1500 - Digital Vengeance: Exploiting the Most Notorious C&C Toolkits

Saturday at 15:00 in Track 4
45 minutes | Demo, Tool, Exploit
Professor Plum*Hacker*

Every year thousands of organizations are compromised by targeted attacks. In many cases the attacks are labeled as advanced and persistent which suggests a high level of sophistication in the attack and tools used. Many times, this title is leveraged as an excuse that the events were inevitable or irresistible, as if the assailants' skill set is well beyond what defenders are capable of. To the contrary, often these assailants are not as untouchable as many would believe.

If one looks at the many APT reports that have been released over the years some clear patterns start to emerge. A small number of Remote Administration Tools are preferred by actors and reused across multiple campaigns. Frequently sited tools include Gh0st RAT, Plug-X, and XtremeRAT among others. Upon examination, the command and control components of these notorious RATs are riddled with vulnerabilities. Vulnerabilities that can be exploited to turn the tables from hunter to hunted.

The presentation will disclose several exploits that could allow remote execution or remote information disclosure on computers running these well-known C&C components. It should serve as a warning to those actors who utilize such toolsets. That is to say, such actors live in glass houses and should stop throwing stones.
Professor Plum
Professor Plum is an experienced reverse engineer, developer, and digital forensics examiner. He holds a graduate degree in Information Security from Johns Hopkins University, and has worked numerous computer incident investigations spanning the globe. He currently works as a Senior Threat Researcher for a Fortune 500 cybersecurity company and previously worked for the Department of Defense performing vulnerability research, software development, and Computer Network Operations.

@professorplum

#defcon25/by_track/track4/saturday #defcon25/By_Day/_saturday