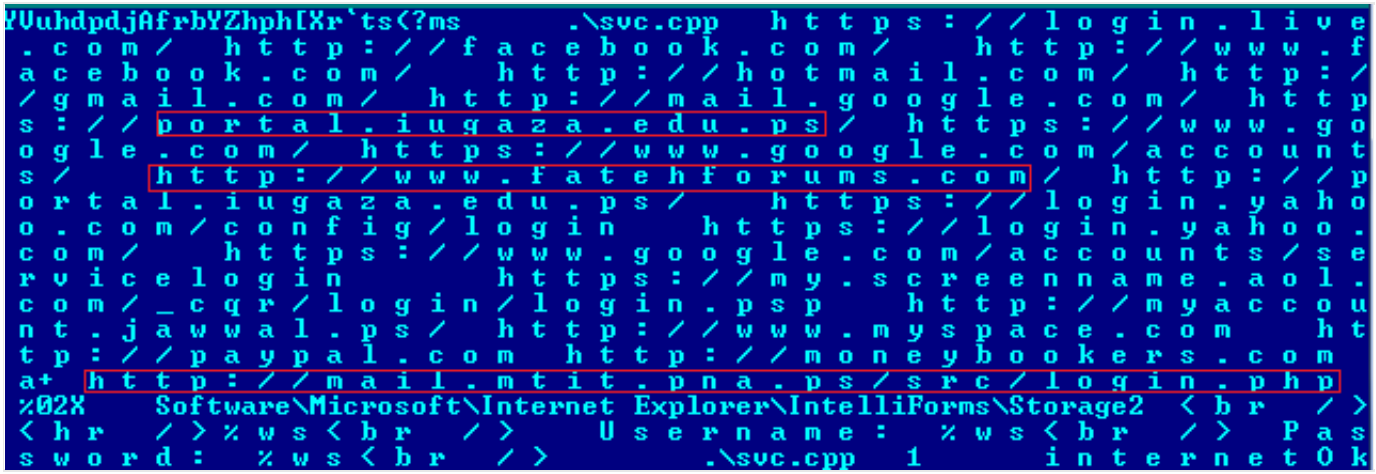
Palebot trojan harvests Palestinian online credentials

December 8, 2011 by Snorre Fagerland -

I sometimes sample the stream of files that come from VirusTotal, so as not to lose touch with what malware is actually floating around. Of special interest are the files where few or only we have detection, because there is a higher probability that such files are false positives that need to be removed. However, yesterday I found an interesting file.

Firts of all, it was relatively clear that it was no false positive, since sandbox and live systems confirmed that it installed using the file name svcshost.exe. It was obviously mimicking the legitimate program svchost.exe, which is a pretty telling hint.

Looking at the file revealed out-of-the ordinary traits. It was over 750k in size, and this is somewhat unusual for trojans. It was not packed or obfuscated, so by just looking at the file image some strings jumped out:



The lowermost of these URL's appears to be a webmail front for the Palestinian National Authority. The list shown is used as input to a function that has as purpose to grab user credentials from IntelliForms. IntelliForms is the name for the autocomplete function that exists in Internet Explorer. The full list of targeted sites is:

"https://login.live.com/"
"http://facebook.com/"
"http://www.facebook.com/"
"http://hotmail.com/"
"http://gmail.com/"
"http://mail.google.com/"
"https://portal.iugaza.edu.ps/"

“https://www.google.com/”
“https://www.google.com/accounts/”
“http://www.fatehforums.com/”
“http://portal.iugaza.edu.ps/”
“https://login.yahoo.com/config/login”
“https://login.yahoo.com/”
“https://www.google.com/accounts/service”
“https://my.screenname.aol.com/_cqr/login.psp”
“http://myaccount.jawwal.ps/”
“http://www.myspace.com”
“http://paypal.com”
“http://moneybookers.com”
“http://mail.mtit.pna.ps/src/login.php”

Digging further into the origin of this file, I find that it is dropped by a WinRAR SFX installer which also extracts and shows the document below (excerpt):

أكد الرئيس محمود عباس مساء الثلاثاء أن السلطة الفلسطينية ستكون من حق من يفوز بالانتخابات القادمة، قائلاً: "حتى لو فازت حماس فسنترك لها السلطة دون أي تردد ودون ربيع عربي."
وقال الرئيس خلال لقاء مع رؤساء التحرير في الصحف المصرية في القاهرة مساء اليوم إن الحكومة المزمع تشكيلها ستكون تكنوقراطية من المستقلين، وهي ليست حكومة وحدة وطنية، وهذه الحكومة أنا مسئول عنها."
وأضاف أن لحكومة التكنوقراط ستكون بمهمتين أساسيتين تتمثل في إعمار قطاع غزة، والإعداد للانتخابات، ومن هنا أي وزير سيكون في هذه الحكومة يجب أن يتمتع بحرية السفر والحركة للخارج.'
وفيما يتعلق باستعداد الرئيس للذهاب لانتخابات مبكرة يتم من خلالها إنهاء الانقسام، قال: "لا مانع لديَ بأن تجرى الانتخابات بعد ثلاثة أشهر من الآن، والانتخابات عندنا تتم بشفافية وإشراف دولي ولا أحد بإمكانه التشكيك بنزاهة هذه الانتخابات.'

The full text seems to be taken from an article in the Palestinian newspaper Al-Sabah (Google translated): www.alsbah.net.

The document, *aylol.doc*, contains very little metadata, so we are not talking about complete newbies in

the targeted attack business.

There are apparently at least two versions of this trojan around. Norman Sandbox technology detected these proactively as W32/Malware, but they will be renamed to Palebot.A!apt and B!apt.

The trojan is still in analysis, and further details may be published later.

MD5′s of samples:

7f3b74c9274f501bf0d9ded414b62f80
25f758425fcea95ea07488e13f07e005
1954622c1fe142200ad06eec12291fcd (RAR SFX).