
目錄

关于	1.1
事件响应基础	1.2
推荐的IR流程和规则	1.3
事件响应示例	1.4
推荐的工具和实用程序	1.5
卡斯基实验室	1.6

卡巴斯基应急响应指南

术语和定义

本章节介绍本指南中使用的术语和定义。以及在本指南内定义的术语。

下面的是本指南中使用的术语：

- **APT**

高级持续性威胁（APT）是一种攻击者可以用获取组织资源访问并且长期不被发现的一种攻击方式。APT攻击的目标最常见的包括侦测和盗窃敏感数据。APT攻击涉及使用定制和高度复杂的软件。

- **artifact**

artifact是在攻击过程中由恶意软件创建或更改的对象。artifact的示例是恶意软件文件，目录，系统日志文件条目和注册表分支。

- **资产**

资产是属于该组织的对象或实体。资产的示例是组织的网络中的工作站，安全控制和存储在工作站上的数据。

- **攻击，网络攻击**

攻击（网络攻击）是攻击者尝试控制，损坏或销毁计算机网络或系统的一种尝试。

- **攻击者**

攻击者是一个组织网络攻击的人（或一群人）。攻击者通常会尝试访问组织的资产。

- **命令控制服务器**

命令和控制服务器（C&C服务器）是向受攻击者入侵的计算机发出命令的计算机。通常，一些恶意软件会向C&C服务器发出请求并接收命令作为响应。

- **防御措施**

防御措施是组织使用的安全控制和过程，以防止网络攻击。防御措施的例子是组织的代理服务器和保护工作站的防病毒解决方案。

- **终端防病毒解决方案**

终端防病毒解决方案是一种保护组织工作站免受网络攻击的软件。终端防病毒解决方案的一个例子是卡巴斯基终端安全解决方案。

- 事件(event)

任何涉及到组织的资产的情况都称为事件。事件通常表示可以在被监控的输入流中识别的消息，模式，值或标记，例如网络流量，错误或信号，计数等等。

- 漏洞利用

漏洞利用是一块软件，一大堆数据或一系列命令，利用攻击者发现的安全漏洞并提供有效载荷。

- 事件（译者注:不作特别说明，事件一般默认为incident）

事件是组织的安全或资产可能受到网络攻击的危害。

- 事件响应

事件响应（IR）是一个解决和管理事件（例如网络攻击）的过程。

- 入侵指标

入侵指标(IOC)是识别网络或系统上的潜在恶意活动的的数据。IOC示例包括异常网络流量，多次失败登录尝试，恶意软件使用的文件的存在以及可疑注册表或系统文件更改，字符串，URL，IP地址和哈希。

- 组织

在本指南中，组织是一个被攻击者攻击的公司。该组织有一个执行事件响应的安全小组。

- 载荷

载荷是攻击者用来达到攻击目标的软件。根据攻击目标，有效负载可能包含恶意或合法的软件，允许攻击者访问敏感数据或对组织造成危害。

- 样本（软件或恶意软件）

软件样本（恶意软件示例）是特定实例或实例的一部分。恶意软件样本由安全小组从受损资产中获得。

- 安全控制

安全控制是组织用来防范网络攻击的设备或软件。

- 安全团队

一个安全团队是由一群组织员工构成的，负责提供安全防护和执行事件响应。

- SIEM系统

安全信息和事件管理(SIEM)系统是通过从组织的工作站，服务器，网络设备和安全控制收集事件来收集事件和其他与安全相关的信息进行分析的一种软件。

- 钓鱼

钓鱼是攻击者采取的一种方法，他或她向组织发送电子邮件以损害组织的资产或获得未经授权的机密数据访问。

- 威胁情报

威胁情报是与潜在或当前网络威胁相关的持续数据流。威胁情报包含入侵指标(IOC)，可用于识别和减轻网络威胁。威胁信息可以集成到SIEM系统中。

- 漏洞

漏洞是组织暴露出的缺陷被攻击者利用进行攻击。

事件响应基础

本章介绍了攻击的杀伤链模型以及针对这些攻击的基本事件响应过程。

攻击生命周期（杀伤链）

本节介绍网络攻击和杀伤链模型的生命周期。

关于杀伤链模型

当进行网络攻击时，攻击者将遵循一系列结构化的操作。描述这组动作的模型之一是杀伤链模型。

最初，军方用杀伤链来描述袭击的结构。当维权者知道攻击者采取的行动顺序时，防守方可以制定防御性战略来对抗攻击。

杀毒链模型被IT安全所采用，可用于描述网络攻击。类似于军事活动中使用杀伤链模式的方式，网络安全团队可以制定防御网络威胁的防御策略。为了成功应对威胁，安全小组必须以防御策略为基础，针对攻击者的行动顺序提供信息。

