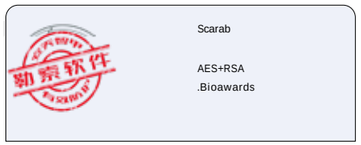
‰ώ ک ﻻ ﻭ ﺇ Qa_p_` ɢ Δ ئ ر



CERT

Scarab

Scarab

2020 11

IEP

Scarab

14

“ .Bioawards ”

“ DECRYPT FILES. TXT ”

96



▲

“ AES+RSA ”

VPN

木马程序

Ł ˬ Ï BD ﻉ ﻝ ɻ YARA
Ɱ ﻝ ɻ Ḥ ﻝ ɻ ë ﻝ ɻ ѽ Ḥ
ﻝ ɻ ﻉ ﻝ ɻ ů ﻝ ɻ ˜ Ѓ WinXP Є ﻝ ɻ
Ч ﻉ ﻝ ɻ й ﻝ ɻ Õ Ļ Ŋ ǐ Ѓ ¾ P ' N ¯ N
Ö B Ĥ

Trojan[Ransom]/Win32.Scarab

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

DLL	
.....	.....

HTML	

安天周观察 2020 12 21 (259) 4 IT

DgpcCwc ł V ώ ` Δ h

FireEye FireEye

CERT

FireEye Windows

FireEye SolarWinds Orion

2020.2.1 HF1 2020

12 15

2020.2.1 HF2

CERT D Golang C

ATT&CK CERT

CERT FireEye D

CommandoVM

“

Qmj_pUglbq ث ـ Δ ruten ɜ ɦ ؤ” X̂ urtigruten Δ h

ـ ا

C2

（

下方二维

wordpre

hurtigrut

