Winnti uses the of exploit RT to targeting Vietnam

Nguyen Anh Hoang
Nguyen Van Thai

Intro
Analysis
Threat Intelligence
Appendix

In late 2019, Cheetah of
C:\Users\public\Libraries\PRINTER\Printer\Lib\x64\x86\TCP\TCP\TCP.exe exploit the zero-day vulnerabilities in Kingsoft Antivirus and Microsoft Office (CVE-2018-8373, CVE-2018-8174, CVE-2018-8453, CVE-2018-8654) to deliver a backdoor to victim's machine. The backdoor is a variant of Winnti family, which is known as Shadowpad. Shadowpad is a modular backdoor, which has been used by APT 17 (Operation Shadowhammer) and APT 41 (Operation ShadowPad). Shadowpad has been used by Winnti group since at least 2017. Shadowpad is a modular backdoor, which