Symantec

安全响应

Regin：能够隐蔽监控的顶级间谍工具

赛门铁克安全响应中心

版本 1.0，2014 年 11 月 24 日

“Regin 是一个极其复杂的软件，可以定制各种不同的功能，并根据目标进行部署。”

Regin：能够隐蔽监控的顶级间谍工具

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Regin: Top-tier Espionage Tool Enables Stealthy Surveillance		
原文作者	赛门铁克公司	**原文发布日期**	2014 年 11 月 24 日
作者简介	赛门铁克公司（NASDAQ：SYMC）是一家信息保护公司，随时随地帮助个人、企业和政府寻求技术带来的机会。赛门铁克成立于 1982 年 4 月，是一家世界 500 强公司，经营着全球最大的数据情报网络之一，为重要信息的存储、访问和共享提供了领先的安全、备份和可用性解决方案。 请参阅文末的公司简介。		
原文发布单位	赛门铁克公司		
原文出处	http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance?utm_source=tuicool		
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	• 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。 • 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。		

	• 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。 • 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。

目录

概述

在恶意软件威胁的世界里，只有极少数的例子可以真正被认为是突破性和几乎无可匹敌的。我们已经发现 Regin 就是这样的一类恶意软件。

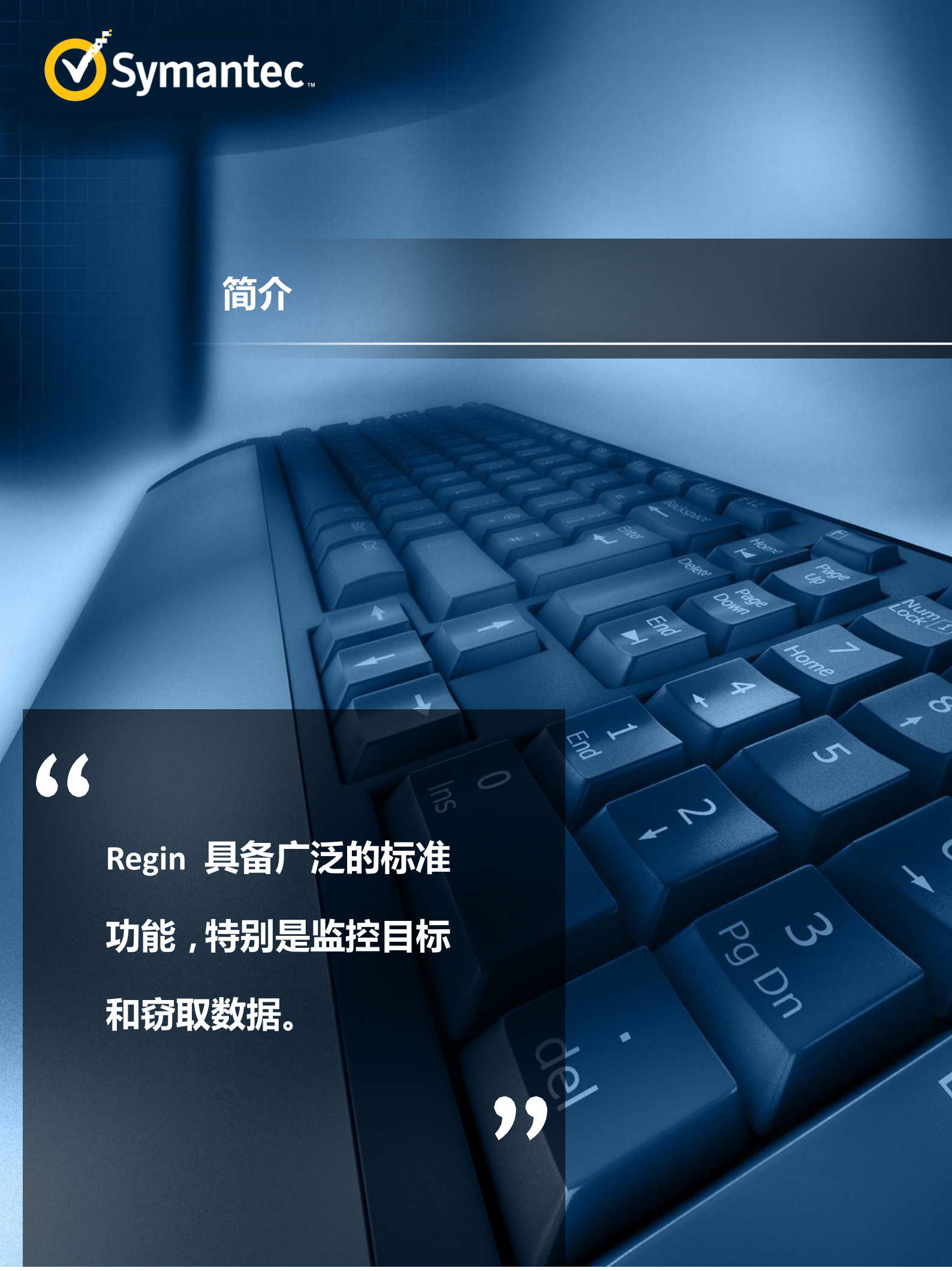
Regin 是一个极其复杂的软件，能够定制各种不同的功能，并根据目标进行部署。它是建立在一个旨在长期执行情报搜集操作的框架之下。它能够在被感染的计算机上隐蔽自身及其活动，在该方面它做的非常好。它的隐蔽性结合了多种我们从未见过的最先进的技术。

Regin 的主要目的是收集情报，其目标包括政府机构、基础设施运营商、企业、学术界和个人。Regin 的先进性和复杂程度表明，它是由资源充足的开发团队历时数月或数年来创建和维护的。

