Bebloh – a well-known banking Trojan with noteworthy innovations

gdatasoftware.com/blog/2013/12/23978-bebloh-a-well-known-banking-trojan-with-noteworthy-innovations

The banking Trojan Bebloh has been known about and studied for a number of years. But even new developments in the malware have not produced any notable innovations – until recently. The observed infection rates with Bebloh in the first half of 2013 were comparatively small – with a share of just 6.3% among all banking Trojans observed by G Data, Bebloh was lagging far behind competitors such as ZeuS. However, an update appeared recently that contains noteworthy changes.

Large increase in infection count following update

In recent months we started seeing alarming new figures: Bebloh started steadily climbing up the statistics ladder and secured a place for itself among the top three banking Trojans in November.

Recently, the malware was distributed as an email attachment, as spam containing fake flight information. Taken everything into consideration, this was more than reason enough to look into what was going on.

An initial comparison between a newer example and the familiar version shows that Bebloh has clearly undergone an update. Only about 75% of the functions in the two versions are the same. Almost 4.5% of the functions in the old version have been deleted or replaced. 20.9% of the functions are exclusively found in the new version. The functional scope has therefore been significantly enhanced.

Malware undergoing change: AV evasion

The interesting innovation in this variant concerns the persistence, or the issue of: how does the malware survive a restart?

As soon as the system is infected by Bebloh, the malware is injected into explorer.exe and the original executable file that contains Bebloh is deleted. In principle this is a perfectly normal procedure for concealing the malware's entry point into the system. However, what is interesting is the fact that the malware is not then moved to another folder and no autostart entry is generated. The malware is no longer found on the hard disk. Therefore, a conventional signature-based virus scanner would fail to find any infection by scanning the

hard disk. As the malware is running hidden in the explorer.exe memory, not even a malicious process is detected. However, to survive a system restart, Bebloh uses an interesting trick.

An invisible window is generated from the explorer.exe process to receive the “Window Messages”, a specific message type generated by Windows.

This means that windows concerning an impending computer shutdown are also issued by Windows.

As soon as Bebloh receives such a message, the malware writes its executable file out of the explorer.exe memory to the hard disk, and an autostart pointing to the executable is generated. Hence throughout the time the system is running, there is virtually no visible clue in the registry or on the hard disk that suggests an infection.

To exacerbate the cat-and-mouse game between AV providers and Bebloh even more, the autostart entry doesn't directly reference the executable file – it relies on a link (.lnk). In addition, the file name used by Bebloh is generated randomly each time, so Bebloh has a different name each time the system is started.

Outlook

The above-mentioned comparison of the program code for the two versions studied proves the hypothesis that Bebloh has not changed much in its basic function as a banking Trojan and still tries to spy on user data. However, the AV evasion updates are something new in the banking Trojan arena, demonstrating that malware authors are continuing to find new ways to prey on their victims even more silently and effectively.

G Data detects the new variant as Trojan.GenericKD.1367361 using the DoubleScan technology. G Data BankGuard also detects and removes the new variant of this malware.

Older Bebloh version, SHA256:
01af2a82eddbfc4dc4720c8e8a483ff91d3b12df792928a435d1fc618055db46

Newer Bebloh version, SHA256:
d4f6a12ffe35a8b39e047d35bedb2860e622580df8d66c68abaad4c8d8162c6a