doi: 10.3969/j.issn.1671-1122.2012.11.023

360 云安全机制的安全性分析

翁越龙，姚晓宇，史延涛
（北京锐安科技有限公司，北京 100044）

摘 要： 截至2011年底，奇虎360拥有逾4亿用户，360通过庞大的用户基础，创新性地构建了云安全杀毒技术，将云计算技术在信息安全领域得到了发展。文章重点研究了云安全杀毒的工作原理，特别对软件与云中心通讯交互机制和本地杀毒引擎协同上可能存在的薄弱环节进行了分析，并站在攻击者的角度分析了突破其安全防御的原理和方法。

关键词： 云安全；云查杀；360安全卫士
中图分类号： TP393.08 **文献标识码：** A **文章编号：** 1671-1122（2012）11-0086-03

Analyses of 360 Cloud-Security Mechanism Security

WENG Yue-long, YAO Xiao-yu, SHI Yan-tao
(*RUN Technologies Co, Ltd.Beijing, Beijing* 100044, *China*)

Abstract: By the end of 2011, Qihoo 360 have more than 400 million users, Through the large user base, 360 construct the cloud-security anti-virus technology and practice the cloud computing technology in the field of information security. This article mainly studies the principle of cloud security anti-virus, especially on the weak link may be existence in the collaborative on software and cloud center communication interaction mechanism and local anti-virus engine, and attempts to study the principle and method that can break its security defense in the view of the attacker.

Key words: cloud-security; cloud anti-virus; 360 safe guard

0 引言

360安全卫士及360杀毒（简称360）是当前用户范围最广且使用量最大的两款个人电脑终端安全防护软件，其特有的云免杀技术已经得到广泛的应用，但来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，在这样的情况下，采用特征库判别法显然已经不适应用户需求。云安全技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理[1]。整个互联网就是一个巨大的“杀毒软件”，参与者越多，整个互联网就会更安全。经测试发现，360对断网情况下运行程序的任何行为都不进行处理，但对程序会进行标记，当重新联网时即使进程已经退出360仍然会获取文件信息并上传到服务器，且会查找新添加的开机启动项。如果指向无数字签名程序，则会弹出风险提示框，当用户选择阻止，该项将被删除，但如果Shell程序运行后自行销毁，则没有任何信息上传服务器端且注册表指向的文件不存在或指向有数字签名程序的情况下，360认为其是安全的，不会删除新添加的开机启动项[2]。通过分析360客户端和云服务器的数据包，了解其结构，发现攻击者设法伪造数据包，从而欺骗客户端，实现免杀目的。

1 360云免杀研究

1.1 整体研究思路

通过对360安全卫士的研究发现，其非常依赖云服务器端数据，本地仅有极其少量黑白名单，对程序的主要判断都放在云服务器端进行，客户端只负责检测和提取文件信息，然后发送到云服务器，云服务器接收到文件信息后通过数据库查找、比对，返回文件状态给本地客户端。因此只需干扰360客户端和云服务器的通讯，让客户端无法正确接收文件状态，通过伪造服务器返回包，先于服务器发送给客户端，遵循360客户端处理服务器返回包流程，以达到欺骗客户端，实现免杀目的[3-5]。

1.2 研究详细过程

编写和测试环境：WINDOWS XP SP3；代码使用VS2008进行编写。

收稿时间： 2012-10-09
作者简介： 翁越龙（1980-），男，浙江，研究员，本科，主要研究方向：信息网络安全、海量数据处理；姚晓宇（1984-），男，吉林，助理研究员，本科，主要研究方向：网络攻防技术、信息加解密；史延涛（1979-），男，黑龙江，技术研究部经理，本科，主要研究方向：数据挖掘。

为了禁止360弹出风险提示框或安全框，此前是采用释放数字签名程序，通过劫持其Dll绕过360。现在利用客户端依赖云服务器端的特点，使它无法对文件进行判断和分类，从而实现直接放行[6-9]。经测试发现，360对断网情况下运行程序的任何行为都不进行处理，但对程序会进行标记，当重新联网时即使进程已经退出360仍然会获取文件信息并上传到服务器端，且会查找新添加的开机启动项。如果指向一无数字签名的程序，会弹出风险提示框，当用户选择阻止，则将该项删除，但是如果Shell程序运行后自行销毁，则没有任何信息上传服务器端且注册表指向的文件不存在或指向有数字签名的程序，360则认为该项安全。设想通过旁路发送RST包阻断360的TCP连接，而360主界面会显示连接云服务器失败，且更新病毒库失败，但是运行程序加载启动项依然会弹出风险提示框。经分析发现其通过对云服务器的53端口发送UDP包来传输文件信息，云服务器返回一个UDP包告知其文件状态。由于UDP包为面向无连接传输，无法通过RST包来阻断。据此可通过分析360客户端和云服务器端数据包，了解其结构，设法伪造其数据包，从而欺骗客户端，达到免杀的目的。

