These Ex-Israeli Surveillance Agents Hijack Your Browser To Profit From Ads

Thomas Brewster Forbes Staff

Senior writer at Forbes covering cybercrime, privacy and surveillance.

Follow

Jun 9, 2015, 11:26am EDT

🕐 **This article is more than 8 years old.**

At the start of last month, Google and Stanford University researchers released a report on a largely legal yet dubious practice in the advertising industry. It's called ad injection.

The process effectively intercepts users' traffic to inject content, namely, those irritating adverts and popups that seem to come from nowhere. Media rightly jumped on the report, highlighting the companies named as the top ad injectors. What went unnoticed, until now, is that most of the searchable organisations involved in this potentially dangerous business are based in Israel. They also happen to have links to the nation's military and its top signals intelligence agency, the Israeli equivalent of the NSA or GCHQ: Unit 8200, which works out of the Israel Defense Forces (IDF).

Ad injection is an old business that started taking off at the turn of the Millennium. It forms part of the convoluted world of personal data trading and marketing. The software used to inject ads arrives not quite as malware, but via what are known as "potentially unwanted programs", often bundled into application downloads or offered as directly-downloaded browser extensions. The Stanford and Google researchers, who collected data on the industry during the summer of last year, flagged 50,870 Chrome extensions as unwanted ad injectors, 38 per cent of which they decided were malware harmful to the security of users' data.

Once on a user's browser, the injector will effectively hijack a browser session and insert adverts on the page when a partnered website is visited. In most cases, the software has complete control over what appears on the user's screen, to the extent it might hijack mouse clicks or force other interactions on the site. The user simply has to trust the software won't do anything malicious.

Injectors also increase the chances of infection from malicious ads, which launch exploits on people's computers when the browser parses their content, as the ad chain isn't particularly well monitored, partly because of the huge number of companies involved. If a criminal hacker can find a weak link in that chain, they can have their ads injected into people's web sessions, hence repeated cases of so-called "malvertising".

A vulnerable ad injector could be exploited by hackers to kill security protections in the browser, notes Udi Yavo, CTO at Israeli security company enSilo, and they can relay plenty of information back to the

software author, including usernames and passwords.

Yavo believes ad injectors "run the fine line between ads and malware". "I would even make the claim that the behavior of the two is nearly identical. The difference between the two is simply the author's intention. While the first is considered a form of revenue-generation through the media, the second is pure cybercrime," he tells FORBES.

Forbes Daily: Get our best stories, exclusive reporting and essential analysis of the day's news in your inbox every weekday.

	Sign Up

By signing up, you accept and agree to our Terms of Service (including the class action waiver and arbitration provisions), and Privacy Statement.

The number of those affected by ad injection is astonishing - more than five per cent of unique daily IP addresses accessing Google, representing tens of millions of users, according to the research report. And people hate it. Of more than 100,000 Chrome user complaints in July 2014, nearly 20 per cent were about ad injection. It's the real scourge of the web, according to its actual users.

The providers make a lot of money too. When the Yontoo browser plugin modified 4.5 million users' private Facebook sessions to include ads, it reportedly earned the creator $8 million. That particular piece of intrusive kit was run by serial entrepreneur Arie Trouw, who built Sambreel Holdings, yet another maligned ad injection specialist.

But his entities have far less coverage than a handful of Israeli businesses full of former intelligence officials. It appears their offensive cyber and big data skills honed during their years at Unit 8200 have made them particularly adept at the practice.

Superfish

So, who are they? I recently reported on one of those firms, Superfish, and its links to the surveillance industrial complex. After it was spotted sitting on Lenovo PCs intercepting traffic throughout late 2014, breaking web encryption along the way, essentially destroying any trust users could have had in their online sessions, it emerged that not only its founder Adi Pinhas was formerly of 8200, he was also employed by Verint, which was linked to NSA surveillance. The company that actually created the encryption-breaking tech behind Superfish, Komodia, was also connected to Israeli intelligence services via its owner Barak Weichselbaum.

Superfish was dominating the ad injection game before the Lenovo caused it much strife. Google and Stanford found the firm injected ads into more than 16,000 websites and was making tens of millions in revenue a year doing so. By the researchers' extrapolations, Superfish appeared in 3.92 per cent of Google views. It has been irritating Apple Mac, Microsoft Internet Explorer and Mozilla Firefox users as far back as 2010. Many complaints about its Window Shopper tool can be found in cursory Google searches.

