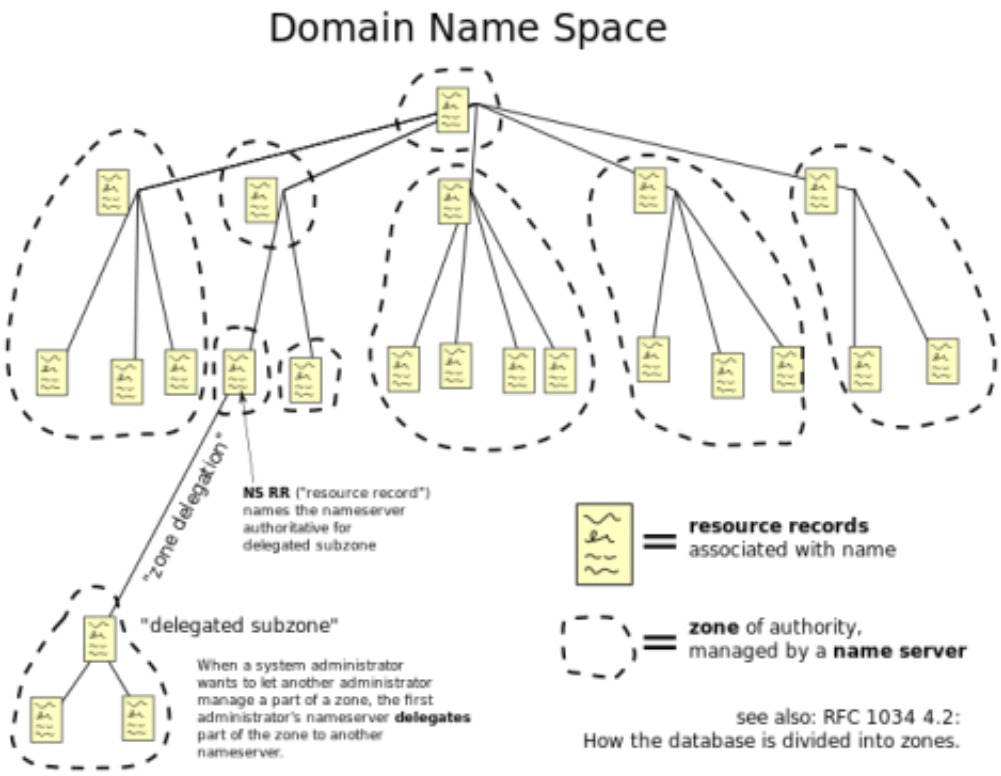
Microsoft No-IP takedown to strike malware draws protests

July 1 2014, by Nancy Owano



The hierarchical Domain Name System, organized into zones, each served by a name server. Credit: Public Domain

Microsoft on Monday staged a takedown of two malware families abusing no-IP services but, in the mission to take down the botnets, legitimate servers depending on dynamic domain name services from No-

IP were, as Dan Goodin of Ars Technica put it, caught in the crossfire. A substantial number of legitimate servers that rely on dynamic domain name services from No-IP.com suffered outages.

Many end users castigated the move as heavy handed. The gist of angry emails coming in from people at various news sites who said they were legitimate users conveyed a similar messages: Hey, Microsoft, who made you the DNS authority? Who gave you the right to sweep away domains? Microsoft had seized 22 domain names the computer giant said were being abused in malware-related crimes against Windows users. In doing so, Microsoft had taken legal steps to do so. Richard Domingues Boscovich, assistant general counsel, Microsoft Digital Crimes Unit, said in a TechNet blog post on Monday, "On June 19, Microsoft filed for an ex parte temporary restraining order (TRO) from the U.S. District Court for Nevada against No-IP. On June 26, the court granted our request and made Microsoft the DNS authority for the company's 23 free No-IP domains, allowing us to identify and route all known bad traffic to the Microsoft sinkhole and classify the identified threats."

While news sites were reporting on complaints by users of outages they were also careful to point out there was no evidence No-IP officially sanctioned or was in league with the malware operators named by Microsoft.

"Dynamic Domain Name Service (DNS) is essentially a method of automatically updating a listing in the Internet's address book, and is a vital part of the Internet. However, if not properly managed, a free Dynamic DNS service like No-IP can hold top-rank among abused domains," said Boscovich. He stated that "We're taking No-IP to task as the owner of infrastructure frequently exploited by cybercriminals to infect innocent victims with the Bladabindi (NJrat) and Jenxcus (NJw0rm) family of malware."

How bad was the threat? He said, "Our research revealed that out of all Dynamic DNS providers, No-IP domains are used 93 percent of the time for Bladabindi-Jenxcus infections, which are the most prevalent among the 245 different types of malware currently exploiting No-IP domains." Microsoft, he said, has seen "more than 7.4 million Bladabindi-Jenxcus detections over the past 12 months, which doesn't account for detections by other anti-virus providers."

Free Dynamic DNS is an easy target for cybercriminals, but it also is well liked by the innocent. Goodin of Ars Technica explained the good and the bad: "Dynamic DNS providers are popular because they allow people to obtain a free subdomain—such as dangoodin.no-ip.org—that automatically maps to whatever IP address the user's computer is using at the moment." The mapping changes each time the user's IP address is updated; Goodin said online gamers and Linux user group members are among the many who enjoy the services. The "but" in all this is that the services, he added, are also useful for "criminals running command and control servers that manage large numbers of infected computers."

Nonetheless, no-IP, which describes itself as offering Dynamic and managed DNS solutions, issued a formal statement on Monday that conveyed how unhappy the team was over the Microsoft takedown. "Millions of innocent users are experiencing outages to their services because of Microsoft's attempt to remediate hostnames associated with a few bad actors."

They said that "Microsoft never contacted us or asked us to block any subdomains" and that "Had Microsoft contacted us, we could and would have taken immediate action. The statement said that "this heavy-handed action by Microsoft benefits no one."

Meanwhile, Microsoft's Boscovich said in his blog posting that "This case and operation are ongoing, and we will continue to provide updates

as they become available."

More information: — blogs.technet.com/b/microsoft_ … ware-disruption.aspx

— arstechnica.com/security/2014/ … eizes-no-ip-domains/

— www.noip.com/blog/2014/06/30/i … -microsoft-takedown/ (NOTE: 5PM EST: the link is not accessible at present moment)