot of these new attacks. It is almost like she is the new Microsoft Windows. How can organizations protect their systems from this type of attack?

Amichai Shulman: I think we should try to answer two different questions. First is how can application owners protect their systems against some attacks, and how they protect their users against such attacks. These are not necessarily the same questions. In terms of protecting the application, you need to do everything you can to mitigate application-level vulnerabilities, be it SQL injection, page injection, or remote file includes and other types of well-known web application attacks. They eventually allow an attacker to insert HTML code into the pages that are being served to visitors.

The other side of this equation, how application owners can protect their users, is concerned with what happens if a site was indeed infected somehow, how can an application be protected against delivering the malicious to users.

There are ways to mitigate this risk as well by inspecting outgoing traffic and finding contents that indicate redirections of users to malicious servers. Of course this kind of solution would require a very high frequency update, with respect to what are malicious servers.

Of course, both types of solutions exist today. Interestingly enough, there are certain application firewalls that are capable of providing the two types of mitigation techniques.

Brian Contos: Well, Amichai, with that do you have any parting comments?

Amichai Shulman: I think that drive-by download attacks are a good example of the evolution of application attack and application hacking, where hackers no longer use a single vulnerability with a specific target of hit and run. Rather, they combine a number of vulnerabilities and techniques into a more sophisticated and more complex attack, with much larger implications over the application and Internet users in general.

Brian Contos: Absolutely, and it seems - correct me if I'm wrong - like a larger and larger number of these attacks are actually becoming transparent to the end user. If we talk about clickjacking and things like that, it seems like they are happening completely oblivious to the actual individual that is being targeted. Is that fair?

Amichai Shulman: Exactly. We'll probably talk about clickjacking in another opportunity, but this is a great example again of combining a number of techniques to create a more effective and more sophisticated attack.

Brian Contos: Fantastic. Well, Amichai, as always it was a pleasure having you.

Amichai Shulman: Thank you, Brian. It's a pleasure to be here.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200