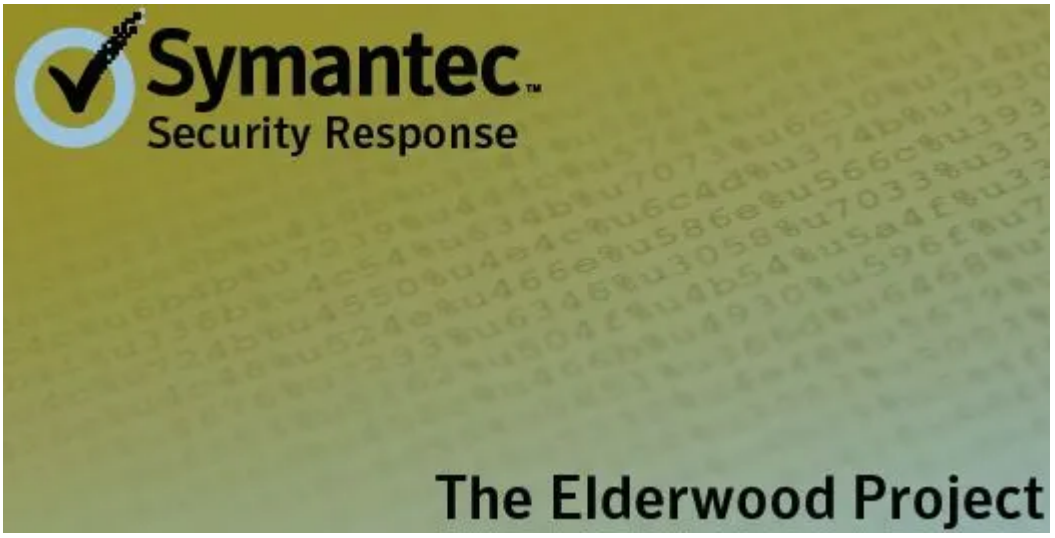
# Elderwood project, who is behind Op. Aurora and ongoing attacks? - Security Affairs

By Pierluigi Paganini

Published: 2012-09-09 · Archived: 2026-04-05 12:54:02 UTC

Pierluigi Paganini September 09, 2012




Today, I would like to discuss the real effects of a cyber attack. We have recently introduced the direct and indirect effects of several cyber espionage campaigns, such as Flame and Gauss, but we have never approached the problem from a future projection, examining the possible impacts of an incident many years after it.

Symantec researchers published an analysis that demonstrates the link between a series of attacks to more than 30 companies and the cyber espionage attacks moved against Google three years ago so-called Operation Aurora.

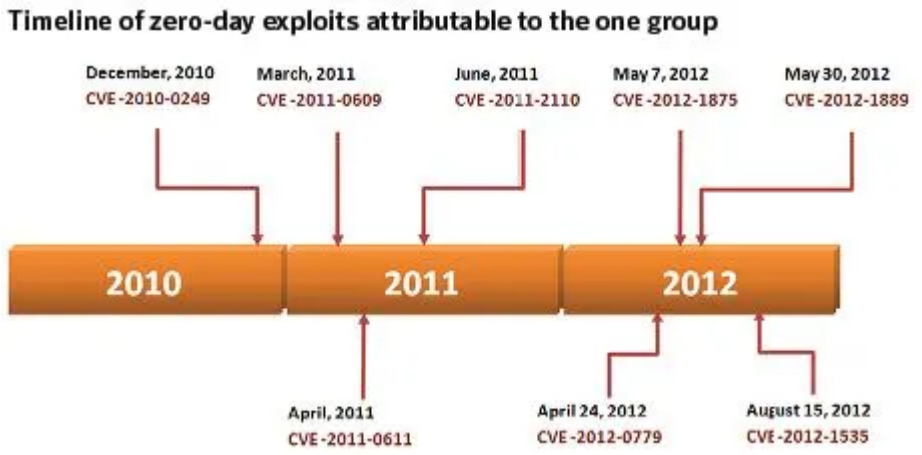
Operation Aurora is considered an epic cyber attack which happened during the second half of 2009 and was publicly disclosed by Google in January 2010.

