

# 攻击者如何入侵: 追踪 APT 源头

非官方中文译本 · 安天技术公益翻译组 译注

文档信息			
原文名称	How Did They Get In? A Guide to Tracking Down The Source of APTs		
原文作者	Information Week	原文发布日期	2012 年 4 月
作者简介	Information Week (《信息周刊》) 是一本在线数字杂志, 探讨现实和虚拟事件, 总部位于加利福尼亚的旧金山。 <a href="http://en.wikipedia.org/wiki/InformationWeek">http://en.wikipedia.org/wiki/InformationWeek</a>		
原文发布单位	Information week		
原文出处	<a href="http://www.darkreading.com/attacks-breaches/how-did-the-y-get-in-a-guide-to-tracking-down-the-source-of-an-apt/d-d-id/1137509?">http://www.darkreading.com/attacks-breaches/how-did-the-y-get-in-a-guide-to-tracking-down-the-source-of-an-apt/d-d-id/1137509?</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	<p>本译文译者为安天实验室工程师, 本文系出自个人兴趣在业余时间所译, 本文原文来自互联网的公共方式, 译者力图忠于所获得之电子版本进行翻译, 但受翻译水平和技术水平所限, 不能完全保证译文完全与原文含义一致, 同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</p> <p>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担</p>		

	<p>任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</p> <p>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</p> <p>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。</p>
--	--

# 攻击者如何入侵：追踪 APT 源头

如果你认为没有受到高级持续威胁的影响，那你可能是没仔细观察。很难确认你的机构正遭受攻击。确定入侵的范围和受害的范围也是个全新的挑战。为了能有效地防御 APT，安全专家需要采用大量的、可协同工作的工具，重新了解系统和数据攻击，并针对其发展出新的方法。

Michael Cobb

Presented in conjunction with

**dark** READING  
SECURITY  
Protect The Business  Enable Access



# CONTENTS

TABLE OF

- 2 作者简介
- 3 内容摘要
- 4 攻击者如何入侵：追踪 APT 源头
- 4 监控和日志
- 4 图 1：挖掘线索
- 5 图 2：事件的事件跨度占攻击时间的百分比
- 6 图 3：初始攻击和初次攻陷的时间差—大型机构
- 7 行为分析
- 8 在进程中发现
- 9 集体力量
- 10 参考链接



## 关于我们

*InformationWeek Reports* 的分析师借助定性和定量的研究、业务、技术的评估和规划工具，和源自经验的最佳实践，以真实世界的视角来武装商业技术的抉择者。联络方式：常务总监 **Art Wittmann** [awittmann@techweb.com](mailto:awittmann@techweb.com)，内容总监 **Lorna Garey** [lgarey@techweb.com](mailto:lgarey@techweb.com)，特约编辑 **Andrew Conry-Murray** [acmurray@techweb.com](mailto:acmurray@techweb.com)，研究总编 **Heather Vallis** [hvallis@techweb.com](mailto:hvallis@techweb.com)。报告下载地址：[reports.informationweek.com](http://reports.informationweek.com)。



**Michael Cobb**  
*InformationWeek Reports*

**Michael Cobb**, CISSP-ISSAP, CLAS, 是一位著名的，拥有 15 年 IT 行业经验的，信息安全领域撰稿人。他是 Cobweb Applications 的创始人和常务董事，也是一位提供数据安全服务的顾问。他是 *IIS Security* 一书的作者之一。他在主流 IT 刊物上发表了大量的技术文章。Michael 还是微软认证数据库专家。

# SUMMARY

EXECUTIVE

**高级持续性威胁**：正如它的名字的字面意思所示：复杂的和顽固的。很难确定你的企业的系统和数据处于 APT 攻击之下，更不用说要发现该攻击的所有组成部分，找出攻击的源头，确定入侵的范围和遭受的损害，以及确定攻击者（后者是所有任务中最困难的）。为了找到问题的根源，安全专家必须充分利用大量的工具，深入分析（通常是手工分析）日志文件、网络流量和程序代码。日志和监控，行为分析和培训是发现和剖析 APTs 的工作的重要组成部分。事实上，许多企业会发现，他们不能单打独斗。将经验、知识库和商业资源以及安全社区资源相结合，将会是消减并最终消除 APTs 的关键。