Regin 是一个多级的、模块化的威胁，这意味着它具有许多组件，这些组件相互依赖，从而执行攻击操作。这种模块化的方法提供了灵活性，攻击者可以在需要时加载针对特定目标的自定义功能。一些自定义的有效载荷是非常先进的，表现出专业领域的专业水平。模块化设计也使得对该威胁的分析非常困难，因为我们必须获得所有的组件才能够充分了解它。这种模块化方法也曾见于其他复杂的恶意软件家族，例如 Flame 和 Weevil（面具），而多级加载结构则类似于 Duqu/Stuxnet 家族。

Regin 不同于“传统的”高级持续性威胁（APT），无论是技术和还是最终目的。APT 通常寻求具体的信息，通常知识产权。但是 Regin 的目的不同，它用于数据收集和连续监控组织或个人。基于大量确定样本和组件，该报告提供了 Regin 的技术分析。该分析阐释了 Regin 的体系结构和多个有效载荷。

简介



“Regin 具备广泛的标准功能，特别是监控目标和窃取数据。”

简介

Regin 是一个多功能数据收集工具，可以追溯到数年之前。2013 年秋季，赛门铁克首次开始研究这一威胁。我们发现了 Regin 的多个版本，其目标包括企业、科研机构、学术界和个人。

Regin 具备广泛的标准功能，特别是监控目标和窃取数据。它还能够加载针对特定目标的自定义功能。Regin 的一些定制有效载荷显示了开发者具备特定部门的专业知识水平，如电信基础设施软件。

Regin 能够安装大量的额外有效载荷，其中一些是针对目标计算机高度定制的。该威胁的标准功能包括若干远程访问木马（RAT）功能，如捕捉屏幕截图、控制鼠标的指向和点击功能。Regin 还能够窃取密码、监控网络流量，并收集有关进程和内存使用的信息。它还可以扫描被感染计算机上的已删除文件并将其恢复。我们的研究还发现了针对具体目标的更先进的有效载荷模块。例如，一个模块被设计来监控微软因特网信息服务（IIS）web 服务器的网络流量，另一个旨在收集移动电话基站控制器的管理流量，而另一个则是为了从 Exchange 数据库解析邮件而创建的。

Regin 使用了一些方法来隐藏其数据窃取行为。有价值的目标数据往往不写入磁盘。在某些情况下，赛门铁克仅能检索到威胁样本，而非包含被盗数据的文件。

时间线

赛门铁克发现了 Regin 的两个不同版本。版本 1.0 似乎至少从 2008 年年末用到 2011 年。版本 2.0 从 2013 年起使用，也许之前也被使用过。

版本 1.0 似乎从 2011 年突然被撤回 此日期之后发现的版本 1.0 样本似乎已经被不当删除或无法访问。

该报告主要分析 Regin 的版本 1.0。我们也触及了版本 2.0，但是只涉及 64 位文件。

赛门铁克这样命名这两个版本是因为目前只发现了这两个。Regin 可能有更多个版本，也许版本 1.0 之前，版本 1.0 和 2.0 之间也有其他版本。

目标分析

Regin 的操作者似乎并没有专注于任何特定的行业。Regin 感染了各种组织，包括私营公司、政府机构和科研院所。

感染出现于不同的地理位置，主要集中在 10 个不同的地区。

感染向量

感染向量因目标而异。在编写本报告时尚未证实可复制的感染向量。目标可能被欺骗访问众所周知的网站的恶意版本，该威胁可能通过 Web 浏览器或通过利用应用程序进行安装。在一台计算机上，日志文件显示，Regin 利用一个未经证实的 Yahoo! Instant Messenger 漏洞。

