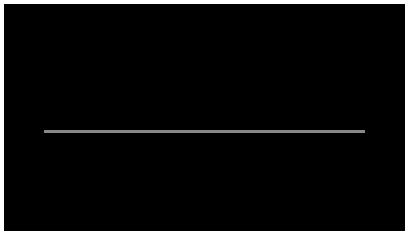
EHDevel – The story of a continuously improving advanced threat creation toolkit

By Alexandru MAXIMCIUC

Archived: 2026-04-05 18:30:06 UTC

More than a year ago, on July 26th 2016, the Bitdefender Threat Intelligence Team came across a suspicious document called News.doc. However, unlike most potentially malicious documents that get processed in our labs, this file displayed similarities with a set of files known to have been used in separate attacks targeted at different institutions.

Our technical dive into the file lead us to a sophisticated malware framework that uses a handful of novel techniques for command and control identification and communications, as well as a plugin-based architecture, a design choice increasingly being adopted among threat actor groups in the past few years.



Dubbed EHDevel, this operation continues to this date, the latest known victims reportedly being several Pakistani individuals. In their case, the threat actors have chosen different lures than the ones presented in this paper, but the modus operandi is identical. Another important discovery lies in the fact that this specialized framework that has been used to gather field intelligence for years in different shapes and forms, and our threat intelligence suggests a connection with the 2013 Operation Hangover APT as well. Our technical dive into the framework revealed an intricate mix of transitions from one programming language to another, code under active development and bugs that were not spotted during the QA process (if there were any).

Midway through our research, additional technical information and news of EHDevel framework have emerged. You can find a partial technical description of EHDevel over at 4HOU (warning: Chinese), as well as news on the India/Pakistan cyberattack in a Reuters report.

Download the whitepaper
