“ ”

“ “ WRAT ”

”

Empire Exploit Pack

C++

U

Python https://mp.weixin.qq.com/

“ ” Go s/y2kRbYCt94yPu-5jtcZ_AA

APT CERT APT

2020 1 15 “ ” “ ”

[1]

“ ” “ ”

2017 7 LNK HTA

Shell “ WRAT ”

CERT Windows

Windows IP IP

Vovalex 4 IP

2021 1 3389 445 139 135 3

D 5

4

6

5

1

1

2 PowerShell

16 IIS

Cookie

3 2 IP

Accurics Å´

Ç H Ɐ A ﻫ ﻕ

A ﺝ ΌO ω ΌO ﻍ