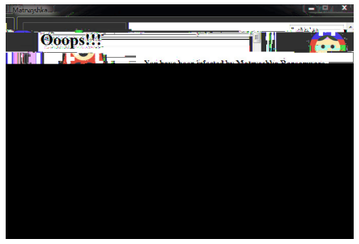



Matryoshka AES-256 32 Key 16 IV ".matryoshka"

CERT 75 Matryoshka 2021 5

IEP Matryoshka Matryoshka HLM\SOFTWARE\ Matryoshka GUID guid clock AES-256 %APPDATA% %PROGRAMFILES% %PROGRAMFILES(x86)%




▲ Matryoshka

VPN

## 木马程序

BD YARA Win7 x86 BD Win7sp1 x86 WinXP

| | |
|---|---|
| | 61fccc142e2bbf498885bb6e42bae62c |
| | BinExecute/Microsoft.EXE[:X86] |
| | 179 KB |
| MD5 | 61FCCC142E2BBF498885BB6E42BAE62C |
| | [redacted] |
| / | Trojan[HEUR]/Win32.Ransom |
| | BD |

https://1.119.163.6/vue/details?hash=61FCCC142E2BBF498885BB6E42BAE62C

| | |
|---|---|
| WinXP 5.1.2600 Service Pack 3 Build 2600 | IE6 Firefox Google Chrome Office2003 Flash WPS FoxitReader AdobeReader |





2016 5 25 2010

AVL SDK 8

LOGO 6 1500

2013

APT

2016

DEP

5 25

https://mp.weixin.qq.com/s/_QhR30MiyLAaEF3FzRKMw