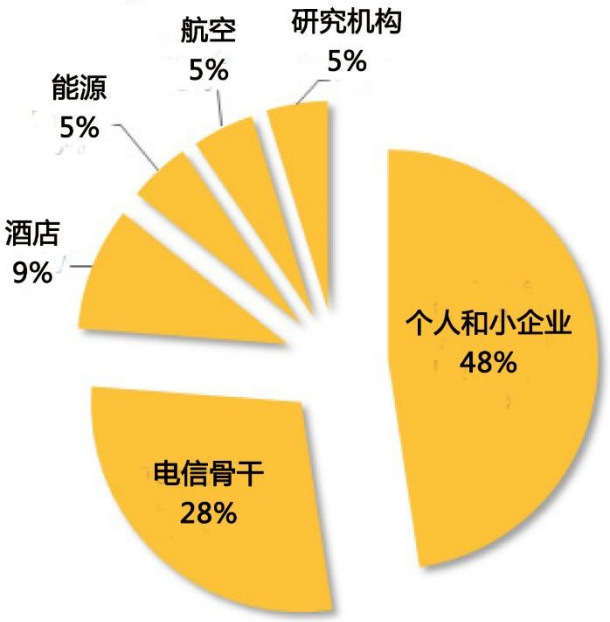


图 1：确定的 Regin 感染（按行业）

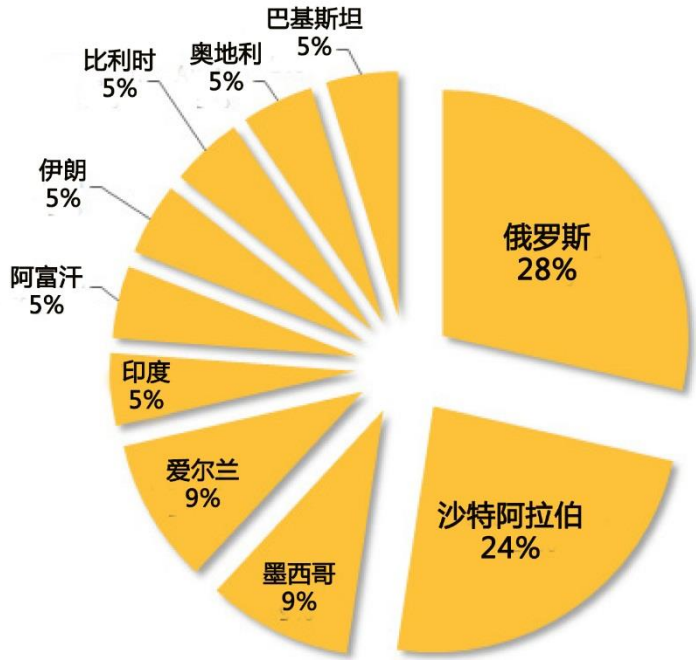
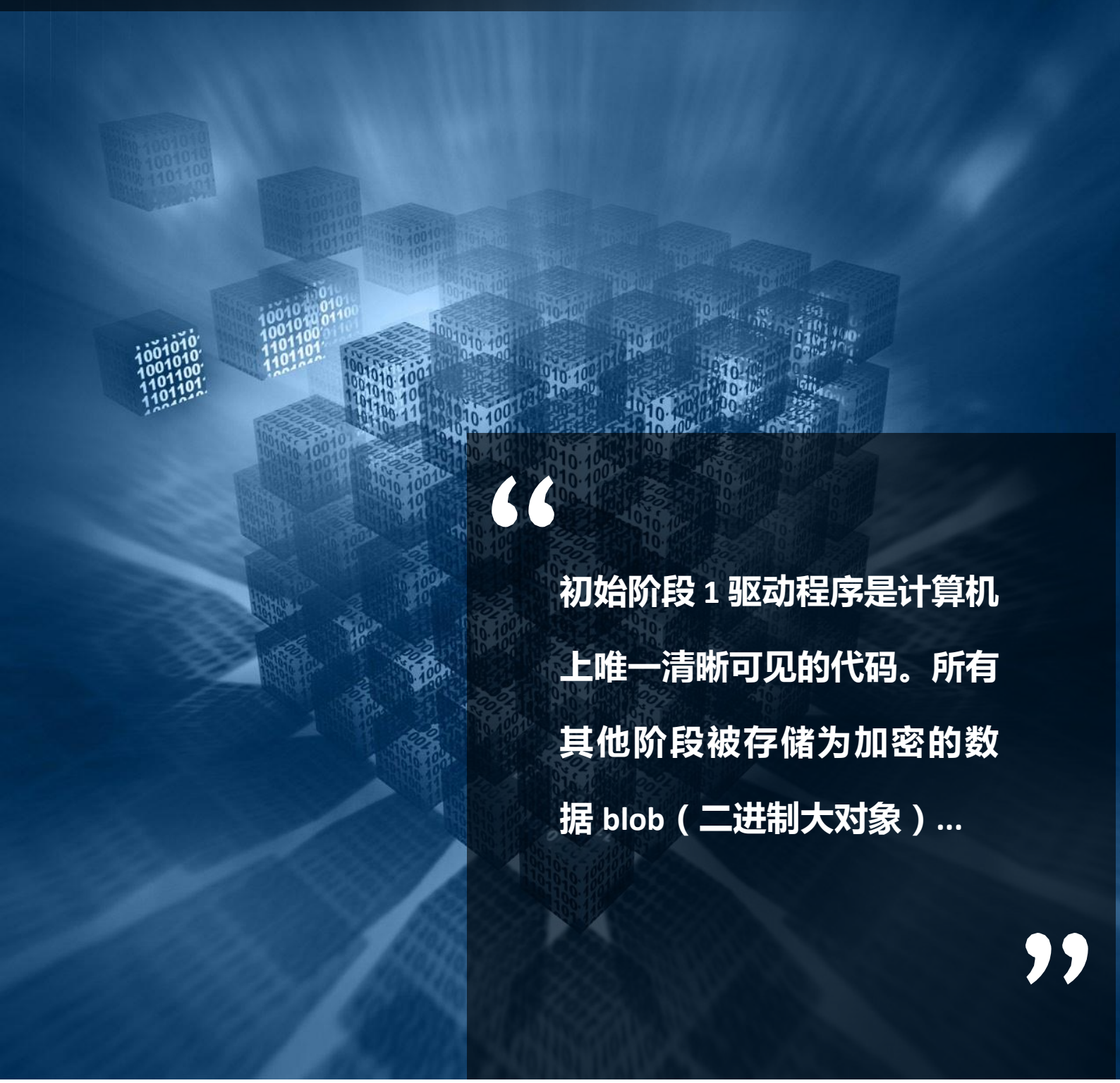


图 2：确定的 Regin 感染（按国家）

体系结构



“初始阶段 1 驱动程序是计算机上唯一清晰可见的代码。所有其他阶段被存储为加密的数据 blob（二进制大对象）...”

