2021 10 25 (299)

CAR

SIEM SOC https://mp.weixin.qq.com/s/pNIUTCSwn-4MUbDTpQV1gA

8

	network02.exe
	BinExecute/Microsoft.EXE[:X64]
	4.50 MB
MD5	F0CF1D3D9ED23166FF6C1F3DEECE19B4
	[redacted]
/	RiskWare[RiskTool]/Win32.BitMiner

https://1.119.163.6/vue/details?hash=F0CF1D3D9ED23166FF6C1F3DEECE19B4

File Size	4.5 MB

7 CERT FTP

FormBook

FormBook

2016

IEP

4.1

3.2

FormBook

2020

2021

“ ”

“ ”

SaaS

92% IT

IT

IT 50%

IT

SaaS

26%

2021

SolarWinds

1