## 攻击者如何入侵：追踪 APT 源头

高级持续威胁是一个复杂的安全问题。但是所有 APT 有两个共性：很难检测他们。他们通过不寻常（通常是零日漏洞）的方式进入你的网络。很难发现 APT，一旦你开始试图检测 APT，一项艰辛的工作就真正开始了：找出问题的源头，确定攻击者并指出攻击已经对你的企业的系统造成了什么程度的影响。

要想发现真正的 APT 攻击代码，需要采用一个主动的、实用的方法。方法涉及对日志文件、网络流量和程序代码进行深入分析。这样做的目标是发现能代表 APT 活动的行为：网络探测和数据泄露。即便是最好的和最聪明的安全团队，之前的一些攻击的复杂性对他们来讲也是个挑战。但是安全专家至少应该知道一个方法来处置一个 APT。在本报告中，我们将探讨可以被用来检测和隔离一个 APT 的工具的类型和过程，并且就如何利用这些工具和过程以构建抵御 APT 入侵的防线，提供独到的见解。

### 监控和日志

所有 APT 的致命弱点是，它不得不将它收集到的数据发送回 C&C 服务器，以便能够成功的完成任务。这一网络活动，以及 APT 搜索网络寻找数据的尝试，将为你提供一些（如果你是幸运的）机会，以使得你

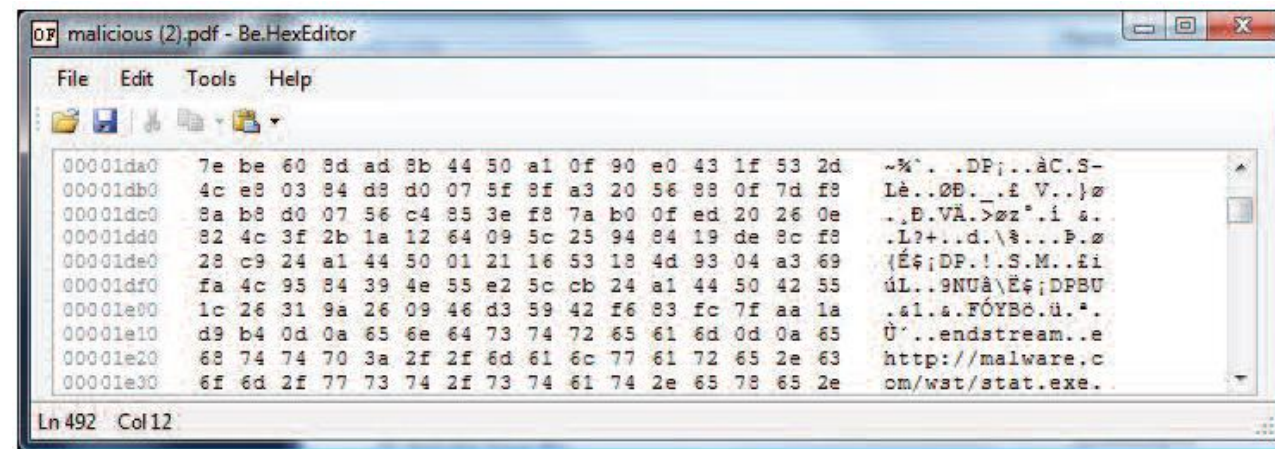
有机会辨别和阻止威胁。因此，至关重要的是，你要广泛的监控和记录网络流量，特别是出站流量。

