周观察

2021 09 20 (296) 4

“ ”

“ ”

BD YARA WinXP

Win7 x86

Win7sp1 x86 BD

	LockBIT_7D68A5BFD028A31F.exe
	BinExecute/Microsoft.PE[:X86]
	863 KB
MD5	66B9CCB41B135F302B3143A5D53F4842
	[redacted]
/	RiskWare[RiskTool]/Win32.Shell2exe

https://1.119.163.6/vue/details?hash=66B9CCB41B135F302B3143A5D53F4842

WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Offce2003 Flash WPS FoxitReader AdobeReader

https://mp.weixin.qq.com/s/K3b-CVMkzTabQpIhUHU_hw

DR

IT

AWS Google D

Azure D

DR

AWS Google Azure D

D

DR

“ ”

Ľ Ľ Azure AWS EC2

AWS Google Cloud Platform GCP

AWS DR

Azure GCP

AWS Azure

GCP

Ľ Ľ

SQL SAP ERP

ů