The sophisticated attacks appeared to have originated in China and aimed at dozens of other organizations, including Adobe Systems and Juniper Networks which confirmed the incident. The press is also convinced that other companies were targeted, such as Morgan Stanley, Northrop Grumman, and Yahoo.

The Aurora attack is one of the most complex operations due to the attacker's capability to exploit several 0-day vulnerabilities, including one related to the popular IE Explorer. In 2010, a notable zero-day exploit was linked to a group of hackers that used a Trojan horse called "Aurora" distributed using an Internet Explorer (IE) zero-day, and targeted a large number of Western companies.

According to the security firm Symantec, the hackers behind the attacks still have knowledge of 0-day vulnerabilities, and at least four of them have been used in recent attacks against different targets across strategic

sectors such as energy, defense, aeronautics, and financial.




Orla Cox, senior manager at Symantec's security response division, reported that it has been exploited at least eight zero-day vulnerabilities since late 2010, and four since last spring. She said:

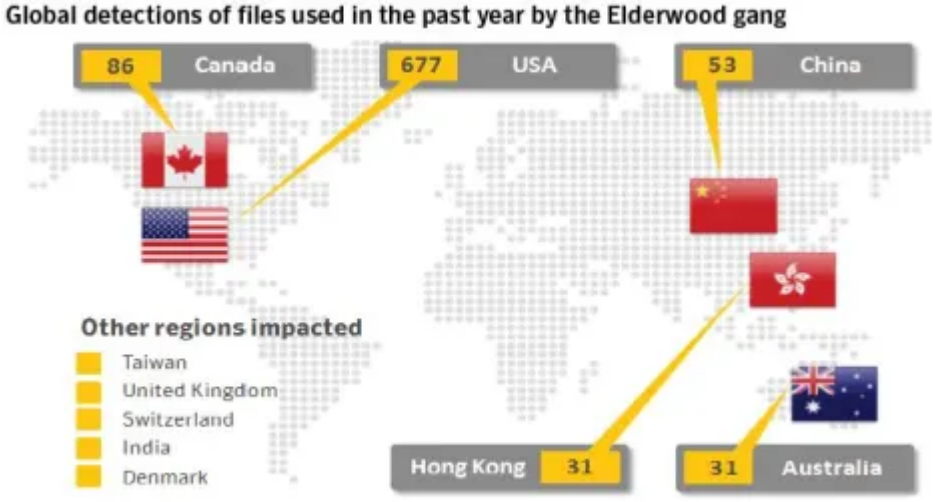
*"We were amazed when Stuxnet used four zero-days, but this group has been able to discover eight zero-days. More, the fact that they have prepared [their attacks] and are ready to go as soon as they have a new zero-day, and the speed with which they use these zero-days, is something we've not seen before."*

The document of the security firm reports:

*"This group is focused on wholesale theft of intellectual property and clearly has the resources, in terms of manpower, funding, and technical skills, required to implement this task,"*

*"The group seemingly has an unlimited supply of zero-day vulnerabilities."*

The attacks part of the cyber espionage campaign discovered by Symantec has been named "Elderwood Project", for their execution has exploited 0-day vulnerabilities in many widely used software, including IExplorer and Adobe Flash Player.



The experts from Symantec declared that some of the exploits have been realized from the knowledge of stolen source code.

*“In order to discover these vulnerabilities, a large undertaking would be required by the attackers to thoroughly reverse-engineer the compiled application,”*

