ISFB: Still Live and Kicking

journal.cecyf.fr/ojs/index.php/cybin/article/view/15

Maciej Kotowicz CERT PL

DOI: https://doi.org/10.18464/cybin.v2i1.15

Abstract

ISFB is also known as Gozi2/Ursnif, sometimes Rovnix. ISFB reappeared in early 2013 attracting some attention from the research community and a lot of confusion in the naming convention and to what was being analyzed. Then suddenly, it went dark again. However, dark does not mean dead. With attention of the world focused on Dridex and Dyre, ISFB silently evolved, hiding from the spotlight to become one of the most complex and fully featured banking trojans out there In this paper, we break the silence surrounding ISFB, giving a full description of this malware capabilities which are beyond those of the average banking trojan: 4 ways of communicating with the CC, half a dozen tricks to steal your money, the ability to create movies of your activity and naturally numerous ways of manipulating your web traffic.

References

[1] D. Jackson, “The unrelenting evolution of vawtrak.”, https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak, 2014.
[2] N. Kuzmin, “Gozi v1 leak,” 2010.
[3] Horgh, “Ursnif still in active development.” http://blog.howpublishedsonmalware.se/post/2014/10/09/Ursnif-still-in-active-development, 2014.
[4] unknown, “Isfb leak.”, https://github.com/gbrindisi/malware/tree/master/windows/gozi-isfb, 2015.
[5] GovCERT.ch, “Gozi isfb - when a bug really is a feature.”, https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature, 2016.
[6] Proofpoint, “Nightmare on tor street: Ursnif variant dreambot adds tor functionality.”, https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality, 2016.
[7] L. Kessem and L. Keshet, “Meet goznym: The banking malware offspring of gozi isfb and nymaim.”, https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/, 2016.
[8] J. Jedynak and M. Kotowicz, “Nymaim: the untold story,”, https://lokalhost.pl/talks/vb2016/, 2016
[9] Kafeine, “A fileless ursnif doing some pos focused reco.”, http://malware.dontneedcoffee.com/2015/07/a-fileless-ursnif-doing-some-pos.html, 2015.

[10] J. Grunzweig and B. Levene, “Powersniff malware used in macro-based attacks.”, http://researchcenter.paloaltonetworks.com/2016/03/powersniff-malware-used-in-macro-based-attacks/, 2015.
[11] D. Kizhakkinan, Y. Wang, D. Caselden, and E. Eng, “Threat actor leverages windows zero-day exploit in payment card data attacks.”, https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html, 2016.