通过收集和分析网络流量记录，安全团队可以提高发现入侵和其他潜在恶意活动的机会。出乎意料的和可疑的行为包括桌面端口扫描，或文件服务器向网

络外发送流量。此类的，未经许可的活动应该引起警惕，触发你的公司的预警升级的过程。

全面的日志将极大的有助于揭示感染的传播。例如，一个连接未知服务器的机器可能表明某种形式的恶意活动。如果管理员能查询 Cisco NetFlow 或类似的数据库，以搜索哪些机器连接到同样的 IP

图 1  
挖掘线索



一旦该混淆攻击的 shellcode 被从受感染的文件（本例中是一个 PDF 文档）中提取出来，十六进制编辑器的检查有的时候能发现内嵌的恶意链接。在此处，一旦 shellcode 被执行，tat.exe 将会被下载下来

数据: Michael Cobb

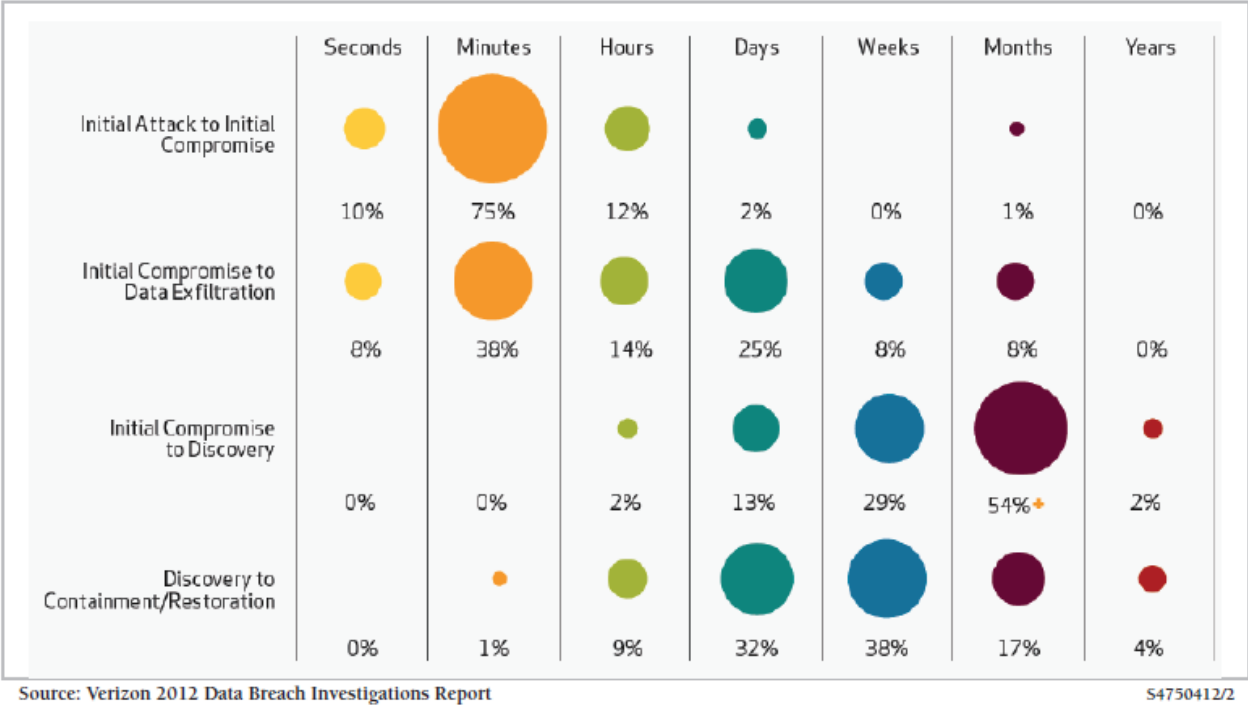
地址和端口，他们就能够针对这些机器做进一步的调查。对这些机器之间的通信的分析能够有助于确定一个攻击源自哪里，哪个机器已经被感染了。

