Deniz_ Kızı

CERT

“ Deniz_Kızı ”

Keslan

2019 12

W BD “ svchost. " B

	deniz_kizi.exe
	BinExecute/Microsoft.EXE[:X86]
	1.23 MB
KB3	583212EB42CE3662B399693BBB7D5FD2
	[redacted]
-	Trojan/Win32.Graftor
	BD

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

UAC	

DLL	
.....	.....

安天周观察
2020 1 13 (216) 4 antiylab

2020 1 8

ATT&CK

AI 5G

“ ”

“ ”

CNCERT

APT

/

CERT 2019

2020 .

ATT&CK ODNI

TCTF

ATT&CK

2000 TCTF

ATT&CK

	Lazarus AppleJeus
英文标题	Operation AppleJeus Sequel Lazarus continues to attack the cryptocurrency business with enhanced capabilities
	GReAT
	Lazarus AppleJeus Lazarus macOS Object-C GitHub Windows Lazarus wfcwallet .NET WFC C2 RasMan Windows
	https://securelist.com/operation-applejeus-sequel/95596/

2020 年七大网络趋势