Endpoint Protection

symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs

Back to Library

Malware Targeting Windows 8 Uses Google Docs

1 Recommend

Nov 16, 2012 05:55 PM

Migration User

Initially, I thought that Backdoor.Makadocs was a simple and typical back door Trojan horse. It receives and executes commands from a command-and-control (C&C) server and it gathers information from the compromised computer including the host name and the operating system type. Interestingly, the malware author has also considered the possibility that the compromised computer could be running Windows 8 or Windows Server 2012.

Figure 1. *Operating Systems check*

Windows 8 was released in October of this year. This is not necessarily a surprise for security researchers as we always encounter new malware when new products are released. However, this malware does not use any particular function unique to Windows 8 and we know that this malware existed before the launch of Windows 8. Based on these facts, we believe this code must be an update to the malware.

Next, I would like to introduce a very unique feature of Backdoor.Makadocs. The latest version of Makadocs does not connect to a C&C server directly, rather, it uses Google docs as a proxy server.

__Figure 2.__ Backdoor.Makadocs connection route

Google docs has a function called viewer that retrieves the resources of another URL and displays it. Basically, this functionality allows a user to view a variety of file types in the browser. In violation of Google's policies, Backdoor.Makadocs uses this function to access its C&C server. It is possible that the malware author has implemented this functionality in an attempt to prevent the direct connection to the C&C from being discovered. The connection to the Google docs server is encrypted using HTTPS, thereby making it difficult to be blocked locally. It is possible for Google to prevent this connection by using a firewall.

We confirmed that Backdoor.Makadocs arrives as a Rich Text Format (RTF) or Microsoft Word document.

__Figure 3.__ Malicious Microsoft Word document

Presently, this document does not utilize any vulnerability in order to drop its component, instead, it relies on social engineering tactics. It attempts to pique the user’s interest with the title and content of the document and trick them into clicking on it and executing it. The following code extract leads us to believe that the malware primarily targets people living in Brazil.

__Figure 4.__ Targeting users in Brazil

Symantec products detect the RTF and Microsoft-Word files as Trojan.Dropper. To stay safe, please ensure that you have the latest patches installed on your computer and keep your antivirus definitions up-to-date.

Statistics

0 Favorited

0 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.