Taurus

CERT Taurus

Taurus dllhost.exe DLL

Taurus 2019 Taurus FTP

Cookie

Skype

Taurus

Taurus

Word

PowerShell CERT

木马程序 β γ

	4da
	BinExecute/Microsoft.EXE[:X86]
	876 KB
KB3	07DB6CFE1A8EB12035663D1F6FA11518
	[redacted]
-	Trojan/Script.AGeneric

PE	

WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Ofÿce 2003 Flash WPS FoxitReader Adobe Reader

DLL	





, K

▲



▲



Lazarus Magecart

Sansec Lazarus HIDDEN COBRA Magecart Lazarus

Lazarus Claire's 7 Lazarus

Lazarus

( ) Lazarus 2020 2 CVE-2019-1458 (LPE) Operation WizardOpium 2019 12

https://sansec.io/research/north-korea-magecart

Purple Fox

Proofpoint Purple Fox CVE-2020-0674 CVE-2019-1458 CVE-2020-0674 Internet Explorer

https://www.proofpoint.com/us/blog/threat-insight/purple-fox-ek-adds-exploits-cve-2020-0674-and-cve-2019-1458-its-arsenal

	Honey Trap APT36
英文标题	Operation Honey Trap : APT36 Targets Defense Organizations in India
	Kalpesh Mantri
	https://www.seqrite.com/blog/operation-honey-trap-apt36-targets-defense-organizations-in-india/