体系结构

Regin 有一个 6 级的架构。初始阶段涉及该威胁内部服务的安装和配置。之后的阶段中，Regin 的主要有效载荷发挥作用。本节将简要地介绍每个阶段的格式和目的。最有趣的阶段是阶段 4 和阶段 5（存储可执行文件和数据文件）。初始阶段 1 驱动程序是在计算机上的唯一的清晰可见的代码。所有其他阶段被存储为加密的数据 blob（二进制大对象）、文件，或存储于非传统的文件存储区域内，例如注册表、扩展属性、磁盘末端的原始扇区。

表 1：Regin 的 6 个阶段

阶段	组件
阶段 0	投放器，向目标计算机安全 Regin。
阶段 1	加载驱动程序
阶段 2	加载驱动程序
阶段 3	加载压缩、加密、连网、和加密虚拟文件系统（EVFS）的处理。
阶段 4	利用 EVFS 和加载额外的内核模式驱动程序，包括有效载荷。
阶段 5	主要有效载荷和数据文件

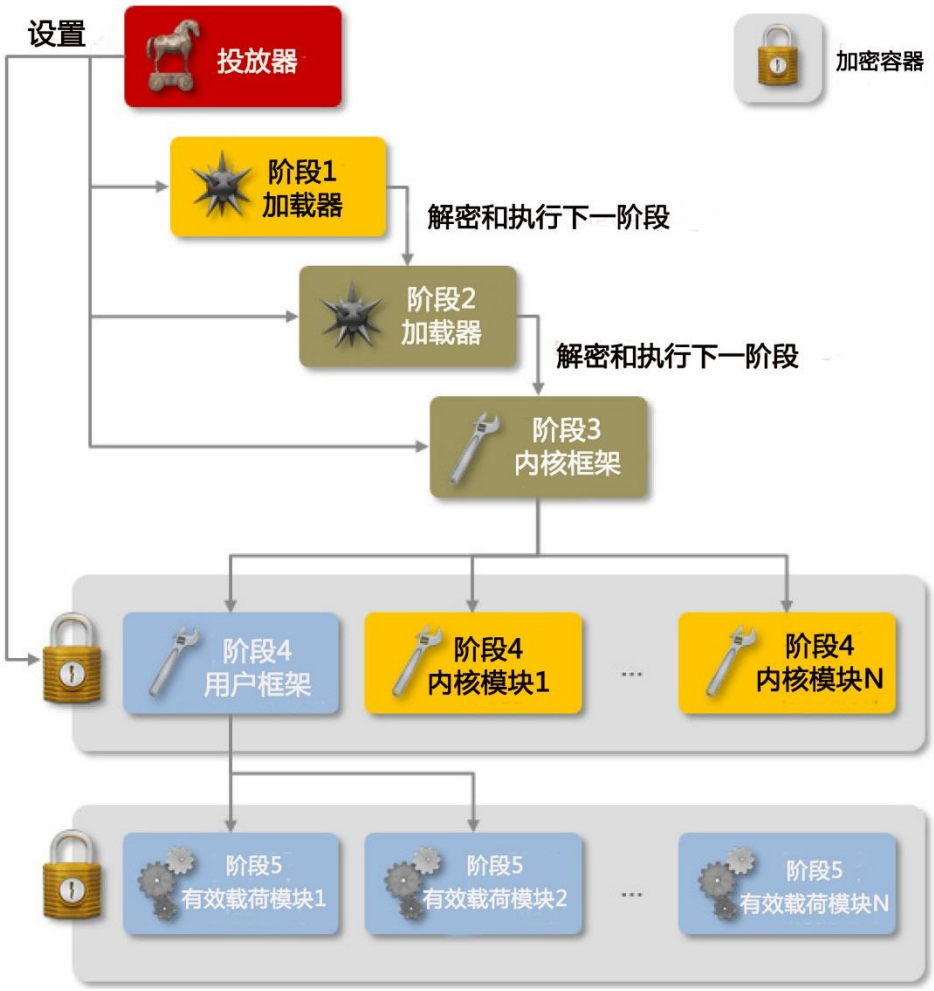


图 3： Regin 的体系结构

阶段 0（投放器）

在编写该报告时，赛门铁克安全响应中心并未获得 Regin 投放器。赛门铁克认为，一旦投放器在目标计算机上运行，它会安装并执行阶段 1。这可能是因为阶段 0 负责建立各种扩展属性和/或注册表项和值，这些内容持有阶段 2、3、4 等的加密版本。投放器可能是短暂的，而不是作为一个可执行文件运行，可能是感染向量攻击代码的一部分。

阶段 1

阶段 1 是威胁的初始加载点。有两种已知的阶段 1 的文件名：

•usbclass.sys（版本 1.0）

•adpu160.sys（版本 2.0）

这些是在阶段 2 中加载并执行的内核驱动程序。这些内核驱动程序可以被注册为系统服务；或可能有相关的注册表项，以便在计算机启动时加载驱动程序。

阶段 1 简单地从一组 NTFS 扩展属性中读取并执行阶段 2。如果没有发现任何扩展属性，则阶段 2 就从一组注册表项执行。

阶段 2

第 2 阶段是一个内核驱动程序，简单地提取、安装和运行阶段 3。阶段 2 不被存储在传统的文件系统中，但是在扩展属性或注册表密钥 blob 中进行加密。

阶段 2 被加密于：

扩展属性

- %Windir%
- %Windir%\fonts
- %Windir%\cursors（可能只在版本 2.0 中）

注册表子项

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RestoreList\VideoBase (possibly only in version 2.0)

这个阶段也可以隐藏阶段 1 的运行，一旦发生这种情况，就没有剩余的清晰可见的代码了。与之前的阶段类似，阶段 2 从 NTFS 扩展属性或注册表项 blob 中发现并加载阶段 3 的加密版本。

阶段 2 还可以监控威胁的状态。该阶段投放文件 msrdc64.dat，大小似乎总是 512 字节。前两个字节被使用，而剩余的字节被设置为零。第二字节显示允许运行的最大实例的数量，它被设置为 2。这意味着任何时候都不能运行一个以上的实例。第一个字节表示多少实例被运行或试图运行。因此，前 2 个字节的潜在组合为：