事实上，带宽监控和网络流量分析工具（例如，NetFlow）应被用于收集通过路由和交换机的 IP 流量以供分析。为了使分析更富有成效，一个著名的基线，预期行为应该被建立。这使得有效规则集的建立变得更容易，因为可以依据预期活动来设置阈值。基线能够提供对零日漏洞攻击的更早的预警，因为攻击时，你的网络上的流量将会开始变得不正常。如果资源紧张，就主要针对高风险网段来建立基线。应该对实施网络和安全策略的规则进行审核，以确保对这些敏感系统和数据的连接是被允许的以及被预期的。

OSSEC 是一款免费的，开源的，基于主机的入侵检测系统（IDS）。该系统提供日志分析，文件完整性检查和 Windows 注册表监控。他结合来自各种防火墙，IDSes，Web 服务器，交换机和路由的日志，以提供实时的关联和分析，策略监控和告警。这类工具对于阻断和抓住恶意代码的信息收集过程（例如，端口扫描和暴力破解）是必不可少。

零日漏洞攻击是大多数负责边界安全的管理员的

图 2  
事件的时间跨度占攻击时间的百分比



噩梦。一种防御方式是尝试检测负载。试图确定 APT 活动的一个主要的步骤是配置 IDS 的检测特征，以通过基于出站流量特征的告警来阻断泄露。例如，

一个采用 PI-RAT 或 Poison Ivy 远程访问工具包的 APT 会被一个 IDS 规则捕获。该规则检测 3460 端口的出站流量中是否存在有 PI-RAT 的初始通讯





策略：检测和抵御高级持续攻击

对于大型和小型企业来说，APT 是一个日益严重的问题。要想防护你的企业使其远离这些针对性威胁，需要时刻保持警惕，进行持续的员工培训，与安全系统共同努力来处置 APT 攻击的每个阶段。公司还需要制定一个补救和应对计划，以便应对尽管尽最大努力，但防线还是被突破的情况。

Download

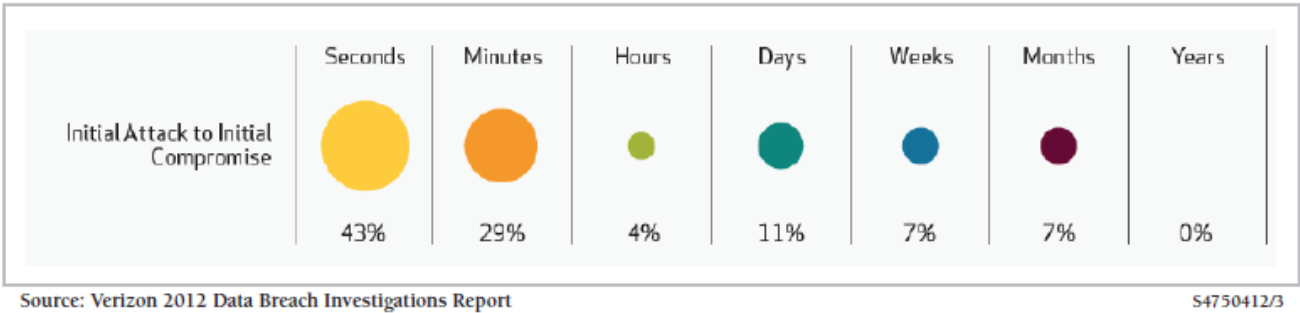
序列标志中的字符串。

尽管我们目前提及的所有工具需要某些手工调试，但是他们是（绝大大部分）自动化的。然而，揭示一个 APT 在需要自动分析的同时，也可能会需要手动分析。

APT 通常做为一个服务运行。在保持对高层的访问和读取其他进程的能力的情况下，它可以恢复一个被试图移除的威胁。重要的是要定期检查日志数据以检查是否正确执行了对控制列表（ALCs）的访问，并评估网络流量态势。例如，如果一个隔离区（DMZ）包含一个 Web 服务器和一个 DNS 服务器，ACLs 被设定为阻断来自任何其他类型的系统的流量，管理员应该检测除 80、443 和 53 端口以外的流量告警。同样的，不正常的上传下载流量的比例可以表明文件正被上载到另一个服务器。此外，一个比常规语句长的 SQL 语句可能是一个 SQL 注入攻击的信号

