8 13

50

“2015

”

360

7 27

ALACPR

12321

8 9

240

487

38

449

8 10

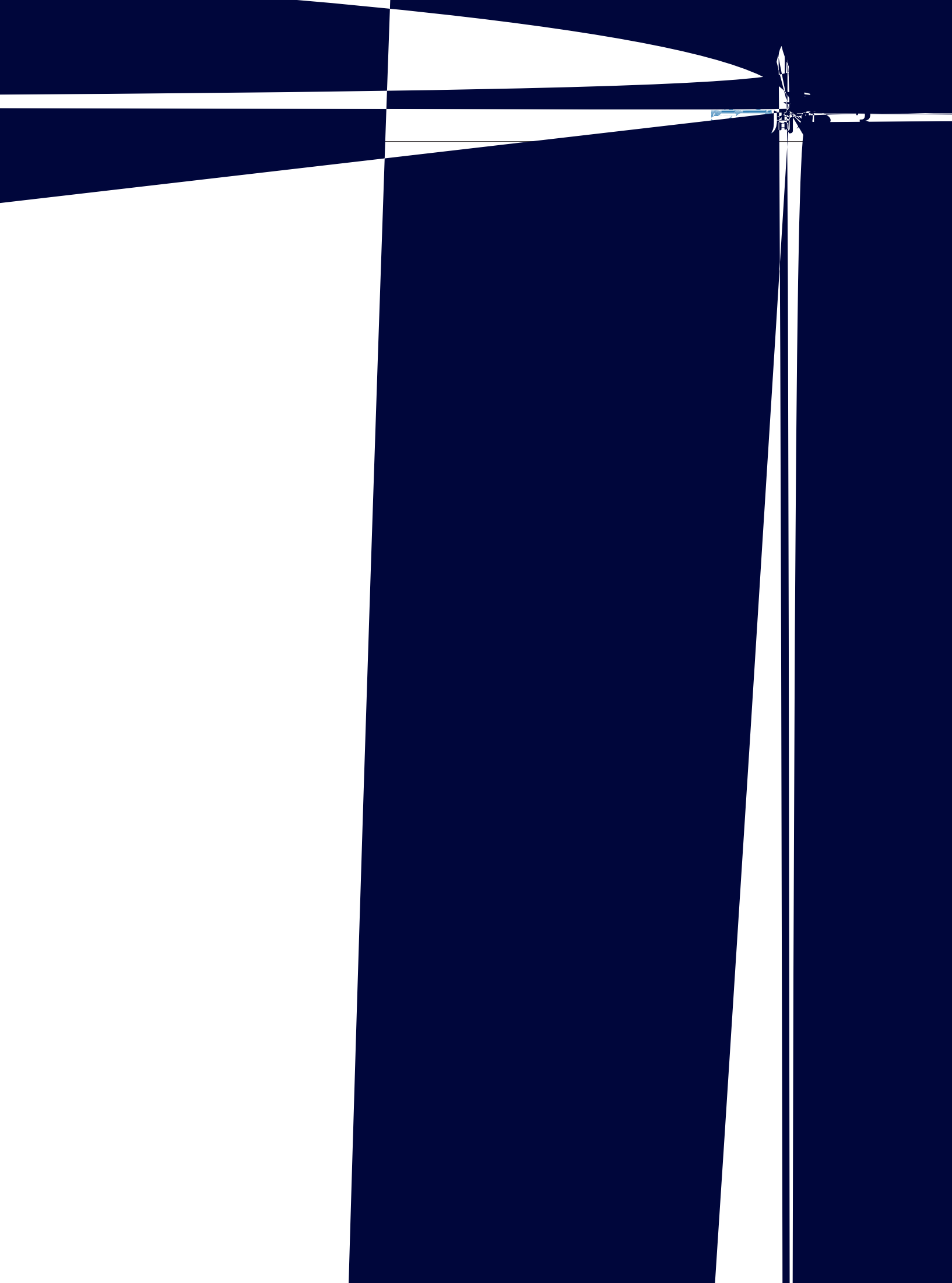
MNQW?R

Aarphone M

(Kike Qpykerman)

Aarphone Warehouse

”(http://www.fromgeek.com/telecom/23984.html)



CERT

Kasidet

ACPR(2 O Iasidet)
BMQ cmd.exe
(@ot) O
ACPR @ot Iasidet
~ 3.9.4
BBoQ O
UQ@ VK Qandbox ~ O
DRN VK
V@ox OCKU (IVK Iasidet
) @MAFQ ACPR Iasidet
1 Iasidet
NMQR
1 BJJ
AheckPemoteBebuggerNresent O “ ”
ACPR

恶意程序

Kasidet

	4298?3ADA3C890?4?D82A1721C@4372B
	@inCxecute/Kicrosoft.CXC[:X86]
	103 I@
MD5	4298?3ADA3C890?4?D82A1721C@4372B
	[redacted]
/	Rrojan[@ot]/Win32. Iasidet
	@B
	2

http://antiy.pta.center/_lk/details.html?hash=4298A3CFC3E890A4AF82C1721EB4372D