当应用于网络攻击时，杀伤链模型识别了几个攻击阶段。在杀伤链模型中，攻击者必须通过每个阶段来达到攻击目标。如果攻击者在任何阶段都被阻止执行（进度），则攻击无法成功。

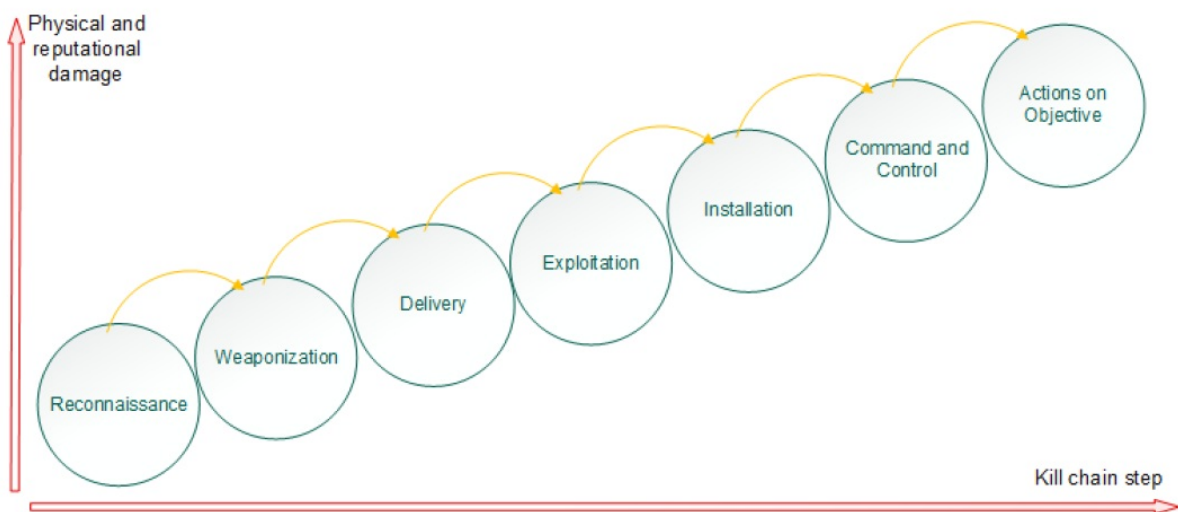


Figure 1: Attack lifecycle (kill chain)

杀伤链模型识别攻击阶段的以下顺序：

1. 侦察
2. 武器化
3. 传播
4. 利用
5. 安装
6. 命令和控制
7. 对于目标操作

网络攻击造成的物理和声誉损失的数量取决于检测到攻击的阶段。阶段也决定了调查的有效性。如果在目标阶段的行动中发现攻击，则安全小组无法对抗攻击，攻击者达到目标。如果在交付或安装阶段早期检测到网络攻击，则会造成最少的损坏。

第一阶段：侦察

在这个阶段，攻击者收集目标组织相关信息及其资产。例如，攻击者尝试获取关于目标组织的结构，组织的技术栈和组织的安全措施的信息。攻击者也可以考虑对员工使用社会工程。例如，攻击者可以创建一个员工社交账户的清单。

为了实现这一阶段的目标，攻击者可以使用被动侦察和主动侦察。被动侦察是在与目标组织的IT基础设施没有直接互动的情况下进行的。例如，攻击者可以获得与被攻击的组织相关的DNS和Whois信息。主动侦察包括与目标组织的积极接触。例如，攻击者可以扫描组织网络中的计算机上的开放端口，搜索安全漏洞，或尝试通过社会工程获取信息。

