Endpoint Protection

Back to Library

The Elderwood Project

1 Recommend

Sep 06, 2012 07:00 PM

A L Johnson

In 2009, we saw the start of high profile attacks by a group using the Hydraq (Aurora) Trojan horse. We've been monitoring the attacking group's activities for the last three years as they've consistently targeted a number of industries. These attackers have used a large number of zero-day exploits against not just the intended target organization, but also on the supply chain manufacturers that service the company in their cross hairs. These attackers are systematic and re-use components of an infrastructure we have termed the "Elderwood Platform". The term "Elderwood" comes from the exploit communication used in some of the attacks. This attack platform enables them to quickly deploy zero-day exploits. The attacking methodology has always used spear phishing emails but we are now seeing an increased adoption of "watering hole" attacks (compromising certain websites likely to be visited by the target organization).

We call the overall campaign by this group the "Elderwood Project".

Serious zero-day vulnerabilities, which are exploited in the wild and affect a widely used piece of software, are relatively rare; there were approximately eight in 2011. The past few months however has seen four such zero-day vulnerabilities used by the Elderwood attackers. Although there are other attackers utilizing zero-day exploits (for example, the

Sykipot, Nitro, or even Stuxnet attacks), we have seen no other group use so many. The number of zero-day exploits used indicates access to a high level of technical capability. Here are just some of the most recent exploits that they have used:

• Adobe Flash Player Object Type Confusion Remote Code Execution Vulnerability (CVE-2012-0779)
• Microsoft Internet Explorer Same ID Property Remote Code Execution Vulnerability (CVE-2012-1875)
• Microsoft XML Core Services Remote Code Execution Vulnerability (CVE-2012-1889)
• Adobe Flash Player Remote Code Execution Vulnerability (CVE-2012-1535)

In order to discover these vulnerabilities, a large undertaking would be required by the attackers to thoroughly reverse-engineer the compiled applications. This effort would be substantially reduced if they had access to 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 primary targets identified are within the defense supply chain, a majority of which are not top-tier defense organizations themselves. These are companies who manufacture electronic or mechanical components that are sold to top-tier defense companies. The attackers do so expecting weaker security postures in these lower tier organizations and may use these manufacturers as a stepping-stone to gain access to top-tier defense contractors, or obtain intellectual property used in the production of parts that make up larger products produced by a top-tier defense company. Figure 1 below shows a snippet of the various industries that are part of the defense supply chain.

Figure 1. *Target sectors*

One of the vectors of infection we're seeing a substantial increase in, called a “watering hole” attack, is a clear shift in the attacking group's method of operations. The concept of the attack is similar to a predator waiting at a watering hole in a desert. The predator knows that victims will eventually have to come to the watering hole, so rather than go hunting, he waits for his victims to come to him. Similarly, attackers find a Web site that caters to a particular audience, which includes the target the attackers are interested in. Having identified this website, the attackers hack into it using a variety of means. The attackers then inject an exploit onto public pages of the website that they hope will be visited by their ultimate target. Any visitor susceptible to the exploit is compromised and a back door Trojan is installed onto their computer. Three zero-day exploits, CVE-2012-0779, CVE-2012- 1875, and CVE-2012-1889 have all been used within a 30-day period to serve up back door Trojans from compromised websites. The increase in the use of this

attack technique requires the attackers to sift through a much greater amount of stolen information than a targeted attack relying on email, as the number of victims compromised by a Web injection attack will be much greater.

Figure 2. *Web injection process used in watering hole attacks*

Any manufacturers who are in the defense supply chain need to be wary of attacks emanating from subsidiaries, business partners, and associated companies, as they may have been compromised and used as a stepping-stone to the true intended target. Companies and individuals should prepare themselves for a new round of attacks in 2013. This is particularly the case for companies who have been compromised in the past and managed to evict the attackers. The knowledge that the attackers gained in their previous compromise will assist them in any future attacks.

Research Paper

We have published a research paper that details the links between various exploits used by this attacking group, their method of targeting organizations, and the Elderwood Platform. It puts into perspective the continuing evolution and sheer resilience of entities behind targeted attacks.

Tags and Keywords

Related Entries and Links

No Related Resource entered.