•0002（威胁不运行）

•01 02（威胁正在运行）

•02 02（威胁正在运行时，第二个实例已经启动）。

阶段 3

阶段 3 是一个内核模式 DLL，不存储于传统的文件系统中。相反，此文件在扩展属性或注册表密钥 blob 中进行加密。

阶段 3 可在以下位置找到：

扩展属性：

- %Windir%\system32
- %Windir%\system32\drivers

注册表子项：

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA5A}

该文件是阶段 2 中的驱动程序的 6 到 7 倍大。除了在阶段 4 中加载和执行，阶段 3 提供了更高级阶段的框架。

阶段 3 和以上阶段基于代码模块的模块化框架。这些模块通过一个私有的定制接口提供功能。在阶段 3 和以上阶段中的每个文件能够向 Regin 的其他部分“导出”功能。

在阶段 3 的情况下，以下图元被提供：

•编制器，解析在阶段 3 和以上阶段中的可执行文件的附加数据中发现的自定义记录。这些记录包含要执行的 Regin 功能的列表。A 记录以数据 0xD912FEAB 开始（低字节序排列）

•压缩和解压例程

•加密和解密例程

•检索高级（阶段 4）组件的存储位置的例程

•处理阶段 4 中使用的加密虚拟文件系统的例程

•网络图元

这些图元通过自定义导出方法提供。

导出方法

通过自定义的导出方法，阶段 3 的 DLL 导出了广泛的功能。用于导出功能的接口不使用传统的 Windows DLL 导出机制（按照名称或序号）。

Regin 导出方法是通过一个元组来引用的。阶段 3 导出几百种方法，分为 12 个主要类别。不同版本使用的数量不同。我们用两个不同的编号方法获取其功能，如表 2 所示。

由于 Regin 的模块化特性，阶段 4 的内核模块和阶段 5 的用户模块（有效载荷）可以使用相同的主要和次要编号方案提供功能和导出例程。

表 2：Regin 的方法分为 12 个类别（示例）

主要的	功能
0001h	内核
000Dh	压缩、解压缩
000Fh	加密、解密
003Dh	EVFS 处理
0007h	容器管理
000Bh	日志管理
0033h	加载
0011h	网络
0013h	网络
C373h	TCP C&C
0019h	UDP C&C
0009h	C&C 处理器

阶段 4

阶段 4 中的文件是由阶段 3 加载的，包括一个用户模式编制器和多内核有效载荷模块。它们作为文件被存储在两个 EVFS 容器中：

- %System%\config\SystemAudit.Evt ：包含阶段 4 内核驱动程序，构成 Regin 有效载荷的内核模式的一部分。
- %System%\config\SecurityAudit.Evt：包含阶段 3 的用户模式版本，文件被注入 services.exe。

当操控 Regin 的攻击者在攻击完成后清理计算机时，他们往往无法从系统中删除阶段 4 和 5 的痕迹。

阶段 4 也使用在阶段 3 中描述的相同导出方法。

阶段 5

阶段 5 包括主要的 Regin 有效载荷功能。阶段 5 的文件被阶段 4 注入 services.exe。

阶段 5 的文件是包含其他文件的 EVFS 容器：

- %System%\config\SystemLog.evt：包含阶段 5 用户模式下 DLL。它们构成了 Regin 的有效载荷。
- %System%\config\SecurityLog.evt :包含阶段 5 的数据文件 ,阶段 4 和 5 组件用其存储各种数据项 。
- %System%\config\ApplicationLog.evt :另一个阶段 5 的日志容器 ,它是由阶段 5 的数据文件引用的。
- %Windir%\ime\imesc5\dicts\pintlgbp.imd （版本 2.0）
- %Windir%\ime\imesc5\dicts\pintlgbs.imd （版本 2.0）

Regin 的有效载荷涉及包含于 SystemLog.evt EVFS 容器中的 DLL 文件。有效载荷的功能因目标计算机而异。定制有效载荷文件将有可能被传输给每一个特定的环境。截至目前，我们发现的示例有效载荷功能包括：

•嗅探低级别的网络流量
•通过各种渠道（TCP，UDP，ICMP，HTTP）提取数据
•收集计算机信息
•窃取密码
•收集进程和内存信息
•爬行通过文件系统
•低级取证能力（例如，恢复被删除的文件）
•UI 操作（远程鼠标指向和点击活动、捕捉屏幕截图等）
•枚举 IIS Web 服务器和窃取日志
•嗅探 GSM BSC 管理网络流量

图 4：EVFS 容器的物理布局

加密的虚拟文件系统容器

Regin 在磁盘上将数据文件和有效载荷存储于加密的虚拟文件系统中。这些文件由主要例程 3Dh 访问。EVFS 容器内存储的文件用 RC5 的一个变种进行加密，使用 64 位块和 20 round（round 是指把数值字段舍入为指定的小数位）。加密模式是逆向密码反馈（CFB）。

EVFS 容器的已知扩展名为*.evt 和*.imd。容器

的结构类似于 FAT 文件系统。一个主要的区别是，文件没有名称；相反地，它们是用二进制标签来标识
的。标签本身是一个主要和次要数字的关联。主要数字通常表明处理文件的主要功能类别。

容器以表 3（低字节序排列）中的标头开始。

标头后面是文件入口表（表 4）。每个文件入口是 13h + taglen 字节长。

其他扇区（表 5）。sectsize 字节的扇区以一个 DWORD 开始，指向下一个扇区（如果该文件不适合单一扇区）随后是有效载荷数据的 sectsize-4 字节。

