Inside a Back Door Attack

June 29, 2011

A colleague of mine recently wrote about one of the June “Microsoft Tuesday” vulnerabilities being exploited in the wild. Because we're a bit like that, we decided to allow the exploit to compromise one of our honeypot computers so we could observe what happened.

The exploit first came to our attention by way of email messages that were initially sent to a customer and then passed on to us for investigation. These messages were sent from an account hosted on a popular webmail service, contained very bad grammar, and were purportedly sent by a Chinese university student. The emails either asked for advice on a particular topic, or thanked the recipient for a recent presentation and included a question related to that presentation. The emails included a link to a Chinese restaurant and the destination Web page contained the exploit for an Internet Explorer 8 vulnerability:

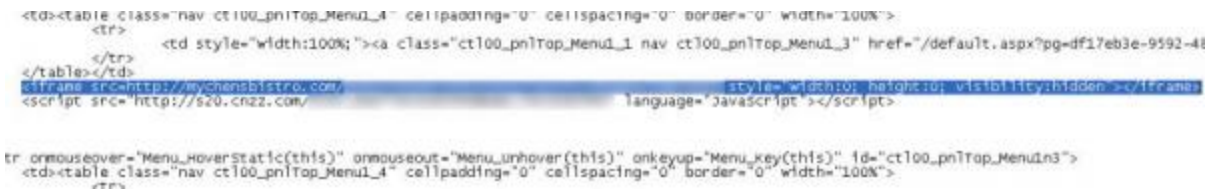

Figure 1: The hidden iframe tag can be seen, in addition to a link to cnzz, presumably for statistical purposes.

Although the scenario in question might be referred to as a "targeted attack," there are of course degrees of sophistication involved in every attack, and definitions of what is and is not a "targeted" attack tend to vary somewhat. In this case, given that the recipients were not Chinese, were not in any way related to a university, were not related to the topic on which advice was sought, and didn’t have anything to do with the presentation mentioned, one has to wonder why the attacker didn't do more to tailor the email message content to the recipient. In the environment in which they were presented, they truly stuck out like a sore thumb, and beg the question of whether this was indeed a targeted attack or just a random phishing expedition.

Either way, given that the exploit was hosted on a Web page belonging to the Chinese restaurant, the easiest way to force the compromise of one of our honeypot computers was to simply browse to that Web page using a vulnerable version of Internet Explorer. We braced ourselves for the impact, and with one seemingly innocent click of the mouse, the exploit triggered and our honeypot computer was duly compromised. The computer we used for this exercise had a fairly basic setup, but we had spent a bit of time trying to make it look

like a genuine person's computer and not just a clone. It had several bait files on it, many of which were viewed by the attacker, and some of which were “downloaded.” Scratch that. Let's call it what it is—some of which were “stolen.”

As mentioned in the previous blog, the exploit uses shell code to download and install a back door that then contacts 323332.3322.org (a dynamic DNS service based in China) on TCP port 80 and awaits further commands. It is interesting to note that the attacker used a brand-new exploit to compromise the computer, but then relied on a very old back door (detected by Symantec since January 2010) to set up remote access.

We didn't have to wait long. Just minutes after the back door was installed, the attacker started discovery of the compromised computer. Some of the commands used were as follows:

```
> ipconfig /all
> tasklist
> netstat -an
> net view
> qwinsta  (terminal services session information)
> net localgroup administrator4  (typo...)
> net localgroup administrators
> net view /domain
> net view /domain:home
> net view /domain:local
> ping [networked_machine] -n 1
> net use \\[networked_machine] "" /user:[networked_machine]\administrator
> net view /domain:workgroup
```

Figure 2: Some of the commands used by the attacker during their discovery phase

Notice the typo on line six? That’s always a good indication you are dealing with a human, as opposed to an automated script or bot. You can see the attacker was interested in the running processes, active connections, specific Windows configuration of the targeted computer, as well as any networked devices connected to the target. You can also see the attacker tried to connect to one of the networked devices using the administrator account. They failed, by design.

Immediately after this, the attacker uploaded a full file and folder listing for all local fixed drives. One of the bait files on the computer must have caught their attention early because the next action was to upload a .pdf file from the honeypot computer. Shortly after that, a base-64 encoded executable file was downloaded and executed on the compromised computer. It turned out to be a different back door, this time one that we hadn't previously seen. It resulted in a second connection to a different IP address and brought an infamous remote administration tool (RAT) known as Gh0st Rat to the party. Another of my colleagues

wrote about this remote access tool back in 2009 and included a very informative video showing what an attacker can do with one of these remote access tools. Take a look if you're not familiar; you may be surprised to see what can be done.

With the introduction of the Gh0st Rat tool, the majority of traffic was now encrypted using SSL, and sessions jumped between the original host at 323332.3322.org and the second back door command-and-control server the Gh0st RAT tool was downloaded from.

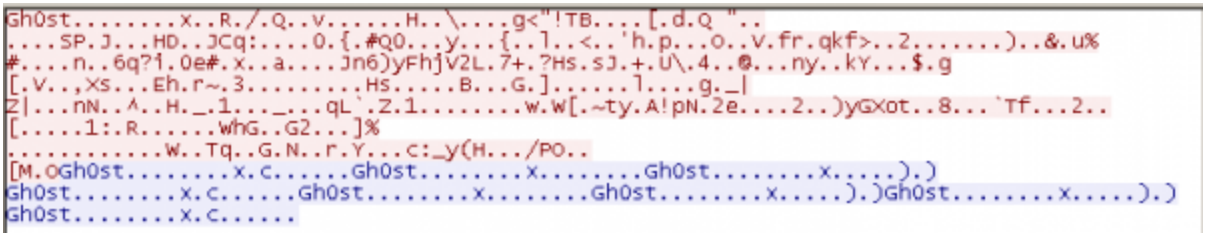

Figure 3: Encrypted traffic, but you can see the obvious references to "Gh0st"

We did see the Outlook Express mailbox file being uploaded as well, as well as the default browser bookmarks. During the short period we monitored the attack before disconnecting the honeypot computer from the Internet, we observed intermittent bursts of activity, but the majority of it took place soon after the honeypot computer was compromised. In total, there were approximately 2.5 megabytes of traffic to our honeypot computer originating from the attacker's two computers, and about 9 megabytes of traffic outbound to the attacker's computers.

So, be aware that the next time you click a URL in an email; you might get a lot more than you bargained for. Keep your security software up to date, and when Microsoft releases those patches, get 'em quick. Believe me, the bad guys are counting on you not doing so.

Note: *A special thanks to Henry Bell for his kind assistance with this article.*