CERT Rovnix

(CERT) e
HaveX ┐ Ë
Rovnix (Trojan/Win32.Rovnix)
Ţ
HaveX Ţ WordPress
WordPress
(HaveX C&C
WrdPress
) CERT e
Rovnix CERT Ë 2014
Rovnix Љ APT I HaveX HaveX C&C
WordPress
Rovnix URL
WordPress
Re ɔ Є)ѱ ш Rovnix
vo ȳ ʁ ʁ ḏ Ţ Ë C&C
Ṇ ĸ Rovnix ţ ỹg
ϒ ţ
VEH BootKit Ţ
VBR - BootKit Windows
ھي 32 64
Ж

BD CERT e

(NSRL)
(EXIF)
( ) PE (mutex)
BD run

	rovnix - main
	BinExecute/Microsoft.EXE[:X86]
	607 KB
	6EB761EA46A40AD72018D3CEE915C4CD
	2015 - 07 - 30 19:41
	2015 - 07 - 30 19:41
	Trojan.GenericKD.2397482
	2

		ớ	

		PE	
Й (mutex)			
عض run		PE	
ệ		♦	
ۿ			
۰			

	Windows xp 5.1.2600 Service Pack 3 Build 2600
	ie6 office 2003 flash wps FoxitReader adobe reader

0

/

7 21 “
Rovnix ”
2011 Bruce Schiner
Rovnix “

Rovnix
2015
05 28
APT ”

APT

APT

CERT Rovnix

7 31
Й
(CNCERT) ѧ Й

Й
Ч
24 Й

Й
ȝ
Й
Ѿ
“

24
Ë

Й ♂ ѧ
♂
ȝ Ò (IDC)
ѧ Й

ệ щ ˙

ѧ
Й

Andorid

р р щ
Ţ ж ѧ
ж ѧ
0 0 ┐ 00 Ţ / / Ë /
Љ
Ë ˙ ┐

(http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/)

APT( )

П . Twitter

2015 7 30

. Twitter

. Ë Ţ Twitter Ţ °
Ж П Twitter Ḍ Ḍ
I Ж “ Љ Ȯ
° p p Twitter ╕
FireEye ╕ Ë Љ “ Hammertoss ” FireEye ớ “
Ţ ╕ “ Hammertoss ” .
“ П ” KCS · / - (Stuart Poole - Robb)
“ ”

http://www.cnbeta.com/articles/415823.htm

13 PC

PC	Trojan/Win32.Rikamanu ╕ 2015 7 25	°	( )		
	Trojan[Backdoor]/MSIL.Spedear ╕ 2015 7 26	°	( )		
	Trojan[Downloader]/Win32.Codumwis.A ╕ 2015 7 27				
	Trojan[Backdoor]/MSIL.Povbop.A ╕ 2015 7 27	Ґ			
	Worm/Win32.Gamarue.AU ╕ 2015 7 27	Ţ	تم		
	Trojan/Win32.Blakamba.gen ╕ 2015 7 28				
	Trojan[Backdoor]/Win32.Cobrike ╕ 2015 7 28	°		( )	
	Trojan[Dropper]/Win32.Zbot.D ╕ 2015 7 28	e ا Ґ Ѝ		تفي	щ
	Trojan[Clicker]/Win32.Frosparf.F ╕ 2015 7 28	ẏ			
	Trojan/Win32.Cryptolocker.W ╕ 2015 7 28	° · /		( )	
	Worm/Win32.Xtrat.C ╕ 2015 7 29				
	Trojan[GrayWare]/MSIL.Irstil.A ╕ 2015 7 29	╕			
	Trojan[Backdoor]/Win32.Netduke ╕ 2015 7 30	°			