进行日志分析的一个重要工具是网络协议分析器，例如，[Wireshark](#)。Wireshark 既能够捕获数据包，又能够读取之前存储下来的，被捕获的文件中的数据包。最重要的是，你可以对其进行设置，以便处理特殊类型的流量。这使得它能更快的和更容易的发现你

图 3  
初始攻击和初始攻陷之间的时间—大型机构



正在大量流量数据中寻找的东西。例如，为了掩饰窃取过程，一些攻击使用速变（fast-flux）来规避基于 IP 的 ACLs，并使攻击者自身的网络更难被辨识。正是对 DNS 日志中此类流量的存在性的辨识才能够显示出是否被攻陷和可能发生的窃取。

另一个有助于安全团队更快速的识别事件和升级事件重要程度的方法是拥有用户友好的 IDS 和防火墙的告警。例如，为 IP 地址分配位置信息，这意味着有关管理员不需要执行主机查找的操作就能发现一个数据库服务器已经与一个外网的计算机建立了一个出站 FTP 连接。此类事件需要立刻被调查。

APT 倾向于使用 HTTP 和 HTTPS 做为数据窃取的方式。因此，对出站 Web 流量的过滤需要像对其他出口过滤那样被广泛使用。捕获和阻止一个 APT 将数据发送出网络的一个方法是使用诸如 [Squid](#) 的代理来允许或拒绝流量。例如，如果只有 Squid 代理才可以在 80/443 端口发起 HTTP/HTTPs 出站 sessions，那么一个 APT 将无法直接通过这些端口将数据传出网络。安全团队需要及时了解当前正在被使用中的最新攻击方法。这样就可以针对此类攻击生成对应的规则，以供自动阻断机制使用，并拒绝对特定目的地址的访问或对

工作时间的活动进行限制。通过 SquidGuard，可以自动更新已知恶意 IP 地址和域的黑名单。

除了入侵检测和网络安全监控，另一个有价值的工具箱是 **Security Onion**。它包括一个能够与 Squid 整合的主机工具。这些工具（包括 Snort，Suricata，Sguil，Squert，Snorby，Bro，NetworkMiner 和 Xplico）可以被用于构建一个分布式传感器和控制器集群，以监控和检测早期 APT 行为。当一起使用这些工具的时候，他们能提供可视化的实时报告。尤其是 Squert，Squert 是一个可视化工具，可以通过应用元数据、时序表示、加权和逻辑分组结果集额外提供检测事件的上下文背景。

虽然，APTs 通常是一个直接的目标性攻击的结果，任何恶意软件都可以被用作 APTs 攻击的初始攻击。例如，**RSA SecurID** APT 攻击始于一个钓鱼攻击，因此，一定要使用一个规则集来辨别和阻断由 **Sourcefire 漏洞研究团队** 进行的钓鱼活动。

