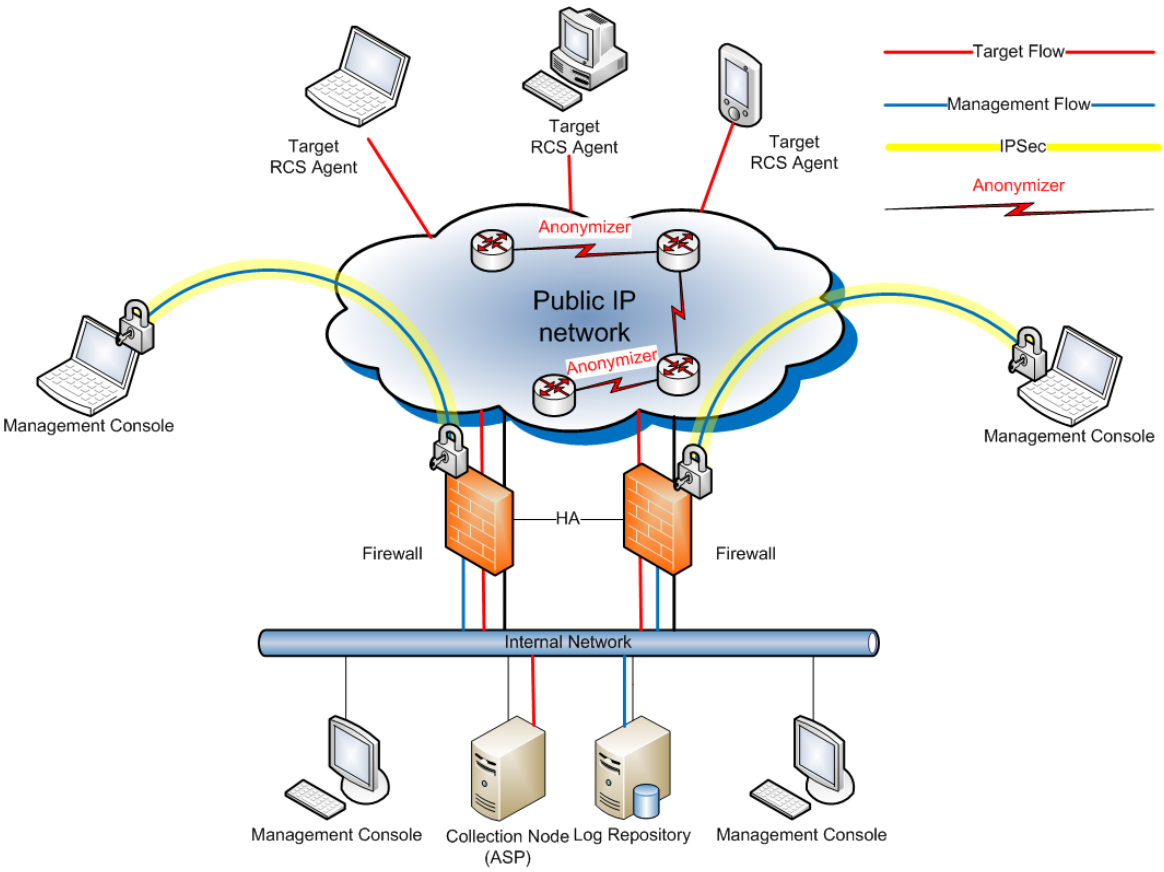
简要分析

Hacking Team 远程控制系统



Content

内容导读

7 月 5 日晚，一家意大利远程控制软件厂商 Hacking Team 的内部数据被泄露出来，其影响力不亚于斯洛登事件及维基解密事件，绿盟科技威胁响应中心随即启动应急响应工作。

1. 6 日，威胁响应中心启动应急分析工作，绿盟 TAC 产品拦截到 Flash 0Day 漏洞攻击；
2. 6 日夜，相关信息及初步建议，第一时间告知客户关注；
3. 7 日，在官网网站发布紧急通告，建议广大用户关注事件进展。分析工作进展进展中；
4. 9 日，发布 Hacking Team 远程控制系统简要分析报告；

