An Overview of a Color-coded Multi-Stage Arsenal

By GReAT on April 11, 2017. 9:59 am

Yesterday, our colleagues from Symantec published their analysis of Longhorn, an advanced threat actor that can be easily compared with Regin, ProjectSauron, Equation or Duqu2 in terms of its complexity.

Longhorn, which we internally refer to as "The Lamberts", first came to the attention of the ITSec community in 2014, when our colleagues from FireEye discovered an attack using a zero day vulnerability (CVE-2014-4148). The attack leveraged malware we called 'BlackLambert', which was used to target a high profile organization in Europe.

Since at least 2008, The Lamberts have used multiple sophisticated attack tools against high-profile victims. Their arsenal includes network-driven backdoors, several generations of modular backdoors, harvesting tools, and wipers. Versions for both Windows and OSX are known at this time, with the latest samples created in 2016.

Although the operational security displayed by actors using the Lamberts toolkit is very good, one sample includes a PDB path that points to a project named "Archan~1" (perhaps 'Archangel'). The root folder on the PDB path is named "Hudson". This is one of the very few mistakes we've seen with this threat actor.

While in most cases the infection vector remains unknown, the high profile attack from 2014 used a very complex Windows TTF zero-day exploit (CVE-2014-4148).

Kaspersky Lab products successfully detect and eradicate all the known malware from the Lamberts family. For more information please contact: intelreports@kasperskycom

An Overview of the Lamberts