### 行为分析

一旦你发现了产生可疑流量的恶意软件，你需要剖析它，做进一步的调查。为了确保代码可控，建立一

个虚拟试验环境来进行这项工作是很重要的。为了尽量的捕获恶意软件运行时的信息，很有必要实用一系列监控工具，这包括：

> **Regshot**——一个开源的注册表比较工具。该工具使用户可以快速的生成一个注册表的快照，然后将其与另一个注册表相比较。

> **TCPView**——显示所有 TCP 和 UDP 终端的详细信息列表，包括本地和远程地址以及 TCP 连接的状态。

> **Process Explorer**——提供已经打开或加载的句柄和 DLL 进程的相关信息。

> **ListDLLs**——一个实用工具。该工具列出了被加载进所有进程或一个特定进程中的所有 DLLs，以及加载特定 DLL 的所有进程。

> **VMMMap**——一个虚拟内存和物理内存分析工具，该工具能够显示出摘要信息和一个详细的进程内存映射，以便辨识进程内存的使用情况。

> **Process Monitor**——实时显示文件系统，注册表和进程/线程活动。

> **Capture-BAT**——一个行为分析工具。可以被用来在程序执行过程中，监控系统状态变化，并辨识哪个进程对文件或注册表的改变负有责任。

正如你看到的那样，很必要使用不同的工具来协助确定一个程序都做了什么以及它是如何做的。没人说这是件很容易的工作。但是，使用其中的一些工具或者所有这些工具将会为你提供一个全面的视图。视图展示了注册表，文件系统和系统状态的修改的信息——所有这些向人提供了一种深入洞察软件运行情况的方式，尽管人们手中没有该软件的源代码可用。

好消息是，所有我们在此处列出的工具都是免费的。不好的消息是，需要拥有专业的知识才能使用其中的大多数工具。此外，即使你能使用所有这些工具，你仍然需要去做相当多的检测工作。例如，如果你怀疑一个被这些工具之一发现的.chm 帮助文件（微软编译的 HTML 帮助，该文件通常被用作传播恶意软件的媒介），你应该搜索关于如何使用.chm 创建木马的相关说明。这样做，你将会知道一些关于隐藏在.chm 文件中的可执行文件的可能使用的名字的线索。例如，Perl2Exe 经常被包含在恶意软件中。因为它能在搜索信用卡或其他个人身份信息中分析大量数据。

### 在进程中发现

另一个你需要密切关注的领域是进程。APT 作者通过网络钓鱼攻击和对受害者进行研究来获取内幕信息。他们利用这些内幕信息来了解目标的业务系统是如何工作的，这使他们可以 hook 到相关进程上。特定的恶意软件通常会在内存和存储中辨识敏感数据，或访问正在被处理的数据。人们期望找到恶意软件

的工作原理，它正在抓取什么数据，是从哪里抓取的；恶意软件在获取数据后，正在向哪里发送数据。标准操作包括检查 SOFTWARE\Microsoft\windows\CurrentVersion\Uninstall 中的注册表 key，以期发现安

装了哪个防病毒软件，将哪个恶意代码 DLL 注入到了正在运行的进程中（explorer.exe 是最有可能的目标之一）。APIs 是通称，包括 GetComputerNameA 和 GetLogicalDrives，被用于收集机器和硬盘信息。收集的数据最有可能被写入一个临时文件，然后被压缩成 cab 格式，并重新命名，放在一个文件中

等待提取。然而，恶意软件编写者长期使用加壳的方式来混淆他们的二进制代码，以躲避防病毒程序的检测并使分析师难以对其进行分析。（打包的最初目的是减少一个可执行文件的大小，并提供加密和防范逆向工程以保护应用程序代码中的合法的知识产权和专有代码）使用诸如 ExeInfo PE 的探测器来搜索隐藏的可执行文件，使用诸如 UPX 的打包器来将其解包。但是采用通用的打包器（例如，UPX），会使人们对恶意代码的检测变得更加容易。因次，APT 很可能使用专有的打包程序来伪装自己。这就需要在进一步察看代码之前，对其进行手工解包。你需要使用一个反汇编工具（例如，IDA）或调试器 OllyDbg 追踪恶意软件的每个行动。这一艰辛的过程的目标是破解程序内部是如何工作的，并确定他在哪里将进程注入到合法程序中去的。

在某些时候，该恶意软件会试图连接到他的 CCS。为了使 APT 与外部 IP 地址建立连接，你可以将连接重新定向到一个 REMnux 系统，监听相关端口以模拟响应。（这显然需要在一个隔离的虚拟环境中进行）。发送加密数据之前，该会话可能会以一个标准的 HTTP 请求开始。我们需要对该流量进行捕获和分析，