The Superfish tech, designed to show "visual ads" (essentially image-led adverts), installs a "little man-in-the-middle proxy" on the user's computer and configures the browser to go through it so it can inject

content into pages, explains Lee Brotherston, researcher at Leviathan Security. Sometimes this injection includes a piece of front-end web code called an iframe that points the browser to the Superfish web server to insert content dynamically. According to Google's study, the tool also reports every site a user visits, their language and country back to Superfish's server.

The company did not respond to requests for comment on its practices. It is imminently going out of business, according to a post on its website.

Jolly Wallet

Despite Superfish's dominance there are many others. Ranked by the researchers as the second most popular ad injecting program with 2.4 per cent of Google views, Jolly Wallet doesn't actually install software on the users' hard drive and wasn't classed by the study as an ad injector *per se*. It does, however, typically come packaged in a browser extension with permissions to read and alter all web content, its aim being to present cashback offers across different sites. It also often runs alongside other injection libraries.

Like Superfish, web denizens have complained about the tool being installed on their computers without their apparent knowledge, pointing to another issue with ad injectors: they often appear on systems from unknown sources.

Jolly Wallet was created by Radyoos, which was co-founded in 2011 by Roy Zisapel, who is also CEO of security provider Radware. He doesn't advertise his connections to Unit 8200, though in an article

from 2011 Zisapel notes he was part of the division. Zisapel seems to be using his experience in both offensive and defensive cyber to profit in two huge markets. He declined to be interviewed for this article.

VisAdd

According to one spyware removal advice site, Jolly Wallet can deliver ads from another Israeli firm, VisAdd, though it was not possible to confirm the connection. VisAdd is a strange, ostensibly shady entity. It has a static website that reveals almost nothing about what services the firm offers. 'Who Is?' searches reveal nothing. It's only through looking at the VisAdd privacy policy in Google caches of the site that it's possible to tell the firm was born in Israel.

But it was growing when Google looked at the firm last year, growing from 0.5 per cent of page views at the start of the research to 1.4 per cent at the time of writing earlier this year. The script scans for specific keywords including "add to basket", "free shipping", and "product review" in multiple languages and when detected payloads are dropped onto the user's browser. It would also hoover up information on user clicks and surfing behavior. Anyone who wants to remove the tool via the VisAdd site can try, though the service provided does nothing whatsoever.

There's no evidence the firm is connected to Israeli government surveillance, but given its location, it'd be no surprise if it was controlled by Unit 8200 alumni.

No Problem PPC

No Problem PPC is ranked as the seventh most popular ad injector, with 0.44 per cent of Google pageviews. The company's main service allows website owners to connect visitors with contractors and small businesses they might be looking for. If the user is interested they can offer up information and call listed companies provided by the widget. Useful, no?

But the company's tool has been seen bundled with other apps as a browser extension, Brotherston says. And, as with the others listed here, there are a number of removal walkthroughs for No Problem PPC. Company founder Daniel Shaked, an IDF reserve for nearly 12 years, notes over email the firm offers up its JavaScript to free software providers, and this has been used to deliver all kinds of ads, including "deceptive" ones, though this has "nothing to do with us". Shaked says No Problem doesn't push out ads, it only connects web users with professionals, first online then over the phone, and it makes money where it facilitates that final call.

iRobinHood

Ranked 11th on Google's most popular ad injectors is DonationTools, run by a company called iRobinHood. Its package both modifies what appears on the page and adds a toolbar to the browser, says Brotherston, who carried out a brief analysis on DonationTools. The version he tested also tried to change the default search engine.

As the name would suggest, iRobinHood attempts to encourage web users to donate to charity. "Every search or purchase made online automatically generates commissions to third parties. iRobinHood redirects these revenues to registered non-profit organisations," its

website says.

In a brief telephone conversation with FORBES, founder Moti Golden said he could not comment on its ad injection practices, indicating his organisation was going through financial difficulties, whilst he had suffered a family bereavement. The organisation counts a number of ex-IDF members amongst its developers, according to LinkedIn profiles, including a former digital forensics expert and a computer crimes investigator.