这是一份快速报告，以便简要分析其中的核心内容，Hacking Team RCS（远程控制系统）。在后续的报告中，我们将会对此次事件进行深入分析，并给出应对方案。在看完本报告后，如果您有不同的见解，或者需要了解更多信息，请联系：

- 绿盟科技威胁响应中心微博
- http://weibo.com/threatresponse
- 绿盟科技微博
- http://weibo.com/nsfocus
- 绿盟科技微信号
- 搜索公众号 绿盟科技

泄露：Hacking Team

7 月 5 日晚，一家意大利软件厂商[1]被攻击，其掌握的 400GB 漏洞（包括 0day）数据泄露出来，由此可能引发的动荡，引起了业界一片哗然。数据包中主要包含几个大的部分：

- 远程控制软件源码，也是其核心，暂且称之为 Hacking Team RCS
- 反查杀分析工具及相关讨论文档
- 0Day、漏洞及相关入侵工具
- 入侵项目相关信息，包括账户密码、数据及音像资料
- 办公文档、邮件及图片
- 其他

Hacking Team

Hacking Team 在意大利米兰注册了一家软件公司，主要向各国政府及法律机构销售入侵及监视功能的软件。其远程控制系统可以监测互联网用户的通讯、解密用户的加密文件及电子邮件，记录 Skype 及其他 VoIP 通信，也可以远程激活用户的麦克风及摄像头。其总部在意大利，雇员 40 多人，并在安纳波利斯和新加坡拥有分支机构，其产品在几十个国家使用[2]

