Xorist

AES+RSA
.ZaLtOn

CERT

Xorist

Xorist

2020 10

IEP

Xorist

“ .ZaLtOn ”

“ HOW TO DECRYPT FILES.txt ”

Ú 3 2

“ C:\Users\ \AppData\Local\Temp ”



“ AES+RSA ”

木马程序

Trojan[Ramsom]/Win32.Xorist

Run	

WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Ofÿce 2003 Flash WPS FoxitReader Adobe Reader

安天周观察
2020 12 07 (257) 4

Ŗ ő ő Ľ 3 . . Ŗ t Ω Ϥ ή Ɣ

11 30 2020

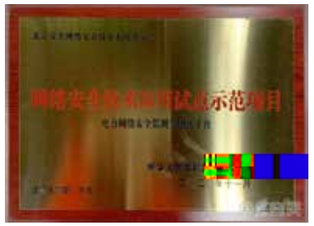
“

”

0.0.

0.0.





“ 2020

” 20

“ ”“ ”“ ”“ ”

APT

2019 “

”

“

” “

” “

” “ 2020

”

IP URL

HASH

“ ”

” “ ”



APT

C2



（下转第二版）