如上所述，这些文件是加密的。其他加密和压缩层也可能存在，虽然那些会通过更高级别的组件进行处理。

表 3：容器的标头

偏移	类型	说明
00h	WORD	以字节表示扇区大小
02h	WORD	最大扇区数量
04h	WORD	最大文件数量
06h	BYTE	文件标签长度（taglen）
07h	DWORD	标头 CRC（循环冗余校验码）
0Bh	DWORD	文件表 CRC(循环冗余校验码）
0Fh	WORD	文件数量
11h	WORD	使用的扇区数量
13h	-	扇区使用位图

表 4：容器的文件入口表

偏移	类型	说明
02h	DWORD	CRC（循环冗余校验码）
04h	DWORD	文件偏移
D8h	DWORD	存储文件数据的第一个扇区的偏移
DCh	BYTE (taglen)	文件标签

表 5：容器的扇区

偏移	类型	说明
00h	DWORD	下一个扇区偏移，或 D
04h	BYTE[sectsize-4]	数据

C&C 操作

Regin 的 C&C 操作非常广泛。这些反向通道操作是双向的，这意味着： 或者攻击者可以在边界网络中向受感染计算机发起通信；或者受感染的计算机可以与攻击者通信。此外，受感染的计算机可以作为其他感染的代理，C&C 也可以以对等的方式发生。所有的通信都强烈加密并以两阶段方式发生，其中攻击者可使用一个信道接触被感染的计算机，指示它在另一个信道中通信。C&C 可以使用 4 个传输协议：

•ICMP：编码和嵌入有效载荷信息，以代替合法的 ICMP/ping 数据。字符串'shit'分散在数据包中以进行数据验证。此外，CRC 检查使用种子 ‘1337’。

•UDP：原始 UDP 有效载荷

•TCP：原始 TCP 有效载荷

•HTTP：有效载荷信息可以在 cookie 数据中编码和嵌入，名称为 SESSID、SMSWAP、TW、WINKER、TIMESET、LASTVISIT、AST.NET_SessionId、PHPSESSID，或 phpAds_d。这些信息可以与其他的 cookie 组合进行验证，名称为 USERIDTK、UID、GRID、UID= PREF= ID、TM、__utma、LM、TMARK、 VERSION 或 CURRENT。

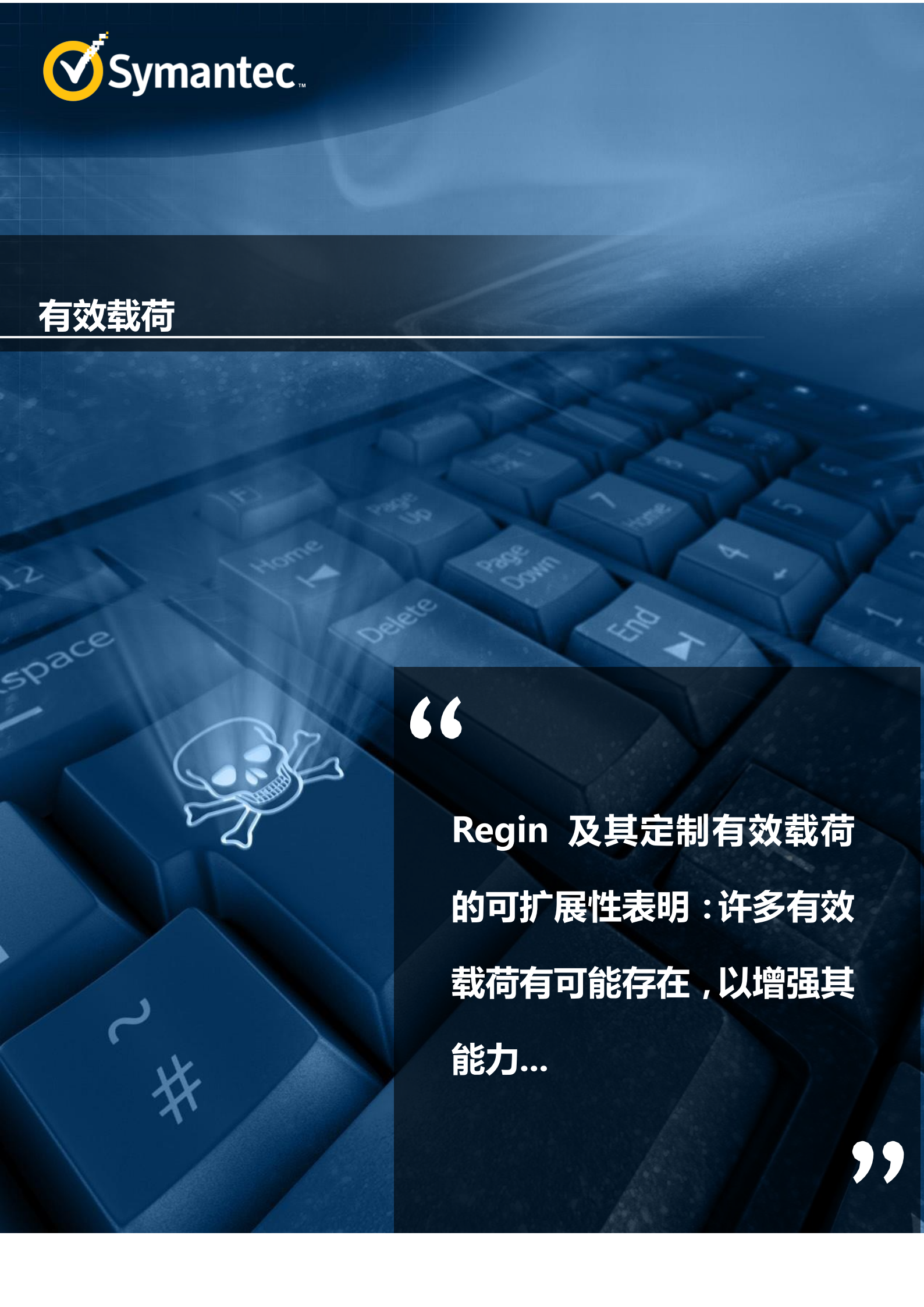
C&C 操作是由各种模块进行的，包括主要类别 C373h、19h、9，以及阶段 5 的有效载荷，如 C375h 和 1Bh。

记录

Regin 记录数据到 ApplicationLog.dat 文件。此文件不是加密的容器，但它被加密和压缩。

Symantec

有效载荷



“Regin 及其定制有效载荷的可扩展性表明：许多有效载荷有可能存在，以增强其能力...”

