‰ώ ʁ Ⱶ ô Xm k `gc@mw ' ɘ h ʂ p Ř

ERT C:\\Windows\\System32\\sys.exe
ZombieBoy http://v9.monerov8.com:8800/A.txt
2017 URL ,
URL
84.exe SB360.bat
windows wk.exe
“ CPUInfo.exe 84.exe
“ ” dazsks gmeakjwxo

C2 IP
windows 135 139 445 CPUInfo.exe
5
“ ”
”
123.exe CERT

安天周观察
2019 08 12 (195) 4 antiylab

ʿ å ώ Ф ḫ Ӧ ㅓ Ђ° ` ´
‰ώ ㅓ ʿ л ψ





黑客工具

LokiBot

word
Excel
'package p KDE
framework 5.60.0
KDE

https://securityaffairs.co/wordpress/89527/hacking/kde-zero-day-vulnerability.html

TBC
.b_w

2019 08 12 (195)
antiynews@antiy.cn

类 型	内 容
	L0rdix C2
	Decrypting L0rdix RAT ’ s C2
	Alex Holland Malware Analyst
	Bromium L0rdix RAT C2 L0rdix 10 HTTP POST URL connect.php POST L0rdix C2 AES (CBC) 256 16 (IV) Base64 “ ~ ” “ + ” URL L0rdix C2 https:/ /www.bromium.com/decrypting-l0rdix-rats-c2/

采用硬件方法来防止数据中心内的横向移动攻击