分析：远程控制系统

大家知道 IT 运维管理中常常用到远程控制软件，比如 Dameware，但 Hacking Team RCS 相比市面上常见的远程控制软件而言，主要区别如下：

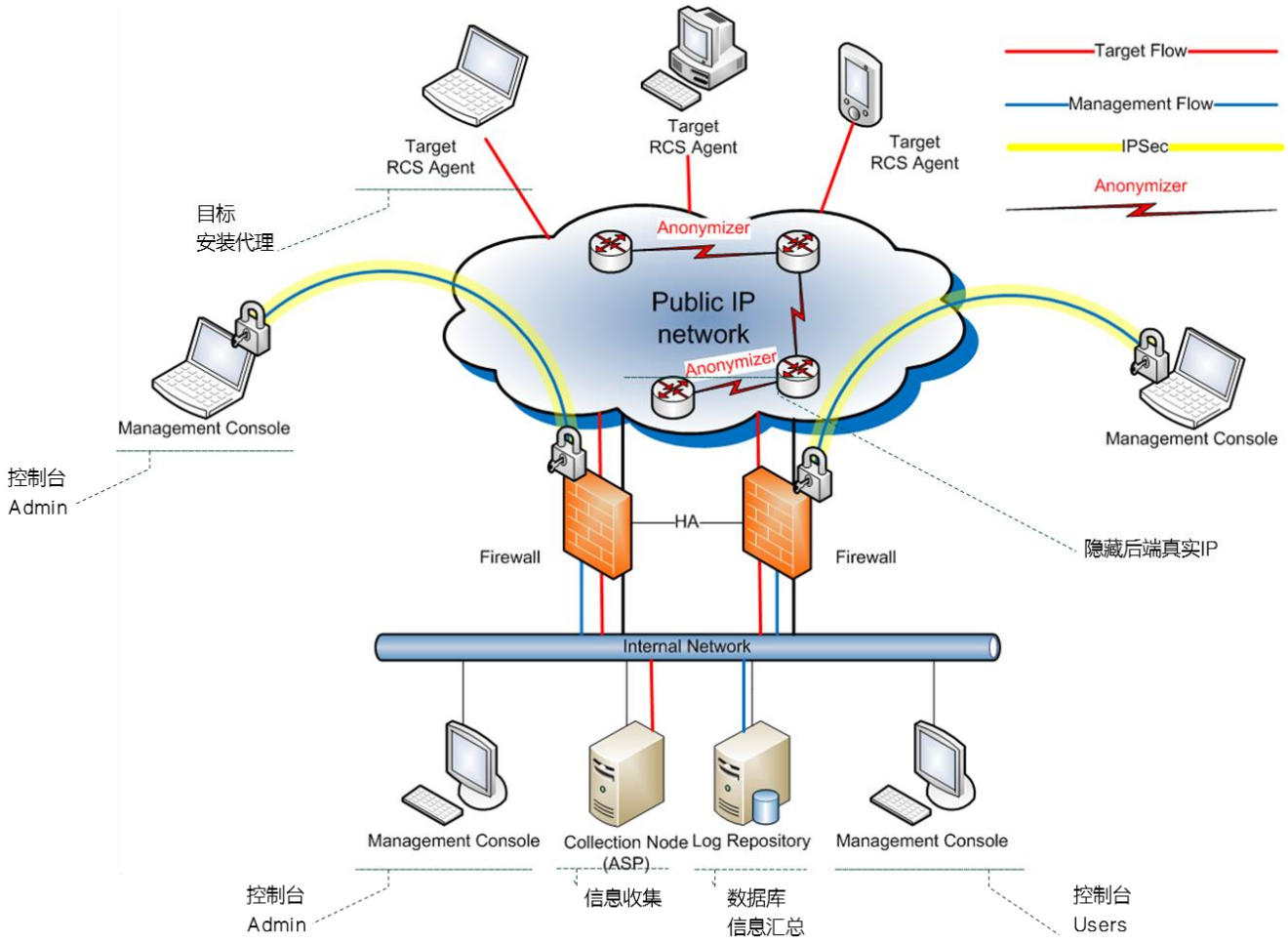
- 系统化管理　　该软件从入侵到目标信息收集分析，有完整的体系架构
  - 这个架构中有不同的功能模块，彼此之间相互配合，完成入侵、安装、信息搜集、监控、集中管理等功能。
- 收集信息　　该软件在后台收集并上传目标用户的信息，包括各类数据、图片、影音等
- 入侵工具　　配合该软件有各种漏洞、利用手段及自动化工具，以便在目标上强制安装 Agent
- 适应能力强　　桌面 OS 从 Windows 到 MacOs X，手机 OS 基本覆盖了市场上流行的系统
- 反追踪　　该软件本地及传播过程数据均加密，让追踪者难以找到攻击者
- 反卸载反查杀　该软件 Agent 不提供卸载方式，并采用各种手段躲避杀毒软件

Hacking Team RCS 系统架构

RCS (Remote Control System)系统是一套非常完善的远程控制系统套件，支持多种平台。

[1] Hacking Team 主页, http://www.hackingteam.it/

[2] Hacking Team介绍 https://en.wikipedia.org/wiki/Hacking_Team



RCS 主要组件

每一块组件具体的功能如下，

- Front-End　　运行在被控制设备上的代理，作为 Back-End 的隔离屏障，保证 RCS 安装的安全性。系统要求是 Windows 2003 or 2008。
- Back-end:　　是整个设施的核心，它存储所有从代理收集到的数据同时处理从管理控制台传来的请求。所有的 RCS 数据都存储在一个标准的关系型数据库，因此该服务还提供额外的功能，比如根据客户的要求实现自动备份和定制数据挖掘。系统要求是 Windows 2003 or 2008。
- Management console　　RCS 的控制台是用于访问和控制所有的远程控制系统（RCS）功能的应用程序。Operators 可以授予系统不同等级的访问权限：Admin 可以创建用户和组，授予权限，管理调查，审核系统；Technician 是创建目标感染、配置/重新配置代理行为的载体；Viewer 浏览来自 target 的信息，对其进行分类或者输出。系统要求是 Windows, MacOS X or Linux。
- Target　　RCS Agent 是监视目标计算机或智能手机上的软件组件。一旦安装成功，Agent 将会通过设备的网络将收集到的数据传送到 Front-End，这些数据有很多种类，比如屏幕截图、电话呼叫等。
    - RCS Agent 有两种安装方式：本地以及远程。本地安装主要是通过桌面系统的 CD 和 USB 存储设备来引导，或者是智能手机的 usb。远程安装则通过 Melting tool、Exploit portal、Network Injector 以及 Remote Mobile Installation。而且每个 RCS Agent 都可以通过远程命令卸载。
    - RCS Agents 的系统要求：