有效载荷

Regin 可以利用各种有效载荷模块传播，或感染后获得有效载荷模块。Regin 及其定制有效载荷的可扩展性表明：许多有效载荷有可能存在，以增强其能力。此外，我们已经发现了尚未恢复的有效载荷模块的数据文件。下表描述了阶段 4 的内核有效载荷模块和第 5 阶段用户模式有效载荷模块，Regin 的几个变种使用过这些模块。

表 6：Regin 阶段 4 内核有效载荷模块和阶段 5 用户模式有效载荷模块

文件类型	主要的	说明
SYS	0003	驱动程序
SYS	C433	Rootkit
SYS	C42B	PE 加载器
SYS	C42D	DLL 注入
SYS	C3C3	似于 WinPcap（协议过滤器 3.5 版）的网络数据包过滤驱动程序，用于设置 TCP 和 UDP 穿透过滤器并绕过防火墙。执行 BPF（Berkeley 包过滤器）字节码，存储于阶段 5 的数据文件中。
SYS	4E69	网络端口拦截 DLL
DLL	C363	网络数据包捕获
DLL	4E3B	通过注册表或配置文件（例如，prefs.js，refs.js 等）检索 Web 浏览器（IE 浏览器，网景，火狐）的代理信息，枚举会话和用户帐户。
DLL	290B	密码窃取程序 •Windows Explorer 凭据 •Windows Explorer 的 PStore 记录 •Internet Explorer 的 LegacySettings •Winlogon 通知程序包中的数据“cryptpp”
DLL	C375	C&C HTTP/cookies
DLL	C383	SSL 通信
DLL	C361	支持加密功能
DLL	001B	ICMP 反向通道
DLL	C399	ApplicationLog.Evt 的记录创建器
DLL	C39F	处理文件：%Temp%\~b3y7f.tmp
DLL	C3A1	其它功能
DLL	28A5	其它功能
DLL	C3C1	其它功能

DLL	C3B5	收集系统信息 •CPU 内存 •驱动器和共享 •设备 •视窗信息（包括类型、版本、许可信息、所有者信息） •安装的软件 •正在运行的进程（通过 HKEY_PERFORMANCE_DATA id 230） •服务 •计划任务和作业 •运行桌面会话 •用户帐户信息 •系统的审计规则/政策 •系统时间和 Windows 安装时间

IIS Web 服务器日志窃取模块 27E9h 是有效载荷模块的一个例子，它在初始感染后安装并针对特定目标部署。

64 位版本

我们只发现了少量的 64 位 Regin 文件。这些样本可能代表版本 2.0，或它们之间的不同可能只是具体到因为 64 位版本的 Regin 的关系。我们也从被感染的计算机中发现了文件，可能与 64 位 Regin 有关（也可能无关），包括 svcsstat.exe 的几个变种，旨在通过管道或套接字检索二进制数据并执行数据的文件。

文件名

除了一些值得注意的不同点，这些文件似乎并没有从根本上与 32 位文件有所不同。

Regin 的 32 位和 64 位版本使用不同的文件名。这些不同点请参阅本报告的第一章和附录。最重要的是，在 64 位版本的 Regin 中，容器的名称被更改了：

•PINTLGBP.IMD 取代 SystemLog.Evt

•PINTLGBPS.IMD 取代 SecurityLog.Evt

各阶段的不同

64 位版本的 Regin 的阶段 1（wshnetc.dll）已不再是一个内核模式驱动程序，因为 64 位 Windows 下的驱动程序都必须签名。相反，阶段 1 是一个用户模式 DLL，当计算机启动时作为 Winsock Helper 加载。阶段 1 不从 NTFS 扩展属性中加载阶段 2，而是查找磁盘的最后一个分区（就物理位置而言），并搜索原始扇区中的有效载荷。

我们尚未发现 64 位 Regin 的阶段 3。我们认为这一阶段可能不存在，因为 32 位版本是驱动程序。与 32 位版本一样，阶段 4 是一个编织器，并使用相同的主要和次要值来导出功能。

阶段 5 使用下列文件名：

- %Windir%\IME\IMESC5\DICTS\PINTLGBP.IMD 包含阶段 5 用户有效载荷，替代 32 位版本中的 SystemLog.Evt。
- %Windir%\IME\IMESC5\DICTS\PINTLGBS.IMD 包含阶段 5 数据文件，替代 32 位版本中的 SecurityLog.Evt。

•没有发现 SystemAudit.Evt 和 SecurityAudit.Evt 的等效文件。

尚未发现阶段 5 的有效载荷模块。

结论

Regin 是一个非常复杂的威胁，用于大规模数据或情报收集活动。这种威胁的开发和运作将需要大量的时间和资源。这种性质的威胁是非常罕见的，能够媲美 Stuxnet/Duqu 恶意软件家族。Regin 的发现表明：攻击者持续不断地投入大量资源来开发用于情报收集使用的工具。Regin 的许多组件都未被发现，可能还存在其他的能和版本。

