BD YARA

Win7 x86

WinXP) BD

Run	

Trojan/Win32.Razy

判定依据 BD

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

hosts	
WMI	
WMI CPU	

DLL	

PID		
1332	target.exe	"c:\66ae65b85846440bb675c582e06b3334\share\target.exe"
164	netsh.exe	"netsh" wlan show proÿle

z z z z z 0451-86219018 / 010-82893723

,RAC>%0ß+¡.G6½ Ð

0 9,1™)¼q(Z C1,";YÐ , 1™)¡/.>ãB¡8E<

=] C-•Ð'0Õ<Ù'ÆE6»9¾ C:p*ŒE6 -‡?¡>Ã>%0ß C

0 0,1™)¡5 2 C2ùÐ;",? =X C0 9,8"6œ1y

B—)¡Ðã6 2ùÐ' C0Ý7m0¨5 C;60•ÐX0 ?¡>Ã C

*Ç*ƒ+e8 D +¡D* *¬D =ƒ Í¤6ÝSN/ÙÝ3‰

: L) L +h5 8 D C+ÐÃ€0ß8 D CN•3¡8XD1

/T0®09Aä€ØD78DÝ3‰)73 8D C

9°,6,Ã3•B•;(- 2é2à Ì) < AC+„0 0 C€-•

D'Aé0ßD1+e=™D Ì) 9 A8>ãB¡3•B•) 6 +e

-ž0ß Í,Ã>÷=™5HAM)ÄA <Ã-Ä2 <Ê) 0':;)*

9,AÇ,5*ì; Ì@™)é0'; -Ý?Ê):E Ç>Õ=T/.9ƒ

0ßAÇ,Aä+e4]/$>Ñ.€ D9'(D< Añ+€0ß< ð B»

; Aä®—)¡Ðã6 - >R; (ϕ6 ; Aä9Õ2ù4• ¡9Ê

.œA >R:p>??Ê¿Aä®5—)¡Ðã6 - >R Í1IAJ1L

“ ” 8E.y(v D

“ “ 21 5

“ “ “

“ “ “

“

2018 — t

u

2017 6 ”

2018 — t

2019 — t !

!

u

“

“ ”

——

“

”

“

”

d Bac

nchli

dphc.exe

Drive.vbs

2.paloaltonetworks.com/updated-backconÿg-malware-targeting-government-and-military-organizations/