Are its practices forgivable given its aims? A Google search shows many are concerned about what the program can do, with some labelling it adware and advising users to steer well clear as its pop-ups link to non-charitable offers. Giving is good but such forceful tactics have clearly put off some.

Crossrider

A vast number of companies are affiliated with ad injectors, either packaging their tools or funnelling ads down to them. One of the biggest is Crossrider, the majority stake of which is held by billionaire Teddy Sagi, a serial entrepreneur and ex-con who was jailed for insider trading in the 1990s. His biggest money maker to date is gambling software developer Playtech. Co-founder and CEO Koby Menachemi was part of Unit 8200, where he was a developer for three years.

According to the Google report, Crossrider was doing plenty of work with Superfish whilst it was still swimming, amongst many others, using various kinds of ad injection techniques. It allows app

developers to build those injection capabilities into their software, using the Crossrider platform, but it seems bad actors have used this for their own means. US antivirus giant Symantec ranks one service based on Crossrider's software, Crossid, as adware with a "high" risk impact. It warns Crossid can inject content and collect information about the user, such as IP address, operating system and browser information.

Is Google wrong?

Crossrider's VP for mobile Ran Goldi says his company is keen to clean up the ad injection industry to ensure that real criminal malware doesn't land on people's PCs. He admits too many bad actors find a way onto the ad chain to insert their malicious code onto the web, hence the firm's participation in the Microsoft Clean Software Alliance.

But he doesn't believe the market is an inherently evil one, far from it. When Superfish intercepted people's traffic from their Lenovo PCs, it was simply trying to provide a useful service, "to give better offers to people in terms of buying and shopping". He and Idan Aharoni, a security-focused entrepreneur and former department head at RSA's anti-fraud team in Tel-Aviv, believe Google has its own interests at heart when criticising ad injection, given its primary source of revenue comes from ads.

"Naturally Google has something to lose from these ad injections, so obviously they are going to paint it as 'dangerous'. Malvertising, the real danger, can happen in Google Adwords just as it is possible to appear in any other ad network," says Aharoni.

Scared of the ex-spies who sell you?

As for the ad injection industry's connection to Unit 8200, Goldi believes the skills used in signals intelligence are the same as those required in targeted ads. "It's pretty much the same thing - catching the bad guy from the intelligence point of view and targeting a good guy to give them the right [content]," he says.

Given Israel "dominates advertising, period", adds Goldi, it should be no surprise the injection game is full of former intelligence officials. 8200 is also the biggest unit in the IDF and military service is compulsory in Israel. Many leave to go into various tech markets, not just security.

But Brotherston says the involvement of ex-8200 personnel in the "very dangerous" injection business is "troubling". "When Snowden released a cache of documents on what signals intelligence was doing within Five Eyes, people were outraged at what their governments were doing with this information. Now consider that Unit 8200 probably has very similar mandates, but is part of another country's government. If they have access, via ex-members, then a signals intelligence unit potentially has direct access to view the contents of what someone is browsing and modify the content," he added.

Nicholas Weaver, computer security researcher at the International Computer Science Institute in Berkeley, doesn't believe the Unit 8200 connection to add injection is of great concern and wouldn't be abused for malicious purposes. But he has different concerns around Unit 8200. He's worried injectors may be transmitting user data from across the world to Israeli servers over unencrypted HTTP

connections. "What worries me is whether any of these systems might cause users to fetch data from Israeli servers over HTTP. These companies may consider themselves benign, but the Israel government is notorious for hacking and industrial espionage, and the Israeli government can use any such traffic to hack individual targets," Weaver adds.

"Traffic visible to an adversary is not just an information leak, but a vector they can use to attack."

Even publishing information on ad injection can land users in legal trouble. Another Israeli firm, Flash Networks, appears to be injecting ad content over Airtel 3G at the network layer - a method described by Weaver as "objectionable". According to a report from India, a local activist called Thejesh GN has been sent a cease and desist letter from the firm's local lawyers, asking him to remove content from GitHub that showed how the injection worked. Again, some of the Flash Networks team, including its VP of research and development, spent their formative years in Unit 8200.

Exposing former spies, it seems, can prove troublesome.

Thomas Brewster   Follow

I'm a senior writer for Forbes, covering security, surveillance and privacy. I'm also the editor of The Wiretap newsletter, which has exclusive stories on...

Read More

Editorial Standards   Print   Reprints & Permissions