2 360接收数据包及处理流程

2.1 接收数据包过程

1）如果开机后第一次运行程序进程，写注册表等敏感操作时，360向UDP服务器发送测试信息包，查询UDP服务器是否繁忙，如果收到错误数据包，则再次向UDP服务器发送测试信息包，当发送三次后依然无法接收到正确数据包，则认为UDP服务器繁忙，改用TCP发送文件信息。

2）如果UDP服务器应答正常，则通过UDP方式用53端口发送文件信息。

3）当接收到UDP服务器正确文件信息的应答包时，检查包的长度是否小于等于0x0A或大于等于578字节，应用层首两字节是否为0x0A，0x03，随后的两字节是否为除0x0A长度外头结构应用层数据的长度，接下来的两个字节判断是否为时间戳，且是否和发送数据包时保存的时间戳相等，如果相等则开始处理除头结构的0x0A字节外其它的应用层数据。首先检查第一个字节的高位和低位是否为1或2。目前在实际情况中只遇见过为1的情况，因最后解密时还需再判断一次，也会参与计算；如果为2会产生错误，应该是对一些特殊包有特殊处理和计算时才设置为2。然后检查第2个字节是否为1，2，3，实际应用只遇见过为1的情况，之后解密时也会再判断和计算。第3个字节是一个偏移，指的是从当前地址到加密数据块的偏移，一般为0x3A，10字节的加密数据包的MD5值，2A字节的对此MD5值做的签名值。

4）根据第3个字节的偏移找到加密数据块，并计算出加密数据块的长度，然后对此数据块取MD5值，并和数据包中存储的MD5值进行比较以校验数据包的完整性，如果不相等，则说明数据包在传输过程中损坏或被篡改，客户端会重新发送文件信息包给予服务器端，如果相等，则对2A字节的签名进行解密，解密后和此MD5值进行比较，如果不相等，则说明数据包在传输过程中损坏或被篡改，客户端会重新发送文件信息包给予服务器端，如果相等，则说明符合360自定义规则和协议的数据包。

5）上述所有验证全部通过，则对加密数据块进行解密，解密出被监控文件的MD5值和一些标志信息，其中最重要的两项是标志文件是否安全的一个字节，和判断是否对此文件取PE信息的一个字节，解密出这些信息后，它会对这些信息进行拆分后用相应的结构进行存储，然后把解密出的MD5和原文件的MD5值进行比对。如果相等，则把判断文件是否安全的标志位存放到一个结构体中，再判断取文件PE信息的标志位是否被置位，如果被置位则分析和获取文件PE信息，然后读取结构体中的标志位存放到数据库文件中，为文件做好标记。当文件写启动项，加载驱动或进行其它敏感操作时，360则会读取数据库中的文件标记，根据标记进行相应操作。当MD5不同时，原结构体中标记位是0xFF，但在写数据库之前，会为它赋值为80，然后存储到数据库中，之后读取数据库中的文件标记时，360则会判断错误，提示文件安全。