第二阶段：武器化

在这个阶段，攻击者使用侦察阶段获得的信息来确定如何执行攻击。攻击者选择漏洞利用，载荷以及向有针对性的组织提供漏洞利用和有效负载的方法。

漏洞利用是一块软件，一堆数据或一系列命令，利用侦察阶段发现的漏洞并发送攻击的载荷。攻击者可能会使用现有软件或开发针对目标组织的漏洞专门定制的新软件来实施攻击。

载荷是攻击者用来达到攻击目标的软件。根据攻击目标，有效载荷可能包含恶意或合法的软件，允许攻击者访问敏感数据或对目标组织造成伤害。

攻击者可以选择以各种方式发送漏洞利用。例如，攻击者可能会使用受感染的Microsoft文件或PDF文档，可移动存储设备上的恶意软件或电子邮件附件。攻击者也可能欺骗公司员工访问恶意和网络钓鱼网址，或者破坏公司员工访问的在线资源。

第三阶段：传播

在这个阶段，攻击者发送漏洞利用到目标组织。

发送方式通常包括使用目标公司的公共资源（例如公司网站上的表单），操纵公司员工之一提供漏洞利益，或逼迫与目标公司合作的其他公司。

第四阶段：利用

在这个阶段，漏洞利用了发现的漏洞并提供有效载荷。

例如，漏洞利用可以使用网络安全漏洞在组织的网络中的计算机上安装恶意软件。恶意软件然后感染组织网络中的其他计算机，并将有效载荷分发给所有受感染的计算机。

第五阶段：安装

在这个阶段，载荷会感染目标计算机，安装自身，并尝试隐藏其活动以避免检测或删除。

通常，载荷将尝试以这样一种方式安装自身，即使发现和修复了漏洞利用的漏洞，仍然保持其可操作性和未检测到的能力。

例如，载荷可能包含后门。后门将其本身安装在受感染的计算机上，修改系统注册表以在系统启动时运行后门，并隐藏自己的进程，因此用户无法在运行的程序列表中看到它。当后门运行时，攻击者可以连接到它并控制受感染的计算机。

第六阶段：命令和控制

在这个阶段，载荷等待来自攻击者的命令。

接收命令的最常见方法是建立与目标组织网络中的命令和控制服务器（或C&C服务器）的连接。C&C服务器由攻击者控制。一旦建立连接，攻击者就可以向有效负载发送命令，并采取行动来实现目标。例如，如果有效载荷包含后门软件，则攻击者可以控制受感染的计算机，访问这些计算机上可用的信息，并监视用户活动。

如果受感染的计算机无法直接访问Internet，并且无法建立与C&C服务器的连接，攻击者可以通过传递其他恶意软件向载荷提供命令。

第七阶段：对于目标操作

在这个阶段，攻击者使用在攻击过程中下载的载荷和其他软件来实现攻击目标。

一旦攻击者掌握该组织的资产之一，他或她将试图窃取，更改或销毁受损资产上可用的数据。

例如，如果攻击的目标是窃取敏感数据，载荷是后门软件，则攻击者可以对受感染的计算机进行控制，并搜索存储在其上的所需数据。

如果数据未被存储在受感染的计算机上，则攻击者可能会使用称为横向移动的技术。攻击者可以使用他或她控制的计算机来感染组织网络中的更多计算机，窃取用户凭据来访问不可用的计算机，甚至欺骗其他员工通过模拟使用受感染计算机的员工来丢弃所需的数据。

应急响应步骤

本节介绍事件响应过程的基础知识。

关于事件响应

事件响应（IR）是解决和管理事件结果（例如网络攻击）的有组织的过程。

事件响应的主要目标包括：

- 减小攻击危害
- 减少灾复时间
- 制定将来防止这种攻击的指示和防御措施。

事件响应的过程从安全事件的调查开始。当安全小组调查事件时，必须确定：

- 攻击途径
攻击者提供有效载荷的手段。
- 载荷和漏洞利用
攻击者利用的恶意软件和其它工具。
- 攻击目标
受攻击影响的网络、系统和数据。
- 造成伤害
攻击造成的物理和声誉损失的数量。
- 攻击状态
攻击生命周期的当前阶段，攻击者是否能够执行行动来实现目标，以及攻击者是否达到攻击目标。
- 攻击时间线
何时攻击开始和结束，何时被检测到，以及何时安全小组能够对攻击做出反应。

