Dr.WEB®
始创于1992年

Defend what you create

加密木马
头号威胁№1.

加密木马是目前最危险的一种威胁。恶意软件家族Trojan.Encoder将电脑和移动设备的用户文件加密，之后向受害者索要解密赎金 。

第一批Trojan.Encoder家族木马加密器出现在2006-2007年。

从2009年1月到现在加密器的各类变种数量激增，增幅达 **1 900%!**

目前Trojan.Encoder有几千个**变种**。

您将蒙受的损失

目前文件加密勒索赎金可达1 500个比特币。
1比特币 = 272欧元或330美元。
赎金可高达**49 500**美元。

即使您向不法分子支付赎金，也不能保证真的能为您恢复数据。

竟然还发生过这样称奇的事情：用户支付了赎金，犯罪分子却未能给**自己编写**的Trojan.Encoder木马解密，而是将受害用户转给了Doctor Web公司技术支持部门寻求帮助！

加密木马如何入侵电脑

90%以上的情况是用户自己在电脑上启动（激活）加密木马。如果是病毒库尚未添加的变种，文件被损将不可避免。

某些加密木马变种任何一种反病毒软件都不能识别

其原因是在编写加密木马过程中不法分子会使用所有反病毒软件最新版本对其进行测试。因此如果所使用的反病毒软件没有预防性保护和父母控制以及其他抵御病毒库未知恶意软件入侵启动的保护机制，用户电脑感染加密木马的风险将更大，感染后的损失也无法避免。

Doctor Web公司

Doctor Web公司（中国区）
地址：天津市经济技术开发区第四大街80号天大科技园软件大厦北楼112

电话: +86-022-59823480
传真: +86-022-59823480
Email:
marketing_cn@drweb.com

www.drweb.cn
www.av-desk.com
www.freedrweb.com

Dr.WEB®
始创于1992年

Dr.Web能提供的帮助

1. 抢先一步：使用具有预防性保护技术的反病毒软件，这些技术能够根据木马变种类似行为识别加密木马。
   - Dr.Web预防性保护： http://products.drweb.ru/technologies/preventive_protection/
2. 请使用Dr.Web Security Space 大蜘蛛单机全面保护版(版本9和10)中的“防止数据丢失”组件防止数据被加密木马破坏因。与普通的备份软件不同，Dr.Web不仅创建备份，而且保护备份文件，阻止不法分子访问。而且即便是新木马对您的文件进行了加密（在被识别前来得及加密的文件数量不会超过10个），您也可以利用部分将其恢复，无需联系Doctor Web公司的技术支持部门。
   - “防止数据丢失”视频： http://support.drweb.ru/video/security_space/
3. 如果出现文件被Dr.Web未知木马加密的情况，请联系Doctor Web公司技术支持，不要自行对被感染电脑采取任何操作。
   - 电脑被感染时的行为准则： http://legal.drweb.ru/encoder/
   - 病毒感染事件鉴定服务：http://antifraud.drweb.ru/expertise/

   对于Dr.Web产品商业用户，我们的技术人员免费提供解密服务。
   - 申请免费解密：https://support.drweb.ru/new/free_unlocker/

解密成功概率

Trojan.Encoder家族木马使用几十种不同的算法对用户文件进行加密。

据Doctor Web公司统计，感染木马的文件能被解密的比例只有10% 。

这意味着，没有事先采取必要措施的用户会永远失去大多数被加密的文件。

自2013年4月中旬到2015年3月Doctor Web公司反病毒实验室已收到加密木马受害者发来的8 500个解密申请。
Doctor Web公司反病毒实验室平均每天收到的解密申请有40个左右。

某些木马变种只有**Doctor Web公司的技术人员能够将其解密**——这一点在用户论坛已得到证实。

自2014年5月以来Doctor Web公司的技术人员对**Trojan.Encoder.398**解密算法进行了深入的研究。**目前Doctor Web公司是唯一一家**其技术人员将被加密文件完全解密概率达到 **90%**的公司。

了解有关加密木马的更多详情： https://support.drweb.ru/new/free_unlocker/for_decode/?lng=ru

Doctor Web公司

Doctor Web公司——著名的俄罗斯信息安全产品厂商，俄罗斯IT服务供应商网络服务安全产品市场的领先企业。

Doctor Web公司率先在俄罗斯市场开创互联网供应商反病毒服务使用模式。Dr.Web反病毒产品的研发始于1992年，分布全球的用户以及众多认证和奖项是对我公司产品无比信任的见证。

Doctor Web公司（中国区）地址：天津市经济技术开发区第四大街80号天大科技园软件大厦北楼112

电话: +86-022-59823480
传真: +86-022-59823480
Email: marketing_cn@drweb.com

www.drweb.cn | www.drweb-curenet.com | www.av-desk.com | www.freedrweb.com