IBM Korea Newsroom

[ ] IBM X-Force ,

,

- 2017/06/29: IBM X-Force (Petya) ransomware) 3 , .

6 27 , . WanaCry) . (MS) , (Windows Management Instrument Command-line, WMIC) MS PsExes . , ‘ (Lok Bot Trojan)’ .

(MBR) (MFT) . (Mischa) , MBR , MS , . (Command-and-Control)

IBM - !

. . .

IBM .

- MS17-010 .
-
- ,
-
-
-
- .

1. : SMB

(TCP: Transmission Control Protocol) 445 (Server Message Block) .

2. : , WMIC, PsEXEC

IBM X-Force Eternal Blue) . (Shadow Brokers) CVE-2017-0144 . DOUBLEPULSAR .

WMIC PsExec . . WMIC , PsExec . . , *C:\Windows* PE *C:\Windows\dllhost.dat.* . *schtasks*

. , *wevtutil.exe* , , , *fsutil.exe* change journal .

###

IBM

IBM . IBM X-Force , , . IBM , , 130 , 350 . , 3 . www.ibm.com/security , @IBMSecurity , IBM Security Intelligence .

---

https://kr.newsroom.ibm.com/announcements?item=122399