Security Alert July 2nd, 2007: e-card infection

After receiving multiple alerts from the US-Certs and other federal agencies, RI DOIT sent the state-wide warning on June 29, 2007 about the e-card email distributed in an attempt to compromise computer systems.

The email with the subject line: "You've received a postcard from a family member!" contain links to a malicious Web site, where JavaScript determines whether the victim's browser has scripting enabled or turned off.

The greeting card email tries a trio of exploits, moving on to the second if the machine is not vulnerable to the first, then on to the third if necessary.

an exploit against a QuickTime vulnerability;

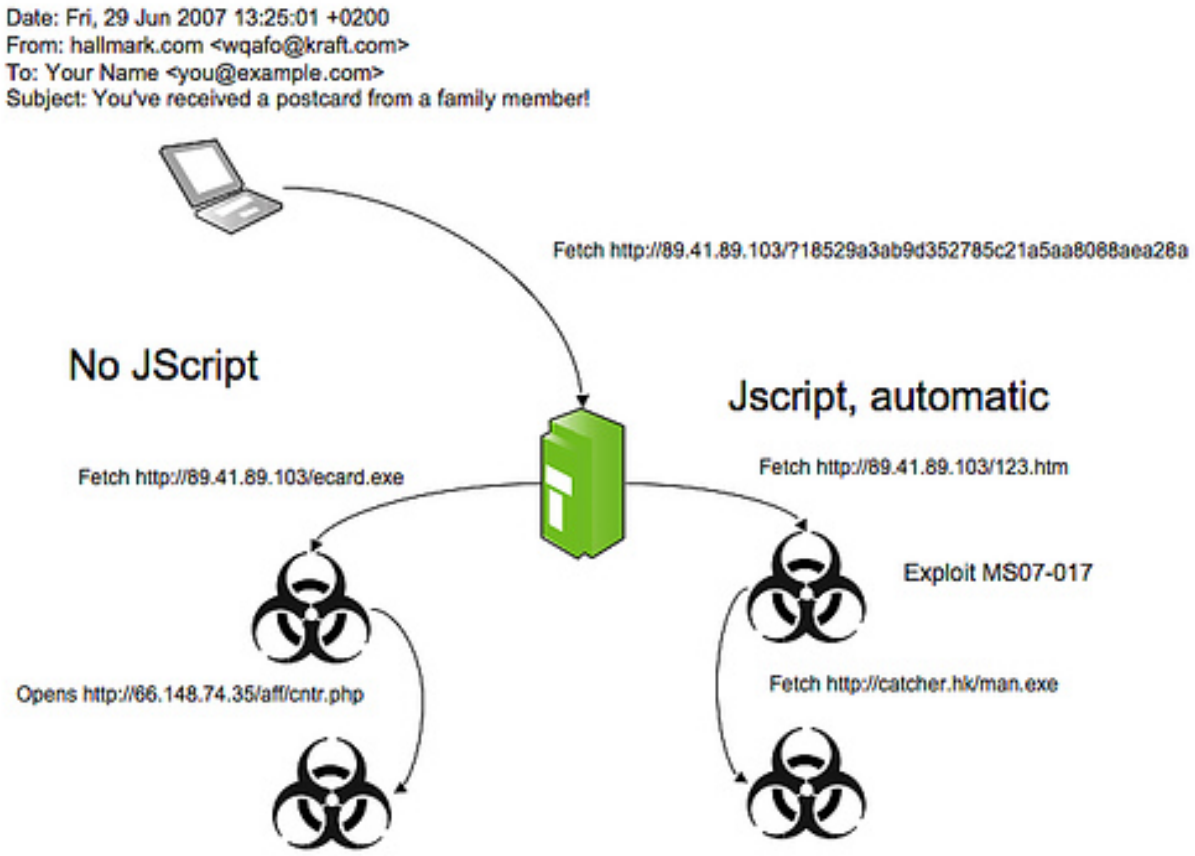
an attack on the popular WinZip compression utility;

an exploit for the WebViewFolderIcon vulnerability in Windows.

The email is very difficult to detect as it tries to exploit multiple vulnerabilities, is NOT tied to a single IP address and does not contain any attachments.

Here is a flow chart of the e-card takes the users from an email to the malicious web site:

Security Alert July 2nd, 2007: e-card infection



.The detection of the infection is hard at this time as there are multiple exploits involved including 2 application-known exlopits. If the workstation is infected, it becomes a "zombie" with a Peer-to-peer botnet component.

We are currently blocking any emails with the above-mentioned subject line. As of now 752 emails made into the State network (using only the State emails and not including DLT) since June 28th, 2007.

We've already blocked 6474 infected emails.

We will inform you about the e-card worm infection asmnore informtion becomes available.

Security Alert July 2nd, 2007: e-card infection

Please instruct your uses NOT to open or click on any links into the emails that come from unknown or unfamiliar senders.

More information can be found at:

http://isc.sans.org/diary.html?storyid=3063

http://www.microsoft.com/technet/security/Bulletin/MS06-057.mspx