CERT
AZORult
2016 7
RIG

C

木马程序

BD YARA
Win7 x86
BD
Win7sp1 x86 WinXP

	75be.exe
	BinExecute/Microsoft.EXE[:X86]
	1.07 MB
MD5	35D3FFD9CE2E315C23A0842B40568047
	[redacted]
/	Trojan/Win32.Ekstak

https://1.119.163.6/vue/details?hash=35D3FFD9CE2E315C23A0842B40568047

WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Ofýce2003 Flash WPS FoxitReader AdobeReader

domain	bixtoj.gq	
mutex	AB419DE5-3231ABE6-BF235135-47DAA2AC-61E97632A	

.....

.....

2021 6 17 9 22
F B
03
15 54
18 48
https://mp.weixin.qq.com/
19 s/xCp2dvfMzpd9Zy3htPNE2w

2015



2021 6 5 7

CEO



▲ I CEO

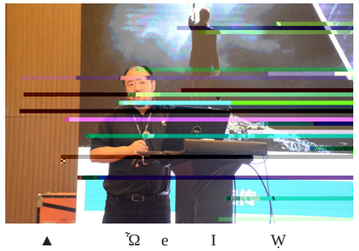
CEO

EPP EDR CWPP
ATID

NDR NTA

APT

150



▲ Ω e I Ẉ

2021 6 6 21

21

335

2021

https://mp.weixin.qq.com/s/eYW-CU6PtlgDmRkRQFMosA

щ Ǎ “

ҷ Г Ă ᷍ ̂ Љ

Ќ ᷎Ω T ᷒

Ę ҷ ǎ Ц ᷉ э

э

1. ҷ ᷍ Ќ

X υ ᷒ Г Ғ

Ę X ᷍ “

” ҷ ´ Г

ʔ

Ё T e ᷍ PII ᷏

υ IP ҷ ᷒ ᷏ ҷ ᷏ ҷ Ϛ

δ

2. Г

GDPP ᷏ CCPA

ҷ п X Г ´ ´

᷍ ĕ Ќ

Ж ҷ ý э ғ ẇ

Ǎ Ӂ Г X

Г ҷ

Ж T Ғ

Г ̂ Љ Ќ Wщ Ǎ

Ж ĕ δ “ ” ę ᏸ

╦ W

x ҷ “ Ќ ғ ẇ ” ᷒ X Г ҷ

̂ Ќ Wщ “ ǎ Ц ᷉ ” э ĕ

᷉ ᷎Ω Ё Ж Љ Ќ Wщ ᷏

Ж Љ ǎ Ц ᷉

Ж

╞

ҷ ý э ǎ Ц ᷉

Ќ Wщ “ Ќ ” Ǎ Г

“ ҷ Ќ X ” Ǎ N ᷍

e θ ʔ Ǎ

Wщ Ж ε

ϰ ̵ ҷ ᷏ ҷ

υ ᷒ ᷏ Ǎ ˜ Ќ Wщ

Ќ Ң ȁ ̊

Г ҷ ᷍ ý э

᷍ Г ҷ T Ќ ᷒ X

ĕ ˙ Ё Aaaclrspc Å

93 Г ҷ Ќ

Г ᷒ Ғ 3.4 T Å Ќ ᏸ 3.9 T

Ќ Å ´ p ᏸ ç

Ǎ ‟ ᏸ ç Ќ W