    - Windows XP, Vista, 7 (32/64 bit)
    - MacOs X 10.6 Snow Leopard, 10.7 Lion
    - Windows Mobile 6, 6.5
    - iOS 3, 4 (iPhone/iPad)
    - Symbian S60 3rd and 5th edition
    - BlackBerry 4.5 or newer
- Anonymizers 目的是隐藏 Front End 真实 IP 地址，由于 Anonymizers 之间的连接数据被完全加密而且没有解密数据，所以可以被放置在任何非信任的网络和国家。
- Collection Node 信息搜集功能是通过 Collection Node 来完成的客户端上传信息的搜集，并且允许客户端从服务器上下载新的配置和插件，这个节点是通过提供 ASP 服务完成交互的。这个节点是整个控制系统唯一能从外部进行访问的节点，因此对它的保护也非常关键，比如使用防火墙等措施进行一定的隔离，也需要使用到 Anonymizer 链来对 ASP 真实的 IP 地址进行隐藏。
    - RSSM(Mobile Collection Node)作为 Collection Node 的一个补充，通过蓝牙等手段完成 Collection Node 的功能，并且该节点也会和 Collection Node 完成同步的过程。
- Log Repository Log Repository(RCSDB)是 RCS 系统的存储部件，存储信息包括:
    - 访问过的网站
    - 文件操作
    - 键盘记录
    - 文档和图片信息
    - VoIP 电话监控(例如 skype)
    - 程序执行信息
    - 音频监视
    - Web 摄像头监视
    - 截屏
    - 即时通信（Skype、WindowsLiveMessenge、Wechat 等）
    - 剪贴板的信息
    - 密码信息（email 账户、WindowsLive 账户等）
    - 发送和接收邮件
    - 电话录音
    - GPS 位置
    - 联系人信息

从上面的分析可以看出来，这一次泄露的 Hacking Team 的各种程序中，比较完整的涵盖了实施攻击各个阶段需要用到的一些控制和利用工具，针对其中的一些较为经典的代码，我们经过研究，给出这些工具包的功能，对使用范围做了大致的描述。在这一套 RCS 里，针对电话、pc、网络均进行了控制和信息搜集。

Hacking Team RCS 基本功能

电话监控

针对电话监控，开发了针对不同平台的 agent 程序，下面是一份列表

- core-winphone 针对 Windows Phone 移动平台的远程控制木马客户端，用于实时收集目标系统状态信息，GPS，通讯录，通话短信记录，日历日程安排等隐私信息，还可以执行录音，截取手机屏幕等定时任务，具有远程打开手机摄像头，开启话筒等功能。
- core-winmobile 针对已经过时的 Windows Mobile 移动平台的远程控制木马客户端。也是用于收集目标隐私信息，且具有远程控制收集录音，截屏等功能。
- core-symbian 针对 Symbian 移动平台的远控木马代理，用于收集 GPS 位置，通讯记录，短消息等敏感记录，并可远程实时监听话筒等功能。
- core-android-audiocapture 安卓平台下的语音监听工具，通过注入 AudioFlinger 相关进程达到记录麦克和听筒音频的功能。整个工具包含注入工具 hijack、被注入的库 libt.so，注入后会记录音频信息到 dump 文件，黑客通过 decoder.py 脚本可以将 dump 文件还原成 wav 文件。可以在安卓 3.x 到 4.x 下运行。
- core-android 一个安卓下的 RCS 应用，功能比较完善，可以收集社交软件的信息，应用中还打包了许多利用工具
- core-blackberry 是黑莓下的 RCS 软件。