调查完成后，安全小组必须使用获取的信息来恢复目标系统，并更新安全策略和IR计划。

关于事件响应阶段

根据有关攻击生命周期的信息，安全小组可以制定防御性战略并将其用于事件响应。事件响应示例章节中提供了应用此类策略的示例。

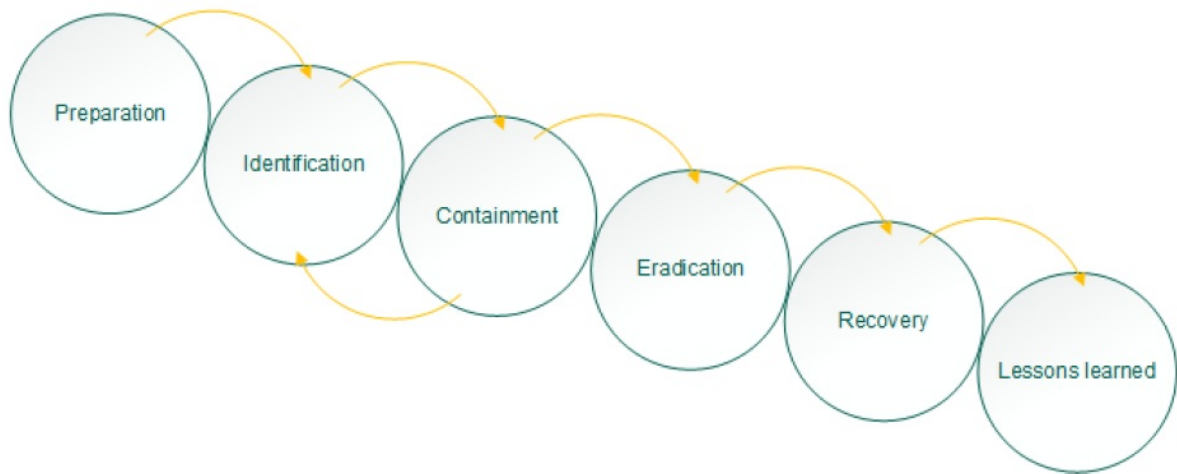


Figure 2: Incident response phases

事件响应过程包括以下阶段：

- 1.准备
- 2.鉴定
- 3.遏制
- 4.根除
- 5.恢复
- 6.经验学习

第一阶段：准备

发生攻击时，安全小组必须采取快速准确的行动。这需要做好准备。安全团队的成员必须准备可以帮助防止，检测和应对网络攻击的流程，工具和策略。

准备工作还必须包括对公司员工的培训。所有公司的员工都必须熟悉安全策略，并知道在面对网络攻击时该怎么办。

进行事件响应的安全小组必须通过不断获得事件响应领域的知识和不断的实践来建立专业知识。

第二阶段：鉴定

在此阶段，安全小组必须确定事件(event)是否是信息安全事件。为此，安全小组必须将可用事件信息与已知的入侵指标进行比较。

入侵指标（IOC）是识别系统或网络上的潜在恶意活动的的数据片段。IOC示例包括异常网络流量，多次失败登录尝试，恶意软件使用的文件的存在以及可疑注册表或系统文件更改。

