BD YARA Win7 x86

BD

WinXP)

, ,			
		PE	

CERT

Tellyouthepass

2019 3

All Users

dVBRr.txt

All

Ä Ŗ Ŗ5

Users

.locked

IEP README.html

Tellyouthepass VPN

Tellyouthepas User_ID

CMD		Tellyouthepass	
DLL		AES+RSA	

C Users





CEO

Dharma 勒索软件提供黑客工具包以简化网络犯罪

Dharma RaaS

RaaS

https://www.bleepingcomputer.com/news/security/dharma-ransomware-created-hacking-toolkit-to-make-cybercrime-easy/

Windows 10

类 型	
中文标题	Group-IB APT RedCurl
	Rent a hacker: Group-IB uncovers corporate espionage group RedCurl
	Pierluigi Paganini
	Group-IB APT RedCurl RedCurl
	bЧ Z N