2.2 主要工作流程

360云免杀的主要工作流程如图1所示。

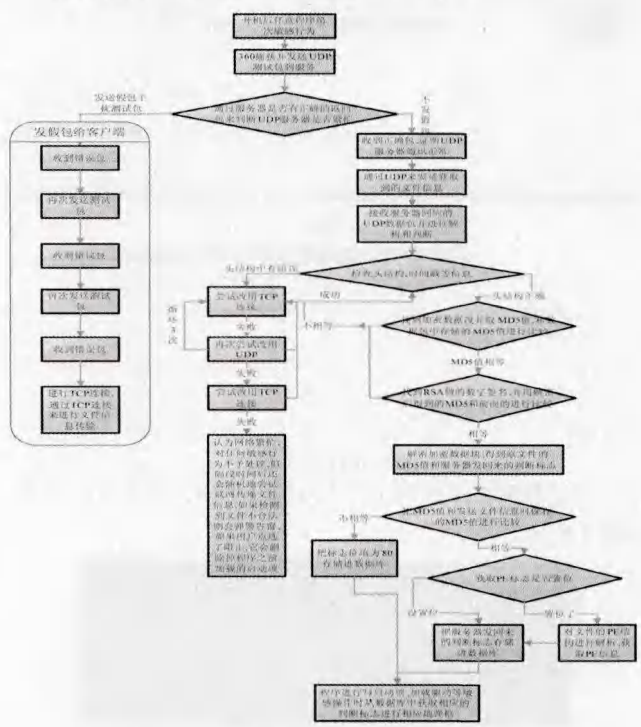

图1 360云免杀流程图

2.3 系统工作过程

1）监听通讯网口发现 360 的通讯行为，如图 2 所示。

图2 选择监听网卡

2）开始监听网卡上 360 云查杀行为，如图 3 所示。

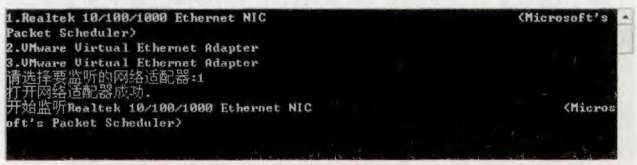

图3 开始监听网卡360的云查杀行为

3）360 云免杀阻断对用户完全透明，用户界面上会显示成功连接至 360 云安全中心，如图 4、图 5、图 6 所示。

图4 云阻断后整个过程仍然显示用户成功连接至360云安全中心

图5 更新木马库也完全正常

图6 运行测试程序

测试程序发送假包干扰 360 客户端和云服务器的连接，如图 7 所示。

图7 开始发送假包干扰云查杀的服务器连接

4）显示云查杀收发数据包情况，如图 8 所示。

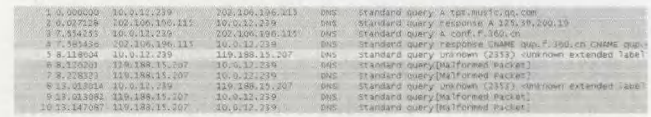

图8 跟踪数据包查杀过程

5）写启动项 360 提示安全，如图 9 所示。

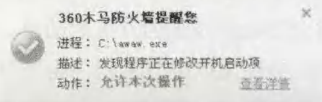

图9 写启动项360提示安全

3 结束语

“云时代”的到来，使得对于云端服务的技术要求大大提高，当“云端”使用者的工作方式简便，就意味着云的另一端的工作量大大增加，安全保证的要求也达到一个更高的层次。在“云时代”，用户的全部数据以及数据的处理都会在服务器端进行，作为信息时代中最有价值的部分，信息及信息处理放在用户的可控范围之外，这本来就是一件需要承担风险的事情。云安全并不是一种纯粹的反病毒技术，我们可以将其理解为一种安全互联网化的思路[10]。利用“云安全”体系，杀毒软件能够更快地收集病毒样本，更快地对病毒进行处理，并能进行常态预警，智能化发展，最终目的可让互联网时代的用户都能得到更快、更全面的安全保护。云安全的发展给现代安全要求提供了更大的可能性，但是云安全本身也存在很多问题，且网络威胁是动态变化的，所以云安全技术永远都处于不断研发、完善和前进的过程中。因此，对云安全的进一步研究显得尤为重要，相信未来的云安全必将为信息安全带来飞跃。（责编 程斌）

参考文献：

[1] 王勇．恶意软件检测与分析关键技术研究 [D]. 上海：上海交通大学学位论文，2009.

[2] 薛质．信息安全技术基础和安全策略 [M]. 北京：清华大学出版社，2007.

[3] 陈丹伟，黄秀丽，任勤益．云计算及安全分析 [J]. 计算机技术与发展，2010，2（20）：2-4.

[4]KOIKE R,NAKAYA N,KOI Y. Development of system for the automatic generation of unknown virus extermination software[C]. Proceedings of the 2007 International Symposium on Applications and the Internet.Washington,DC:IEEE Computer Society,2007:8-8.

[5] 刘鹏．云计算发展现状 [DB/OL].http://www.cnw.com.cn/server-cloud/htm2009/20090403_171367.shtml，2009-04-03.

[6] 任伟．密码学与现代密码学研究 [J]. 信息网络安全，2011，（08）：1-3.

[7] 单长虹，张焕国，孟庆树，彭国军．一种启发式木马查杀模型的设计与分析 [J]. 计算机工程与应用，2004,40（20）：130-132.

[8] Yang Tang,Patrick P.C.Lee,John C.S.Lui,et al.FADE:Secure overlay cloud storage with file assured deletion[A].Proc of the SecureComm'10[C].New York:ACM Press,2010.380-397.

[9] 杨永川．信息安全 [M]. 北京：中国人民公安大学出版社，2007.

[10] 那罡．从云安全到安全云 [N]. 中国计算机报，2010-08-02（036）.