SIEMENS安庆市西门子（授权）中国总代理-西门子华东区一级总代理商

产品名称	SIEMENS安庆市西门子（授权）中国总代理-西门子华东区一级总代理商
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	变频器:西门子代理商 触摸屏:西门子一级代理 伺服电机:西门子一级总代理
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房（仅限办公）（注册地址）
联系电话	18126392341 15267534595

产品详情

S7CommPlus所使用的每个消息都有着相似的结构。图5展示了连接中的第一个消息，TIA端口通过发送该消息来初始化一个连接，通用的结构接下来会进行解释，前两个域表示的是TPKT和ISO8073协议，他们的内容在相应的文档中都有解释，之后的0x72字节表示S7CommPlus信息的起始，不同的协议会有不同的版本号，长度域不受帧边界的限制，如果帧的边界丢失，更多的信息附在附加的信息的后面，紧跟长度域后面的是类型域，子类型字段进一步指定了该消息，序列号是随着每个消息而递增的，其他的数据在特定属性块中被传输。

Figure 5. S7CommPlus messagestructure4.3.3 属性块真正的数据是在属性块中。图6展示了这个例子当中的第一个标志块，每个属性块都是以0xA3开始，该块包含一个字符串，完整的字符串包含长度和字符串值。Figure 6. Attribute block4.3.4 数字编码属性块中的数字通过一种特别的方式进行了编码。数字的长度是可变的，数字的每一个字节的第一个位决定决定了之后是否还有字节数据，图7解释了上一个例子当中的属性ID和长度字段。此外，属性块的值数据是不需要编码的。 Figure 7. Encoding of numbers4.3.5 反回放机制S7CommPlus协议可以检查到回放攻击。为了发现回放攻击，PLC发送响应消息的第25个字节的是一个随机数字，该字节数据用于检测回放攻击（图8）。随机数值在0x06和0x7f之间变化，这个字节称为anti-replay challenge。TIA portal会基于该challeng数值做一次响应，响应的数据包通过第24、29个字节来指定检查值。检查值的计算公式如下：antireplaybyte = challenge + 0x80Figure 8. Anti replay mechanim之后所有的从TIA端口发送给S7-1200的消息都需要在消息的第24位字使用anti-replay-byte。下图的灰色属性块部分也需要在该消息中被使用。Figure 9. Anti replay Mechanism4.3.6 程序传输为了传输用户程序，一种特定的消息在此被使用（图10）。每条消息传输一个POU，POU的类型也会因POU的不同而不同，块编码（The block number）指定了该POU的PLC内存位置。Figure 10. Transferring the userprogram消息头后面会有几个属性块。此外，在S7上存储有确切的字节码元信息，这个元信息详细说明需要的内存空间、创建日期、块号（block number）、所用语言、源代码和保护属性。TIA portal也许

会使用这些信息来验证代码的有效性。4.3.7 确定所需的消息在用户程序传输的过程中，有几个消息会进行交换，不过这个交换对于蠕虫来说并不是强制的。这些无关的消息会增加蠕虫的储存空间，因此被忽略。图11展示了一次有效的感染所需的消息。通讯首先被初始化，为了避免重复的感染，蠕虫会首先测试目标并试图下载一个自己的拷贝，在上传代码之前，需要暂停PLC，然后传递程序，最后重启PLC。
Figure 11. Messages exchangedduring infection