安天周观察

2020 4 6 (225) 4 antiylab

wisecleaner.com Windows

CERT

CoronaVirus KPOT CERT

CoronaVirus

KPOT

CoronaVirus 2020 IEP KPOT

3 RSA+AES CoronaVirus

CoronaVirus.txt ATT&CK

0.008 (50 1.

) •

KPOT



▲ ATT&CK

VPN RDP FTP

CERT 2019

CERT

wisecleaner.best

CoronaVirus trynda. •

xyz KPOT trynda.

CoronaVirus KPOT xyz 2 file1

KPOT Cookie file2 file1 KPOT file2

CoronaVirus

2. KPOT

•

KPOT

▲ VPN RDP

Trojan/Win32.DelShad

DLL	

UDP

IP		IP	
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.111	68
192.168.122.61	138	192.168.122.111	138
192.168.122.111	138	192.168.122.255	138
192.168.122.111	137	192.168.122.61	137
192.168.122.111	137	192.168.122.255	137

TCP

IP		IP	
192.168.122.111	1352	192.168.122.61	139

2020 4 6 (225)
antiynews@antiy.cn

FBI	Kwampirs
FBI Warns of 'Kwampirs' Malware Supply Chain Attacks	
Marianne Kolbasuk McGee	