Virus Bulletin :: Linking Xpaj and Nymaim

Thursday 5 October 10:00 - 10:30, Red room

Doina Cosovan (Security Scorecard)
Catalin Valeriu Lita (Security Scorecard)

Interesting things have been written before about the Xpaj and Nymaim malware families. Xpaj has been known since 2008 and was dubbed one of the most advanced file infectors. Its purpose is click fraud achieved through various sophisticated mechanisms. Meanwhile, Nymaim, which appeared on the malware scene in 2013, is a downloader that spreads various malware families. It is well known for using an advanced custom obfuscation engine, which makes it very difficult to analyse the code.

Although there are many technical articles and white papers describing each of these malware families separately and in great detail, up until now, we are not aware of any correlation having been made between the two families. Indeed, from a high level overview, they don’t seem to share any similarities other than the fact that both of them are hard to analyse. However, at a reverse engineer's level, we have discovered interesting similarities in the domain generation algorithm, the communication protocol, the compression technique (the custom "ARCH" structure known to be used by Nymaim in order to keep the aplib32 compressed data is also used by Xpaj), the encryption/decryption algorithms (for example, all Nymaim and Xpaj samples have been using the same algorithm for decrypting strings since 2008, when the first Xpaj samples were identified in the wild), and the way in which the code is written and obfuscated.

There are two interesting details which we would like to highlight in order to make the similarity incontestable. One of these is that we came across Xpaj and Nymaim samples that were using the same RC4 encryption key. The other is that we found an Xpaj dropper from 2012 that has the same MZPE header stub as some Nymaim samples from 2014. The only differences between the header of that particular Xpaj dropper and the header of the unpacked Nymaim samples were the size of image, the checksum, and the entry point. This means they have the same value even for fields such as the linker version (1.67) or the timestamp (2007-10-31 11:11:38). These fields are usually generated by a compiler, but it is not unusual for malware writers to generate an MZPE header and use it for multiple samples by changing only some specific fields required for the code to execute properly. One of the reasons for doing this is to avoid using tools which will add traceable information inside the headers. Thus, the fact that we found so many similarities, and the fact that the same MZPE header stub and the same RC4 key were used for samples from both malware families, suggests they were created by the same cybercriminals. The reason the link between these malware families has gone unnoticed for so long is partly because of the advanced polymorphic engine which managed to make the code unrecognizable. At this moment, we can confidently claim that there is a strong connection between the two malware families.

Doina Cosovan

Doina Cosovan received Bachelor's and Master's degrees from the Alexandru Ioan Cuza University of Iași, Faculty of Computer Science, where she is currently pursuing a Ph.D. She was recruited for *Bitdefender*'s malware research team in her second year of college, where she worked for five years prior to joining *Security Scorecard*. Some of her interests include malware, botnets, reverse engineering and machine learning.

Cătălin Valeriu Liță

Cătălin Valeriu Liță received a Bachelor's degree in computer science from the Technical University Gheorghe Asachi, Romania, Iasi, Faculty of Automatics and Computer Science. He also has a Master's degree in information security from the Alexandru Ioan Cuza University of Iași, Faculty of Computer Science, and another Master's degree in business administration from the Alexandru Ioan Cuza University of Iași, Faculty of Economics and Business Administration. Currently he is pursuing a Ph.D. at the Faculty of Computer Science. Prior to joining *Security Scorecard* he worked for nine years in *Bitdefender*'s anti-malware team.