桌面系统监控

- core-macos 其中包含一个用于 Max OS X 平台可执行文件 macho 文件的加壳加密混淆程序。同时还包含针对 Mac OS X 平台的远程控制木马客户端程序，用于收集目标系统网络连接，文件系统等信息，还可以窃取 iMessage,Skype, 剪贴板等应用的敏感信息，同时还可以键盘记录，截屏，打开摄像头等。
- core-win32 windows 平台木马，主要功能包括：1.窃取主流浏览器如 Chrome、FireFox 和 IE 的 Cookies 等信息 2.对用户 GMail、Outlook、Facebook、Twitter、MSN、Skype、ICQ、Yahoo、Google Talk、Mozilla Thunderbird 等使用进行监控，收集相关信息收集如：帐号信息、相关联系人信息等。监控的 MSN 版本从 6.0 到 2011，Yahoo Messager 版本从 7.x 到 10.x，ICQ Messenger v7.x 3.对麦克风和摄像头进行监控
- core-win64 和 core-win32-master 对应，同样是 windows 平台木马，但项目只是包含了 64 位系统特有的 api hook 框架.
- soldier-win windows 平台木马，功能包括：获取目标计算机基本信息窃取浏览器 chrome、firefox、IE 密码和 cookies 窃取 facebook、gmail、twitter、Yahoo 相关信息屏幕监控、摄像头监控等
- scout-win windows 平台木马，功能相对简单：screenshot、获取目标计算机的基本信息如：CPU，内存，用户名等信息。具有少量简单的反检测机制，如 AntiVM、动态获取 API 地址、黑名单等。子项目 VMProtectDumper 是针对某一版本 VMProtect 的脱壳机

辅助入侵功能

为了在 target 上安装受控端软件并获取主机控制权，还有提供了一些必要的功能

- driver-macos 包含一个 Mac OS X 平台的内核级 Rootkit ，具有用户进程隐藏，文件系统隐藏等功能，还可以 hook 系统调用， mach_trap_table ，并实时追踪用户空间后门的运行状态。
- core-packer 用于 Windows 平台 PE 可执行文件的加壳,加密混淆程序。

- core-android-market 应该是安卓下的类似推送新闻的应用，包括一个名为 org.benews.BeNews 的安卓端的 apk 应用和本地运行的 server，通讯数据为 bson 格式。apk 应用具有自启动功能，会启动推送服务
- core-android-native 安卓相关利用工具的集合，包含了所有安卓 4.1 版本以前的利用工具，包括了 put_user_exploit、towelroot 中的利用工具、selinux 的利用工具等
- vector-ipa ipa 是 Injection Proxy Appliance 的缩写, Injection Proxy Appliance 是 RCS 系统一部分。
    - RCS Injection Proxy Appliance (RCS IPA)是用于攻击的安全设备，使用中间人攻击技术和 streamline injection 机制，它可以在不同的网络情况下透明地进行操作，无论是在局域网还是内部交换机上。
    - IPA 可从监控的网络流量中检测 HTTP 连接，进行中间人攻击，主要有三种攻击方式注入 EXE, 注入 html 和替换攻击。当监控的 HTTP 连接命中预先设置的规则时，IPA 将执行注入攻击。IPA 可以设置需要注入的用户(如 IP 地址)，资源(如可执行文件)等规则。
- driver-win32 core-win32 对应的内核驱动模块，提供功能诸如：权限提升、操作敏感注册表、恢复 SSDT 等。
- driver-win64 相对 32 位版本的驱动，只是注释掉了很多功能代码。
- vector-silent 木马辅助程序：Dropper 和 depacker
- vector-applet 应该是用于挂马的 Java Applet。使用的有可能是未知漏洞，漏洞在 twostage 和 weaponized 文件夹下的 readme 中油描述，“通过 XMLDecoder 获取一个 Bridge 实例的引用，从而导致一个类混淆”。
- vector-edk Intel UEFI（统一可扩展固件接口）BIOS 后门植入工具
- vector-offline2 离线安装 RCS 工具包，可在物理接触时植入 RCS 后门。 可将离线安装工具刻录在 CD-DVD/USB 等可引导介质上，当可物理访问到计算机系统时，可利用该介质启动系统，将后门直接植入计算机中的操作系统中。目前支持对 Linux/OS X/Windows 系统的离线安装。提供了友好的图形界面，可自动识别计算机上存在的不同操作系统，并可识别每个操作系统上存在的用户，然后可针对不同用户分别植入不同类型的后门。
- vector-offline Windows 版的离线安装工具。
- vector-recover 一个 Windows 版的下载器。下载器本身会修改图标和版本信息，将自己伪装成东芝的蓝牙助手工具:btassist.exe。下载器本身会循环访问两个地址的固定 URL:GET /gh/3735928545/deadbee2 判断下载数据的前 32 字节是否是"3j9WmmDgBqyU270FTid3719g64bP4s52"，如果是的话会从第 33 字节开始保存后续数据到临时目录下的 msupd64.exe 文件中，然后执行该文件。
- vector-rmi 一个发送 WAP PUSH 信息的命令行工具，可以将链接以短信形式发送到支持 WAP PUSH 功能的手机上。可自定义各种参数。