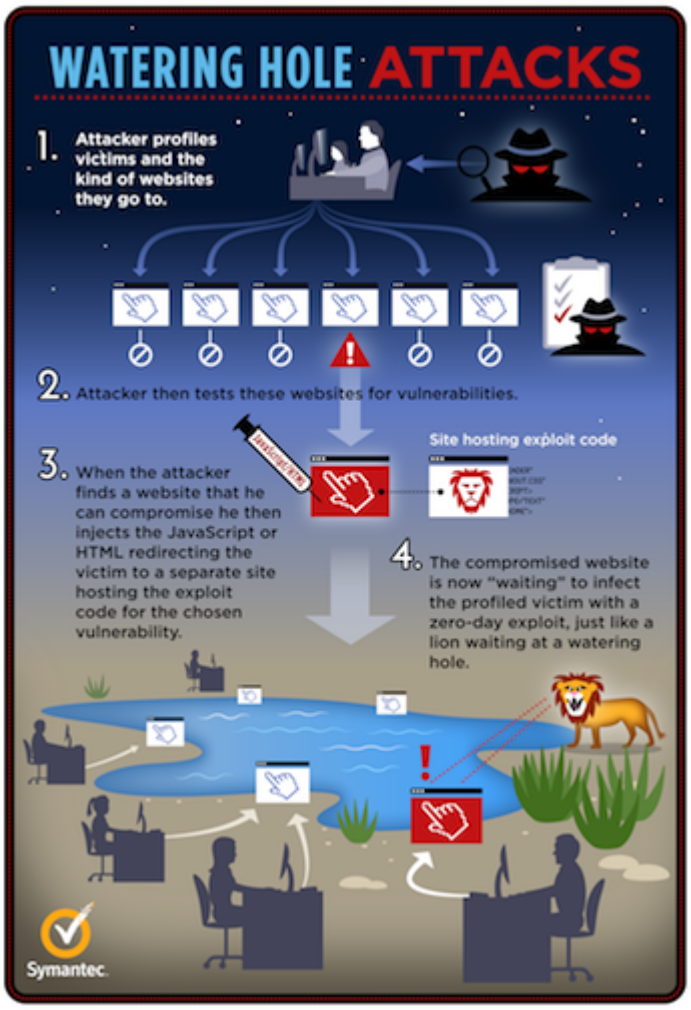
*“This effort would be substantially reduced if they had access to the source code. The group seemingly has an unlimited supply of zero-day vulnerabilities. The vulnerabilities are used as needed, often within close succession of each other if exposure of the currently used vulnerability is imminent.”*

The attacks conducted during the recent months have been using an unusual method to infect the victims with malware, it has been named “watering hole” attack and consists of injecting malicious code onto the public Web pages of a site that the targets are supposed to visit.

The method of injection isn’t new and is commonly used by cyber criminals and hackers, the main difference between their use in cybercrime and watering hole attacks are related to the choice of websites to compromise and use in the attacks.

The attackers haven’t indiscriminately compromised any website, but they are focused on choosing websites within a particular sector to infect persons of interest who likely work in that same sector and are likely to therefore visit related websites. The Symantec report states:

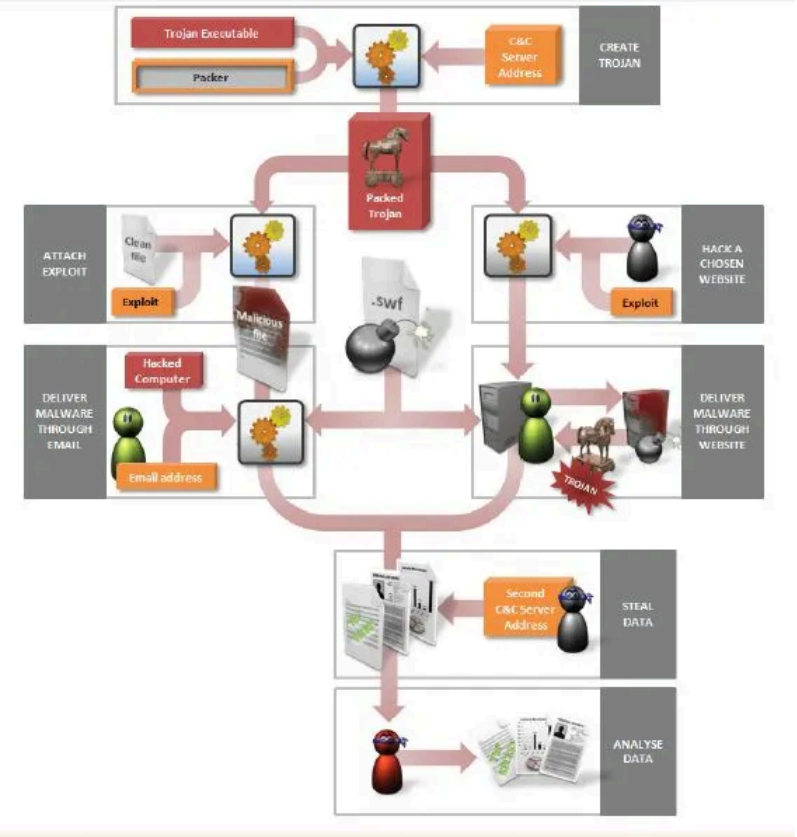
*“Targeting a specific website is much more difficult than merely locating websites that contain a vulnerability. The attacker has to research and probe for a weakness on the chosen website.*
*Indeed, in watering hole attacks, the attackers may compromise a website months before they actually use it in an attack. Once compromised, the attackers periodically connect to the website to ensure that they still have access. This way, the attackers can infect a number of websites in one stroke, thus preserving the value of their zero-day exploit. They are even in a position to inspect the website logs to identify any potential victims of interest. This technique ensures that they obtain the maximum return for their valuable zero-day exploit.”*