为了收集IOC，安全小组可以从公开报告和威胁资料中获取信息，并对恶意软件进行静态和动态分析。

在不启动软件的情况下执行静态分析。它可以用于获取几种类型的IOC，包括软件使用的Web和电子邮件地址以及其文件的散列。

动态分析需要在受保护的环境（沙箱或独立计算机）中执行该软件。动态分析允许检查与之相关的软件行为和IOC收集。

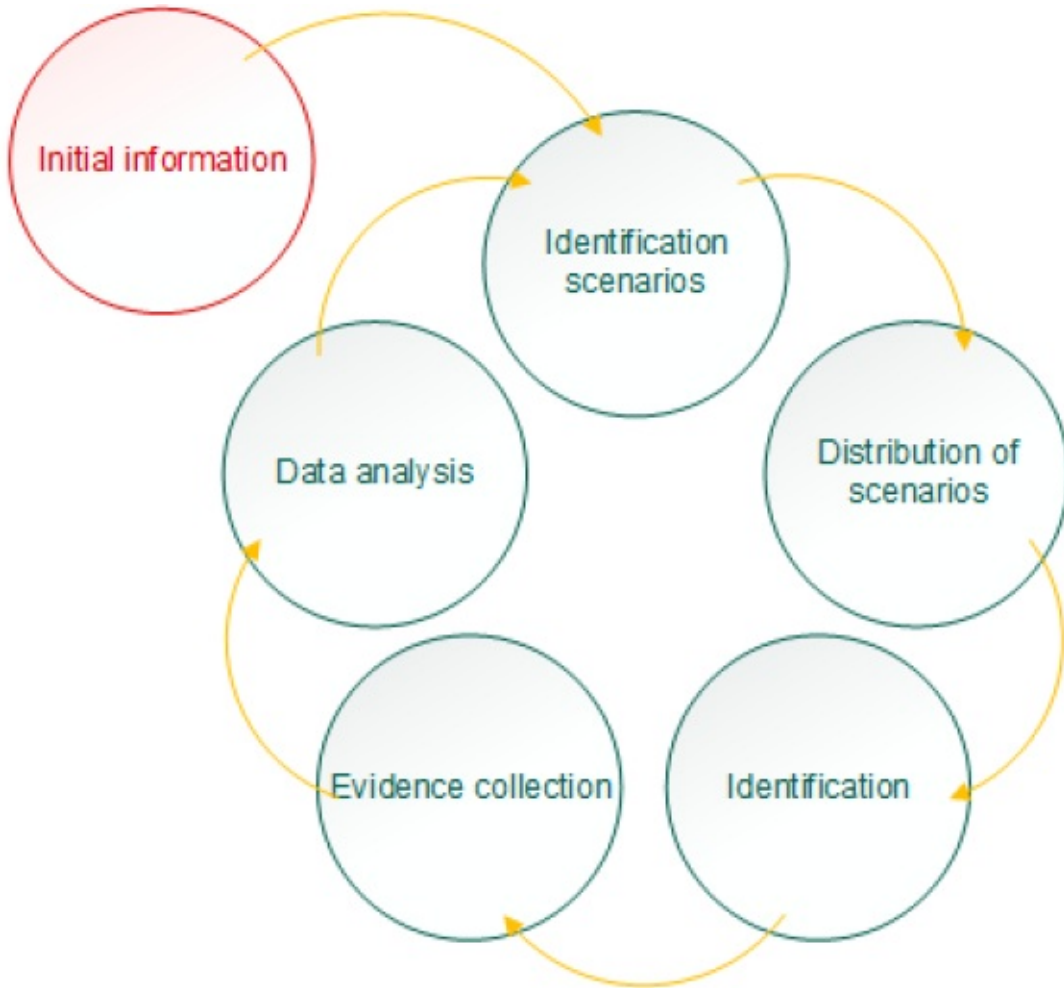


Figure 3: IOC collection cycle

收集IOC是一个循环过程。根据有关攻击的初步信息，安全小组可以创建检测方案。应用这些场景通常可以检测到新的IOC。新的IOC有助于进一步识别攻击并获得更多信息，从而创建一个循环。

只有事件（*event*）被认为是信息安全事件，才能继续执行IR进程的剩余阶段。

第三阶段：遏制

在此阶段，安全小组必须识别受损的计算机，并调整安全策略，以防止公司资产的进一步感染。安全小组还必须重新配置组织的网络，避免受到已经被攻击的资产的影响。

例如，如果组织网络中的其中一台服务器受到攻击者的危害，则安全团队必须将该服务器与网络隔离。安全团队还必须调整路由策略，将此服务器的负载分发到其他服务器。

第四阶段：根除

在此阶段，安全小组必须将受损资产恢复到原始状态。这通常涉及删除恶意软件，恢复配置和删除恶意软件遗留的任何组件。

例如，如果计算机受到后门软件的侵害，安全小组必须删除后门软件，将受损文件和系统注册表恢复到原始状态，并删除后门软件安装文件。

第五阶段：恢复

在此阶段，之前受到攻击的资产重新投入使用。安全小组必须监测资产的状况一段时间，以确保威胁得到彻底消除。

例如，如果组织网络中的其中一个服务器已恢复，则安全小组将其重新安装到组织的网络中，调整路由策略以使用此服务器，并监视服务器的行为一段时间以确保没有可疑活动。

第六阶段：经验学习

在这个阶段，安全小组必须对事件进行分析，制定有助于防止今后发生事件的措施，并更新此类事件的事件应急计划。

这些措施可能包括调整安全政策，改变组织资产的配置，以及对公司员工进行信息安全培训。

事件响应计划是一组书面指示，可以识别事件和对其的响应。即使不可能在将来完全防止事件发生，事件响应计划也将有助于尽可能减少事件发现所需的时间，提高事件响应的有效性。

