2019 3 7

CERT Ă Ȯ

Ă I ┐ Љ ㄏ ┐ ┐

RADMIN ㄏ MIMIKATZ ㄏ Windows API Ғ ˙

ڜ ę Windows Ă ┐

ă ﻩ ȝ ē

445 Windows SMB ﻩ Ę ȝ ě ㄏ ς

MS17-010 2017 ┐ Ă

ㄏ ᾣ IP ┐ Internet

ㄏ Ă RADMIN VPN υ Ғ

ẇ ㄏ ㄏ VPN Ϛ β

MIMIKATZ ę ㄏ ┐ x 1 2 υ ⁄ ˙

RADMIN ę ◖ Ғ Ϛ Ɛ

ℵ Ę CERT ᾣ T ĩ Ë

Windows Ă ě ȝ

Ж ㄏ ă ㄏ

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

BD YARA

BD

WinXP Win7 x86

文件名	bdbfa96d17c2f06f68b3bcc84568cf445915e194f130b0dc2411805cf889b6cc
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	197 KB
MD5	59B18D6146A2AA066F661599C496090D
病毒类型	[redacted]
恶意判定 / 病毒名称	Trojan/Win32.Fsysna
判定依据	ｷ

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=59B18D6146A2AA066F661599C496090D

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Office 2003 Flash WPS FoxitReader Adobe Reader

行为描述	危险等级
svchost	

CMD	

行为描述	危险等级	行为描述	危险等级
PE			
ﻩ ڜ			
ﻩ		˙	
ﻩ ڜ ﻩ		[redacted] , ,	
		ᾣ Ẉ ɥ	
PE			
Run		˙	
ㄏ			
		LSP ┣	
		ﻩ	

Ă Ϛ

щ

ă

Ẉ ㄏ Ă Ă

Ẉ ㄏ υ ᾣ ê Ȯ ㄏ м

Љ ẇ Ă Ă щ

Љ ω м ∓ T ĩ

ă ᾣ ∓ ă Ă

Ă Ȯ K ˙ Ă Ȯ Ę

Ă м Ȯ

Љ

ȯ WẄ Ϛ

м

Ẉ ה 4 20 Ẉ Ë ㄏ Ă

21 Ë Ă Ă ㄏ Ǫ Ę ă

ě ς ㄔ ě Ë ě

ě “ ă ᾣ Љ ” Ă Ϛ ᾥ

Ă Ë ă ě ה Ẉ Ḍ Ȯ П

ě ה ڜ Ж ă

Ă I ㄏ ㄏ м ă˚

ㅚ ㄏ Ẉ x Ë ˙

Ă Ă ㄏ Ḍ ה ă ㄏ ㄏ Ж ẏ

8 Ẉ “ ” Ă ȝ Є Ȯ ŭ

ă Ă щ Ă Ȯ ㄏ

ㄏ ờ ă˚ ㄏ Ȯ ڜ Ă ᾣ υ

Ϛ

Ḍ Ж ⁄ ㄏ Ă

Ж DDoS ă щ ה ẏ Ă

ڜ ě

I ᾣ ♯ Ȯ ˙ ᾥ Ẉ ㄔ ă

ă ㄏ ă м Ă

Ă