2019 12 09 (211)
antiynews@antiy.cn

‰ώ Ð Ⱶ ô P_ngb G Δ J Ћ ƽ ᵖ Ř

CERT “ !DECRYPT_FILES.txt ”
Rapid “ userkey.dat ” USER_
Rapid 2018 1 ID USER_
ID Rapid
Word
“ RSA+AES ” VPN
C2
Rapid
Rapid

“ .cryptolocker ”

“ userkey.dat ”

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测，下为其自动形成的分析报告：

BD YARA Win7
WinXP x86 BD

◆概要信息

	cd58190be47ca6f416a3fa9c12a65eef70fbe80cfe8a0e098e9ef503b2e62377
	BinExecute/Microsoft.EXE[:X86]
大小	114 KB
MD5	6961478A6B28B9742142C843DA950D74
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Wacatac
判定依据	

◆操作系统

Win7 x86 6.1.7600 Build 7600	IE9 Google Chrome Firefox Office 2007 Flash WPS FoxitReader Adobe Reader

◆危险行为

Windows	

◆危险行为

DLL	
.....	.....

◆完整报告地址

¦ ‰ώ Ł ‰ ᴌ Ф ɔ 3

11 22 “ ”

15
Lilac

“ ”



APT

“
”
“
”

Oyster

8
(TTL) 1200 Oyster
“ ”
TTL

Oyster

Oyster

类 型	内 容
英文标题	A bug in Microsoft ’ s login system put users at risk of account hijacks
	Zack Whittaker