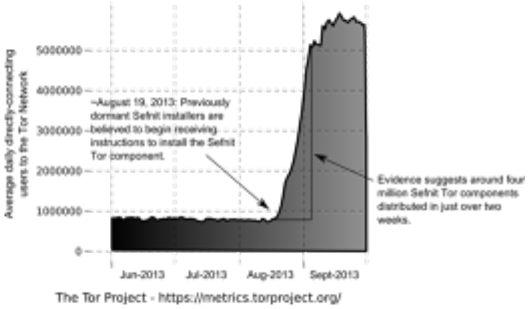
Microsoft Reveals Secret Ability To Remotely Uninstall Programs From Your Windows PC

After hackers started using a botnet to mass-download Tor clients, Microsoft committed a remote mass-uninstall across millions of personal computers.

By David Lumb (/user/david-lumb)

Last August, the Tor browser network received a massive spike of 4 million signups. As it turned out, a botnet was installing Tor on victims' PCs and using the browsers to start mining Bitcoins. Pressed between a rock and a hard place, Microsoft swiftly sent a remote command to uninstall the Tor browser (http://www.dailydot.com/technology/tor-botnet-microsoft-malware-remove/)--a backdoor which ostensibly no one in Windows-land knew existed.

As it turns out, Microsoft had accounted for this scenario--it's right there in Windows’ terms of service. As Microsoft explains in a blog post (https://blogs.technet.com/b/mmpc/archive/2014/01/09/tackling-the-sefnit-botnet-tor-hazard.aspx?Redirected=true), once the Sefnit malware that infected these computers starts downloading components, it keeps the computer connected to the Tor network even if Sefnit is uninstalled. Since that particular old Tor client doesn’t self-update, it would remain an open door for reinfection and given Tor's history of high-severity vulnerabilities, that was a weakness Microsoft couldn't abide.



The Tor Project - https://metrics.torproject.org/

This graph above tells the story week by week. Millions of computers that had been infected with the Win32/Sefnit malware powered up on August 19, 2013 and began using Tor. As Tor had just under a million users directly connected to the Tor network, a 400% spike in Tor network distributions over a two-week period was a pretty noticeable jump.

As the Daily Dot's Patrick Howell O'Neill points out (http://www.dailydot.com/technology/tor-botnet-microsoft-malware-remove/), using an exploit to install software in the background of Windows was a mistake, as it caught Microsoft's attention. The hackers also unintentionally formed a working relationship between Redmond and Tor developers: Microsoft says in its blog post that it "consulted with Tor developers" when deciding how to proceed. Tor developer Jacob Applebaum said that communication between Tor and the tech giant amounted to a single question: Whether a normal user would install Tor in the directory paths and as a service. Tor said that it was very unlikely--a solid clue to Microsoft that something nonhuman was installing Tor deep in Windows.

At the 30th Chaos Communication Congress in Hamburg on Dec 27, Applebaum shared details of the incident (https://www.youtube.com/watch?v=CJNxbpbHA-I#t=16) and his fears of Microsoft's ability to remotely rip pieces out of its

OS at will. Tor executive director Andrew Lewman, however, was less concerned: Having Microsoft keep your operating system "secure" is part of the opt-in terms of service.

[Image: Flickr user Alexei Kuznetsov (http://www.flickr.com/photos/8663336%40N03/5480421664/in/photolist-9mhAgG-9qCnaQ-bp6yrx-86dFAN-bognwf-bBkhgg-bognKJ-9dUAHT-bpixTw-8nfNfi-9MGksj-fgyYUS-dNpMtP-bzKxaR-7xGBFb-8yoQum-bJ9pgp-8htxUU-7B8Lrn-dE2CEF-9AiGwR-7X9tt2)]

DAVID LUMB

David Lumb is an all-around reporter who has dabbled in the startup world and once did an investigative article on pizza.

(http://www.fastcolabs.com/user/david-lumb) Continue (http://www.fastcolabs.com/user/david-lumb)

January 21, 2014 | 3:28 PM

YOU MIGHT ALSO LIKE

(http://www.infoworld.com/d/microsoft-windows

ADD NEW COMMENT

LOG IN

Type your comment here.

0 COMMENTS

No comments yet. Be the first!