保护方案

Regin 组件被命名为 Backdoor.Regin。

附录

附录

数据文件

表 7：阶段 4 的框架 DLL 使用的数据文件

主要的	次要的	说明
0001	-	-
000D	-	-
000F	01	高熵 blob，加密数据
	02	高熵 blob，加密数据
003D	-	-
0007	-	-
000B	01	包含路径到日志文件中。
	2	小的 8 字节文件
0033	01	单一的 DWORD，如 111CH
	3	单一的 DWORD，如 1114h
0011	-	-
0013	01	未知的记录列表
	02	一个字节，如 3
C373	01	netpcap 驱动程序的 BPF 字节码--允许 UDP 直通
	02	一个 WORD 值，如 1
0019	01	netpcap 驱动程序的 BPF 字节码--允许 UDP 直通
	02	一个 WORD 值，如 1
0009	00	单一的 DWORD，如 11030B15h
	1	包含 C&C 的位置信息
	2	要执行的 C&C 程序： • (C375, 1) param= 08 02 • (19, 1) param= 44 57 58 00 • (C373, 1) param= 08 02 • (1B, 1) param= 20 00
	3	要执行的程序 • (4E69, 2) • (19, 2) • (1B, 2) • (C373, 2)(• C375, 2) • (C383, 2)(C363, 2)
	07	用于解密 C&C 数据包的 RC5 值
	09	未知数据
	08	未知数据
	12	单一字节，如 1
	17	未知数据

因为数据文件存储在一个容器中，所以不具有名称。就像阶段 5 的模块一样，它们可通过它们 filetag（文件标签，主要和次要标识符的联合）引用。主要标识符表明哪个主要例程类别可能处理或创建文件。

并非所有的数据文件已被发现，所以目前的信息仍然是不完整的。

还未发现与阶段 4 的内核模块相关的数据文件。

表 8 列出了阶段 5 模块使用的数据文件。

而使用这些数据的相关模块尚未发现。

表 8：阶段 5 的模块（有效载荷）使用的数据文件

主要的	次要的	说明
C363	02	6 字节（01 00 00 00 00 00）
4E3B	-	
290B	-	
C375	01	Dword（1）
	02	Dword（0）
C383	01	Dword（1）
	02	Dword（0）
	10	64 字节（512 位）Diffie Hellman，P（素数）
	11	字节（2）的 Diffie Hellman 的，G（发生器）
C361	10	文件包含时间戳和高熵 dataUnclear
	11	DWORD（E10h）
	12	DWORD（2）
001B	-	
C399	-	
C39F	00	小文件，18h 字节，低熵
	01	加密 unicode 的路径：
C3A1	01	小文件，6 字节（08010000 0001）
28A5	02	小文件，18h 字节，未知
C3C1	-	-
C3B5	-	-
C36B	-	-
C351	-	-
2B5D	-	-
C3CD	-	-
C38F	-	-
C3C5	-	-
27E9	-	-

表 9：孤立的数据文件

主要的	次要的	说明
4E25	00	字节（1）
	01	字节（2）
28A4	00	未知
	02	小文件，8 字节（0100 000000 0000 00）
DEAB	01	小文件，8 字节（00 0001 010400 0000）

威胁信标

以下详细信息可帮助您确定是否已经被 Regin 感染。

文件 MD5

2c8b9d2885543d7ade3cae98225e263b

4b6b86c7fec1c574706cecedf44abded

187044596bc1328efa0ed636d8aa4a5c

06665b96e293b23acc80451abb413e50

d240f06e98c8d3e647cbf4d442d79475

6662c390b2bbbd291ec7987388fc75d7

ffb0b9b5b610191051a7bdf0806e1e47

b29ca4f22ae7b7b25f79c1d4a421139d

1c024e599ac055312a4ab75b3950040a

ba7bb65634ce1e30c1e5415be3d1db1d

b505d65721bb2453d5039a389113b566

b269894f434657db2b15949641a67532

bfbe8c3ee78750c3a520480700e440f8

文件名/路径

usbclass.sys

adpu160.sys

msrdc64.dat

msdcsvc.dat

%System%\config\SystemAudit.Evt

%System%\config\SecurityAudit.Evt

%System%\config\SystemLog.evt

%System%\config\ApplicationLog.evt

%Windir%\ime\imesc5\dicts\pintlgbs.imd

%Windir%\ime\imesc5\dicts\pintlgbp.imd

%Windir%\system32\winhttpc.dll

%Windir%\system32\wshnetc.dll

%Windir%\SysWow64\wshnetc.dll

%Windir%\system32\svcstat.exe

%Windir%\system32\svcsstat.exe

扩展属性

%Windir%

%Windir%\cursors

%Windir%\fonts

%Windir%\System32

%Windir%\System32\drivers

注册表

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RestoreList\VideoBase

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA5A}

公司简介

赛门铁克公司（NASDAQ：SYMC）是一家信息保护公司，随时随地帮助个人、企业和政府寻求技术带来的机会。赛门铁克成立于 1982 年 4 月，是一家世界 500 强公司，经营着全球最大的数据情报网络之一，为重要信息的存储、访问和共享提供了领先的安全、备份和可用性解决方案。该公司在 50 多个国家设立了分公司或办事处，用于超过 21,500 名员工。90%的世界 500 强企业是赛门铁克的客户。2013 财年的收入为 69 亿美元。

欲了解更多信息 ,请访问 www.symantec.com 或与赛门铁克联系：go.symantec.com/socialmedia。

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

对于具体的国家办事处和联络电话，请访问我们的网站。

赛门铁克全球总部
美国，加利福尼亚州（94043），山景城
Ellis 大街 350 号
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com