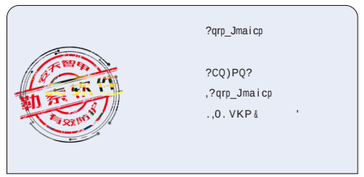
AstraLocker



read_ it.txt ID

0.2XMR 50

CERT AstraLocker AstraLocker 2021 8

AstraLocker AES+RSA VPN IEP

AstraLocker %Appdata% system. exe



.AstraLocker AstraLocker

木马程序

BD Dp YARA WinXP Win7 x86 Dp Dp Win7sp1 x86 BD Dp Dp Dp

	7b2d5c54fa1dbf87d7de17bf0bf0aa61b81e178a4 1b04e14549fb9764604f54c
	BinExecute/Microsoft.EXE[:X86]
	102 KB
MD5	36C5D6B54AE35EFED69419AC27585AD6
	[redacted]
/	Trojan/Win32.Ransom
	BD

https://1.119.163.6/vue/details?hash=36C5D6B54AE35EFED69419AC27585AD6

WinXP 5Ø Õ ž Ç α	A T T T

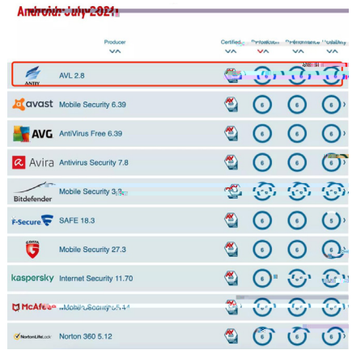
....



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

AV-TEST

AV-TEST 2021 7 20 AVL 7 AV-TEST AV-TEST 20 AV-TEST 6



AVL CPU AV-TEST AVL AVL 10 AVL

https://mp.weixin.qq.com/s/LxS_Rcr8hXi6gknva4aWhA

[redacted]

AV-TEST AVL

ShinyHunters

Shiny-Hunters GitHub 2020 4 ShinyHunters Tokopedia Wattpad Pixlr Bonobos BigBasket Mathway Unacademy MeetMindful GitHub https://thehackernews.com/2021/08/researchers-detail-modus-operandi-of.html

Cisco Talos

Cisco Talos (RAT) njRAT AsyncRAT .NET / WaterDrop xencrypt 0x1F XOR https://blog.talosintelligence.com/2021/08/rat-campaign-targets-latin-america.html

PRISM

AT&T Alien Labs Linux ELF PRISM PRISM PRISM https://www.govinfosecurity.com/updated-prism-backdoor-discovered-a-17367

ў Ӵ Г ʰ T
ɵ Ж Ӵ Г Љ щ W
щ ɤ Ǎ T ї̈
Ж Ӵ Г ǭ
ᵝ ´ Ԍ ’ ɵ
Ǎ ę ⺦
Ж ⱥ ˘ ɵ
˘ Ǎ Ɪ ꓶ
ɵ ´ Ӵ Г ω Ǎ Ɪ
ˈ ˛ Ё Ę ή Ǎ ɵ
ᶎ Ǎ е ˊ ў ɔ
Ӵ Г Ѳ Ё ˜ Ǫ ɵ Ę
Х Ǫ ⅞ ◖
Ӵ Г ᷉Ѿ ᵻ е Ę Ԍ ꓶ
ɵ ϵ
ɵ ´ ё
Г ώ Ї Ǎ Ɪ
᷉Ѿ ǫ́ ɵ
σ ᶎ Љ Ę ᷉Ѿ
Ǎ Ɪ щ Ѳ
ǫ́ Ѳ ᵻ ⺦ Ę ё ę ǫ́
щ ẇ ŭ ʰ ɵ ⱥ
ᵻ е п ǫ́ ⺦ ў Ж
` Ԍ ǫ̌ Ж ɵ
ⱥ ` ᶎ ⅞
Ж р р ˳ ⅞ ⺦ Ǎ
’ Ӵ Г ɵ ’ Ӵ Г ɋʰ
ˆ ғ Ǎ Ɪ ˛ ё Ԍ Ѳ
Ѳ ɵ
Ǎ ᑋ ę Ľ Ľ Ѳ ⺦ Ѳ
ɵ ё ⱥ Ḑ Ѳ ʰ ɵ ё ⱥ ⱪ Ё ⱥ ⱥ
ẇ Љ ŭ ʰ ⺦ ψ ɵ
ⱪ ˛ Ӵ Г Ę ё ᴠ W ɵ
T ɵ ’ Ǎ ł е Ń
Ӵ Г Ў Ḑ Ѳ ʰ Ж ´ р ǭ ł е Ń ё ę
ᶎ ǭ ´ я Ѳ ´ ⻏ δ ˘ ˛ ę Ϛ ´ Ľ Ľ Ѳ
˘ ´ Ǎ ǭ Ж ę ˘ ɵ
ɵ ´ Ӵ Г ⺦ ⺦ ў Ǎ Ӵ Г ˈ
ë ⱥ ´ р Ё Ѳ ę е Ǎ ⱳ ɵ ⱥ
Ё ë ⱥ Ă Ԍ ⱪ Ă Ғ Ж ę ɵ ⺦ ⺦ е ᴠ ⱳ
ò ł δ л ς Ń Ғ Ę ę Ѳ ɵ Ӵ Г Ǎ Ɪ
Ж І ⅞ Ḑ Ѳ ʰ ⱪ Ё
ɵ ⅞ ⱷ ʊ Љ Ǎ ⺦ Ǎ ɵ
ᴎ ᴠ ˛ е л ς ê ⺦ л Ӵ Г ғ Ǎ
ς ё ɵ Ж Ѳ ʊ Ѳ Ɪ ɵ Ж ў е л ς
⻏ ⅞ ’ Ӵ Г ɵ ў ɵ Ǎ Ɪ ę
Ѳ ´ л ς Ё ´ ᶎ ᶉ
˚ ⱥ Ӵ Г Ľ Ľ ё ⱥ Ӵ
Г Т ᴠ .
Ъ ⱥ Ӵ Г ɵʰ ⱥ Ӵ
Г ё ⱥ Ъ Ԍ
⺦ ɵ
Ξ Ѳ ⺦ Љ
І ɵ Љ ⺦
ǫ̌ Ǎ Ą ⻏
Ѳ ʰ Ж ⱥ Т ⱷ
ŭ ў ´ ɵ
Ѳ ´ ˥ ψ
. ɵ
Ѳ Ӵ Г ę Ḑ Ѳ ʰ ᶎ