Hacking Team RCS 入侵手段

Hacking Team RCS 软件入侵目标，主要通过如下三种方式：

感染移动介质

与很多木马、病毒及流氓软件的传播方式一样，该软件首先还是采取这种低成本的方式进行，感染一些能够接触目标的移动媒体，比如 CD-ROM、USB 等，即便是 OS 或者 BIOS 设置了密码也一样可以感染，从而获取一些环境数据，比如电脑是否可以上网等，为后续的动作提供参考依据。

代理攻击

采用软件或硬件的系统，能够在网络会话过程中修改和注入数据，在某些情况下，可以注入到系统并难以被检测到。同时，也能够感染 Windows 平台上的可执行文件，如果目标电脑从网站上下载并执行这些可执行文件时，Agent 将在后台自动安装，用户不会知晓。

APT

如上两种方式都无法奏效的时候，就会采用多种形式组合入侵，采用相关的漏洞、入侵工具及更多利用手段，详细的分析及防护方案，在后续的报告中呈现。

Hacking Team RCS 信息上传

用于搜集客户端搜集信息的上传通道，是一个强加密和需要认证的通信过程，同时整个上传通道的设计是基于复杂网络环境的，考虑到防火墙、带有域认证功能的代理等等，会通过模仿一个正常用户浏览 web 的过程来进行这一些操作。

信息搜集功能是通过 Collection Node 来完成的客户端上传信息的搜集，并且允许客户端从服务器上下载新的配置和插件，这个节点是通过提供 ASP 服务完成交互的。这个节点是整个控制系统唯一能从外部进行访问的节点，因此对它的保护也非常关键，比如使用防火墙等措施进行一定的隔离，也需要使用到 Anonymizer 链来对 ASP 真实的 IP 地址进行隐藏。

RSSM(Mobile Collection Node)作为 Collection Node 的一个补充，通过蓝牙等手段完成 Collection Node 的功能，并且该节点也会和 Collection Node 完成同步的过程。

威胁情报

SECURITY

从目前此次 Hacking Team 泄露事件情况来看，其造成的反应如同斯洛登及维基解密事件的影响，关键在于尽可能快的了解到相关的情报，以便尽可能快的启动应急响应机制。威胁情报的获取及响应都体现了防御能力的建设程度，威胁情报服务体系至少包含了威胁监测及响应、数据分析及整理、业务情报及交付、风险评估及咨询、安全托管及应用等各个方面，涉及研究、产品、服务、运营及营销的各个环节，绿盟科技通过研究、云端、产品、服务等立体的应急响应体系，向企业和组织及时提供威胁情报，并持续对对匿名者攻击事件进行关注，保障客户业务的顺畅运行。

如果您对我们提供的内容有任何疑问，或者需要了解更多的信息，可以随时通过在微博、微信中搜索绿盟科技联系我们，欢迎您的垂询！

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。