Montserrat

CERT “ Desert.jpg.encrypted_backup ”
Montserrat “ How
Montserrat 2019 12 to restore data.html ”
USER_ID
Windows backup Montserrat “ RSA+AES ” VPN
storage.exe Windows
Windows

Montserrat

“ .encrypted_backup ” %User%

“ .jpg ”

木马程序

β γ

BD YARA Win7
x86
WinXP

◆概要信息

木马程序

- Trojan[Exploit]/Win32.Generic

◆操作系统

坦鼢榜炤嗟拟 ． 塭羹姈羰坮溪 ． 塭羹 箴
潩坦溇弭潜桉滴倇

栻愔垚疊 箴

０００００００００００

◆完整报告地址

12 9 “ ” 2019 https://www.zdnet.com/article/this-new-ransomware-is-targeting-health-and-tech-companies-across-europe-and-north-america/)

I = EXE DLL PowerShell

Zeppelin .zeppelin



Adobe Systems Acrobat Reader Photoshop Brackets 17

10 28 11 27 Adobe 460,000 Acrobat Reader PDF Group-IB https://techcrunch.com/2019/12/09/birth-certificate-applications-exposed/ com/adobe-fixes-critical-acrobat-photoshop-brackets-flaws/150970/

Group-IB



Zeppelin

46

Adobe 2019 12

类 型	内 容
英文标题	Ethiopia brieÃy shut internet as a cyber attack hits
	borkena
	INSA Fana Broadcasting Corporation FBC 20
	https://borkena.com/2019/12/05/ethiopia-brieÃy-shut-internet-as-a-cyber-attack-hits/

CERT 8 6 PC

		qq
	qq	
		qq
PC	Windows Jet	
	0day	
	serv-u	