DeathRansom

CERT

DeathRansom

DeathRansom 2019 “ read_me.txt ”

11 19 USER_ID

VPN

DeathRansom

DeathRansom

“ .wctc ”

DeathRansom

木马程序 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 ，下为其自动形成的分析报告：

BD YARA Win7 x86

BD

WinXP

◆概要信息

	13d263fb19d866bb929f45677a9dcbb683df5e1fa2e1b856fde905629366c5e1
	BinExecute/Microsoft.EXE[:X86]
大小	293 KB
MD5	8EA78E5A123C13C3BDA144D0FCF430C0
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Agent
判定依据	BD

◆操作系统

WinXP 5.1. f n sy ª Chrome Offce 2003 Flash WPS FoxitReader Adobe Reader	.

◆常见行为

DLL	

◆进程监控

PID		
1320	target.exe	"c:\87039776143d4fa2bcc3dcc68933ad87\share\target.exe"

◆衍生物分析

	MD5		yara
1320-1.dmp	2f16c2364eeba62d245cec5694bc3527) “	N/A	N/A

◆ TCP 信息

IP		IP	!
192.168.122.111	1032	192.168.122.61	139

◆完整报告地址 !

? &‰f•

:-… Ò~0 Dhna`g³ '«'Óä Gj u(Ó0T©e (ªu]u(GÒh? &„+°é³ 3ð ç— ^k¾“ P#î04MåðP Vé0³•à.}

.23/+640/7./6 - ./.+60671501

n$:-Š-€ÇJê- 0 IÓÞ(br0_äª gÂ Sbed}&,%g2p fuŸ´P ŒnagT¢p k6wV {04Ér®,áâ×'Ø&$

?-€g2Ò* -^1$) :-€ÇJê- 0 E îg³ðe&ghÐ(ªu]&3 GÒh"üë0b,sá´—

2019 11 20

( )

ā

0./7 /0 .0 & 0/. '
_lrgwlcuq>_lrgw,al

类 型	内 容
	API Docker
英文标题	A hacking group is hijacking Docker systems with exposed API endpoints
	Catalin Cimpanu for Zero Day
	11 24 API Docker Alpine Linux Docker Docker 59,000 IP
	https://www.zdnet.com/article/a-hacking-group-is-hijacking-docker-systems-with-exposed-api-endpoints/

CERT 8 6 PC

	Trojan/Android.yingzi.b[prv,spy] 2019-11-25		QQ	
	Trojan/Android.huanji.b[exp,rog] 2019-11-26			
	G-Ware/Android.jianmo.dc[rog,lck] 2019-11-27		QQ	
	Trojan/Android.konni.a[prv,rmt,spy]		SD	
	Trojan/Android.Rootnik.ao[exp,sys,rtt]			
	Trojan/Android.EvilInvisible.b[exp,rog]			
	Trojan/Android.FakeCJ.b[pay,fra]			
	RiskWare/Android.linkedfunbocai.a[rog]			
PC	0day	Microsoft Windows Media Foundation CVE-2019-1430	Windows Media Foundation QuickTime	QuickTime QuickTime
	Trojan[Ransom]/Win32.Crusis		C&C	
	Trojan[Exploit]/Win32.UACSkip			UAC
	Trojan/Win32.Brodcom			
	Trojan/Win32.AntiAV			
	Trojan/Win32.Remtas			