CSO

FEATURE

Router malware: Fact or fiction?

Given that malicious software isn't always found locally on the machine itself, Ronald and Dylan Kaplan share how to pinpoint the characteristics of router malware

By Ronald Kaplan and Dylan Kaplan

CSO | Aug 28, 2014 11:17 AM PT

Malware affecting a computer's operation is not always found in the computer itself. Just recently we encountered a common operational issue on several computers in our home network. Various browsers on different computers running different operating systems were intermittently redirecting webpages. The issue manifests itself by redirecting webpages to an unfamiliar merchant site.

[Home routers: Broken windows to the world]

The confluence of characteristics of the particular malware, cache history of a user, settings on a particular computer, and how the aberrant browser behavior manifests itself can result in the troubleshooting effort becoming a head-scratcher. Issues relating to webpage redirection are likely attributed to a spurious domain name services (DNS) server.

[What's wrong with this picture? The NEW clean desk test]

DNS Server function

DNS servers are replicated all over the Internet and are fundamental to the user friendliness of the Internet. These servers enable users to browse the web using the friendly URL naming (e.g. Google.com) instead of the underlying IP address (74.125.239.37) that actually locates the servers containing the desired content.

The twist on this malware episode is that several computers with different operating systems (i.e. Windows 8, iOS7, OS X) were all affected, not all surfed websites would be redirected, some websites were DNS resolved on one computer but not on another. This complicated the effort of troubleshooting from the more familiar issues associated with contracting local malware. Why was this issue intermittent and not consistent among all computers on our network? How is it that multiple computers with different OSs were all infected? Why wasn't our anti-malware software able to identify or remove it?

Problem Isolation

A little troubleshooting effort enabled us to narrow the down what DNS server each computer was using, whether it is legitimate and how it was assigned to the computer. As we assembled the pieces, our router surfaced as the only common element. We have never personally seen or encountered router malware, so

this was a both intriguing and initially a bit scary. Our first thoughts were the usual, what personal information did the perpetrator harvest?

[Malware infections tripled in late 2013, Microsoft finds]

Next we thought, how were they able to penetrate our router? How will we be able to find the actual modifications to the router made by the malware? How will we be able to restore the router to its original functionality? Will we be able to make modifications to our router configuration to prevent future occurrences? Then came the panic: Whatever damage is occurring needs to cease immediately.

At this point we were not thinking about the trying to fully understand what had happened, how they got in, making copies of all the elements of the footprint the malware left, only how quickly we can reset the router, update the firmware and secure it better than before.

Malware which alters DNS settings often have an agenda; most collect money for website hits from merchant vendors. This is often the incentive for hackers to write and circulate their malware. The internet is rife with this type of fraud, where website hosts have contracted to pay for “hits” or views of their website instead of paying often large fees for directory listings creating web traffic.

The role of the router

Most routers are configured and managed remotely and are therefore configured to enable password protected remote login. Clearly, this is a vulnerability. If the router can be reconfigured, it can be made to malfunction. One service most routers provide is called DHCP (Dynamic Host Configuration Protocol). DHCP functions by loaning computers connected to the router information needed for them to send and receive information on the Internet, specifically an IP address. This is often performed by the router to enable computer networks to share a limited number of IP addresses among a large number of users. This is much the same as how telephone networks share a limited number of phone numbers with a larger number of employees. Much the same as a private phone line installed in an executive’s office, this IP assignment can also be done on individual computers without the aid of DHCP.

[Toss routers with hardcoded passwords, expert says]

Additionally, DHCP can be configured to provide primary and secondary DNS table locations (where the computers will look for the translation of google.com to 74.125.239.37) to the computers serviced by the router. The fact of whether or not DHCP was used on a particular computer in the subject network may not be initially known by the troubleshooter, which will likely add more confusion to the problem isolation effort. Since we determined that multiple computers connected to the router were affected, we focused our efforts on the configuration parameters of DHCP within the router.

Regardless of the OS connected computers are running, all computers utilizing DHCP to obtain their IP address or DNS table location would be equally affected.The seemingly unpredictable nature of the redirections might be attributable to the fact that DNS resolutions are temporarily stored in cache on user machines. Certain resolutions could have been placed in cache before the exploit and would therefore those sites could be addressed properly.

Hindsight is 20/20

Too many times in the past, network problems were solved without a real understating of what caused the problem, all the specifics of the symptoms and exactly what was done to resolve it. This is often very pragmatic, but not personally or professionally satisfying. There are steps, like restoring a backup, upgrading an application or operating system or rebooting, which will alleviate a problem, but will not provide good insight to how it got there or how to avoid its reoccurrence.

[Exploit released for vulnerability targeted by Linksys router worm]

In this case,we were able to isolate the source of the problem by virtue of the characteristics of the symptoms. Certain components could be eliminated from consideration by the global nature of the symptoms. Since hindsight is 20/20, it now appears obvious that the DNS server assigned by DHCP is likely what caused the symptoms we observed. We wish it was obvious when we first encountered the problem.

Mr. Ronald Kaplan, MS, MBA is a partner at SICons, a management consulting and computer forensic expert witness firm in Los Angeles. Dylan Kaplan, BS, is a recent graduate of the Eller College of Management at the University of Arizona, specializing in Management Information Systems. While at the University of Arizona, Dylan worked at Apple Inc. providing technical support.

Insider: How a good CSO confronts inevitable bad news ›