RadRAT: An all-in-one toolkit for complex espionage ops

labs.bitdefender.com/2018/04/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/

Bogdan BOTEZATU

April 13, 2018

Around February this year, we came across a piece of malware that had previously gone unnoticed. Buried in the malware zoo, the threat seems to have been operational since at least 2015, undocumented by the research community.

Our interest was stirred by its remote access capabilities, which include unfettered control of the compromised computer, lateral movement across the organization and rootkit-like detection-evasion mechanisms. Powered by a vast array of features, this RAT was used in targeted attacks aimed at exfiltrating information or monitoring victims in large networked organizations.

In addition to its very powerful data exfiltration mechanisms, RadRAT features extremely interesting lateral movement mechanisms that

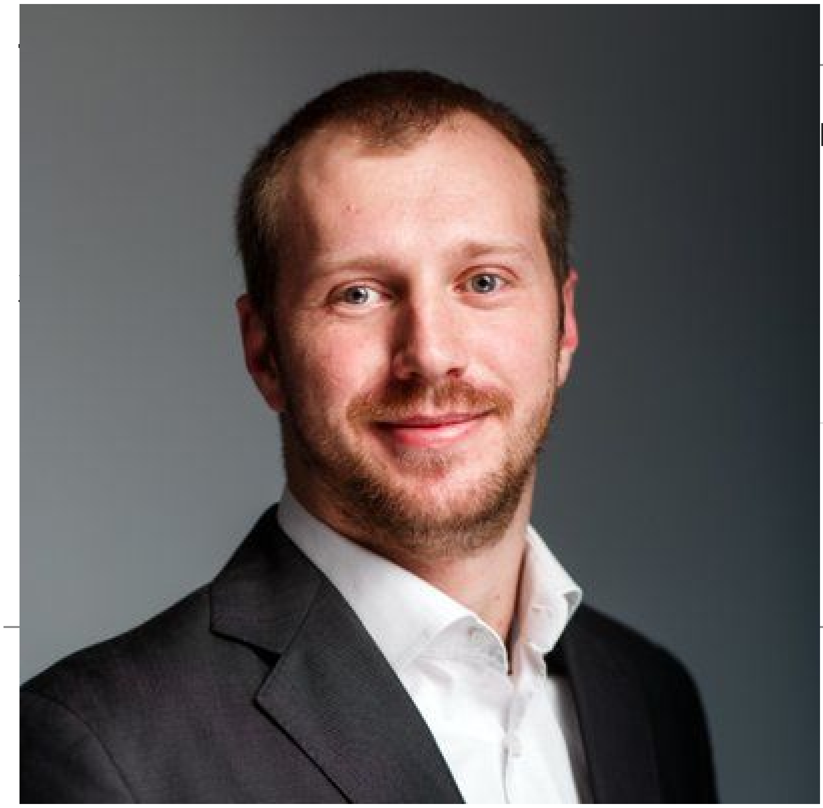
– Mimikatz-like credentials harvesting from WDigest.dll and kerberos.dll;
– NTLM hash harvesting from the Windows registry, inspired from the source code of the Mimikatz lsadmp tool;
– Using the infected machine to retrieve a Windows password from the LanMan (LM) hash, by cracking previously sniffed NTLM authentication challenges;
– An implementation of the Pass-the-Hash attack on SMB connections.

Download the whitepaper

TAGS

anti-malware research whitepapers

AUTHOR



hood at @Bitdefender as director

Bookmarks