Once a victim visits the compromised site, the software for which the 0-days have been designed will make it possible the infect the machine.

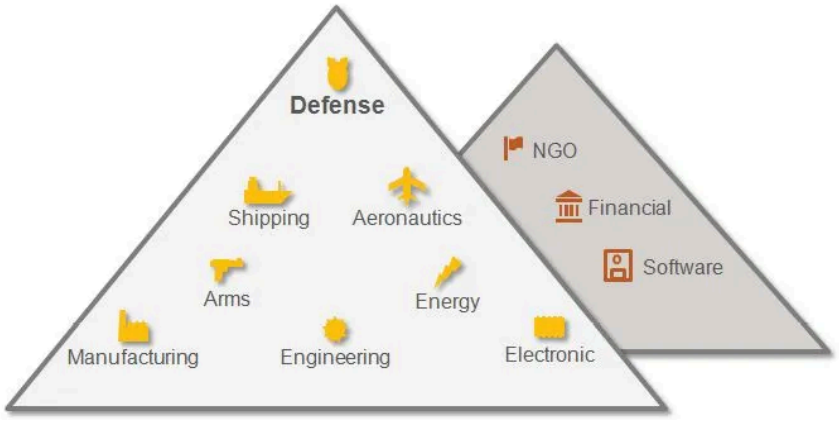
Symantec researchers have detected the use of this method using at least three different zero-day exploits in the last month.

The researchers believe that a specific platform has been implemented to conduct the operations, all the attacks use a  Trojan to infect the target computer that is packaged with a packer, and also the address of the command-and-control (C&C) server. The delivery of the malware to the final victim is either through an email or a web-based vector.




I opened the post supporting the idea that Aurora attacks are state-sponsored, it's clear that I have no evidences for this, but the nature of the job, the targets chosen and the complexity of the operations make me believe that it is a result of a government project.

**Target sectors**




The unique certainty according to Symantec is a connection between the most recent attacks and those used in attacks in 2011, demonstrable with common technical features and a noticeable similarity in the timing of the attacks and the types of vulnerabilities used between the 2012 and 2011 attacks.

*"After this initial compromise, the attackers consolidate their beachhead and begin to analyze the stolen information, spreading through networks and maintaining access as needed. By analyzing the information gathered, the attackers can identify yet more targets of interest"*

Cox said Symantec has no hard evidence of this:

*“But this is a full-time job,”*

*“The work they do is both skilled and time consuming. They would have to work at it full time, so someone is paying them to do this.”*

*“The analysis has shown that certain organizations have been hit in different ways, indicating that they’re of particular interest to [their paymasters],”*

I leave you all the interpretations of the Symantec expert, but I think that her thought is not far from mine.

Waiting for further analysis, any manufacturers who are in the defense supply chain need to be wary of these types of attacks. Subsidiaries, business partners, and associated companies are considerably privileged targets, an easy way to penetrate the defense system of large companies

*… raise your guard, the enemy may already be in.*

| | |
|---|---|
| [adrotate banner=”9″] | [adrotate banner=”12″] |

**Pierluigi Paganini**

**(Security Affairs – Elderwood Project, Operation Aurora)**

[adrotate banner=”13″]

---