以检查该请求是否有任何下载更多恶意软件的企图，或者确定是否该流量能提供有关攻击背后的攻击者的进一步线索。应该指出的是，虽然你可能能够通过 IP 地址追踪到该 IP 的注册拥有人，你可能也不能毫无疑问的证明，正是该注册拥有人将你的机构做为攻击目标并入侵了你的机构。

### 集体力量

显然，要想发现一个 APT 并且充分明白它做了什么，需要进行全面的和熟练的分析。为了使你对这些工作具有的挑战性有个概念，我们以 DuQu 木马程序为例。

去年年底，发现了基于 Stuxnet 的恶意代码。这个威胁被命名为 DuQu。因为他创建的文件以 DQ 做为前缀。研究人员分析了代码，但是无法确定它究竟是什么，以及它是从哪里来的。在三月初，Kaspersky 实验室请求帮助，通过众包（crowdsourcing）来帮助破译 DuQu 程序中命令和控制通信模块的代码。经确认，大部分代码是用 C++ 写的，但是有一部分看起来像是由一个全新的编程语言写的。结果发现，这是面向对象 C 代码被

要想发现真正的 APT 攻击代码，需要采用一个主动的、实用的方法。方法涉及对日志文件、网络流量和程序代码进行深入的分析。

## 公有云中的身份管理

,并就哪一种方式适合你的企业,提供了建议。



Microsoft Visual Studio Compiler 2008 通过特殊选项编译而成的。这表明他是被一个由“old school”开发者组成的专业团队开发并整合进 DuQu 的。可能是一些重用旧的,经过良好测试的,来自于一个现存的软件项目的代码。按照这种说法,有针对性的恶意软件往往是非常模块化的,允许构建每个攻击过程(尤其是那些处置泄露的代码),并通常自动发回窃取的数据而不需要攻击者下达发送命令。总之,这些攻击是复杂而多变的。安全专家的有关寻找并了解攻击的努力必须同样精明和灵活。

最后,正如 Kaspersky 依赖社会帮助其剖析 DuQu 那样,安全社区通过联手的方式来对抗 APT 也是非常重要的。事实上,共享所有收集到的,关于一个 APT 的信息对于增进我们对攻击的了解,并因此防御这些攻击来说是非常重要的。FIRST 是一个全球论坛。有来自政府,商业和教育组织的应急响应和安全团队参与在其中。他的任务是在事件预警中促进合作和协调。它可以帮助那些拥有信息资产,吸引外国和竞争对手注意的组织机构协调他们的安全工作。

MORE  
LIKE THIS

## 参考资料

**InformationWeek** 今年发表了至少 150 份报告，他们对[注册用户是免费的](#)。我们将通过提供来自于 IT 专业人士的分析和建议，来帮助你筛选供应商的宣传，评估 IT 项目 and 建设新的系统。在我们的网站上，你会发现：

**数据库防御**：对贵公司最敏感数据的最大威胁可能是那些拥有合法访问企业数据库的权限，但是没有合法意图的员工。虽然从内部发生数据泄露的事件有所下降，但是外部攻击经常效仿他们，并造成严重损失。请遵循我们的建议来降低风险。

**为你的企业选择合适漏洞扫描器**：在一个企业的安全计划中，漏洞扫描器可以被用于检测和修复系统问题，监控安全控制策略的有效性。然而，一个漏洞扫描器只有在被用做一个漏洞管理系统的一部分的时候，才能够增强企业的安全状况。在这个管理系统中，产品、流程和人共同努力寻找、辨识、排序和减轻威胁。

**策略：用户活动监控的基础**：标记正常的活动，监控不正常的用户，这是发现潜在的数据和系统漏洞的一个重要的策略。但是，选择正确的工具只是工作的一部分。如果没有足够的培训、有效的部署和一个好的响应方案，攻击者可能会占上风。

**其他**：署名报告，例如信息周刊薪酬调查、信息周刊 500 和年度国家安全报告，国家全面安全问题等。