推荐的IR流程和规则

本章介绍了事件响应和进行事件调查的规则和建议。

准备

本节为事件响应过程的准备阶段提供建议。

防御措施

为了有效防范网络攻击，安全团队必须采取防御措施保护组织资产。建议创建几层保护，从而创建一个可以抵御多种攻击方式的网络攻击的防御边界。

例如，考虑以下防御措施：

- 在所有工作站上安装终端防病毒解决方案。
- 在网络中安装入侵防御系统。
- 通过防火墙保护互联网的网关。
- 互联网访问只能以授权的方式通过组织的代理服务器进行。
- 组织使用SIEM系统跟踪事件。SIEM系统集成了威胁情报。
- 网络攻击的诱饵系统（也称为蜜罐）由安全小组隔离并密切监控。

卡巴斯基实验室专家不断开发新的安全解决方案，为各种信息安全威胁以及网络和网络钓鱼攻击提供全面的保护：

- 为了保护工作站免受已知的，未知的和高级的威胁，卡巴斯基实验室专家开发了卡巴斯基终端安全。
- 为了保卫企业免受有针对性的攻击和高级威胁，卡巴斯基实验室专家创建了卡巴斯基反目标攻击平台（KATA）。

有关卡巴斯基实验室企业安全解决方案的更多信息，请参阅：

<http://www.kaspersky.com/enterprise-security>

渗透测试

渗透测试是对计算机系统的模拟攻击，可以检测其中的安全漏洞。渗透检测可以由第三方组织进行，渗透测试的结果将被报告给安全小组。然后，安全小组可以使用此信息来修复这些漏洞。

获得专业知识

安全小组成员必须（通过学习）不断增加事件响应理论和实践的知识。

卡巴斯基实验室课程提供广泛的网络安全课程，从基础到专家的技术和评估。所有这些都可以在客户处所或当地或地区卡巴斯基实验室（如果适用）上课。有关教育的更多信息，请参阅<http://www.kaspersky.com/enterprise-security/intelligence-services>

了解信息安全领域的事件和趋势以及关于新兴的网络安全威胁的信息以及针对这些威胁的防护措施至关重要。例如，作为卡巴斯基威胁情报门户解决方案的一部分的APT报告服务可以持续访问卡巴斯基实验室调查和高调网络间谍活动领域的发现。

收集应急响应信息

安全小组必须收集有关事件和事件响应过程的信息，并制定准备好的事件响应计划。该信息可以包括事件报告和有关组织内发生的事件历史的信息。

识别

本节为事件响应过程的识别阶段提供建议。

事件触发器

本节描述可能是信息事件触发器的事件(event)。

本节中描述的事件和事件触发器不构成与网络攻击相关的可疑行为的完整列表。

什么是事件触发器

事件触发是指潜在存在网络威胁的事件。当生成事件触发器时，安全小组必须意识到可能正在进行网络攻击。事件触发器允许安全团队将信息事件与事件区(event)分开来。

关于事件源

事件可以来自多种来源。这些来源可能是防APT系统，蜜罐，入侵防御系统和很多其他安全控制。

基于本指南的目的，事件被认为来自单一类型的事件源 - SIEM系统和旨在管理企业网络中的端点防病毒解决方案的系统。

由SIEM系统生成的事件触发器

SIEM系统可以从非常广泛的软件和硬件安全控制范围（包括代理服务器和防火墙）汇总信息。

在由SIEM系统汇总的事件(event)中，由于将安全控制事件与威胁馈送匹配而产生的事件可以被认为是事件触发器。这种事件的存在表明，在安全控制产生的事件中检测到来自威胁情报的入侵指标(IOC)。

为了本指南的目的，假设使用卡斯基实验室的数据馈送将事件与SIEM相匹配。数据情报是卡斯基威胁情报门户的一部分。

例如，组织网络中的计算机上的恶意软件尝试访问恶意URL。与常规URL一样，组织的代理服务器会生成带有恶意URL的事件，并将其发送到组织的SIEM系统。然后SIEM系统尝试将此URL与卡斯基实验室威胁资讯提供相匹配。匹配成功，因为这是卡斯基实验室威胁资讯提供中包含的恶意网址。SIEM系统收到一个新的事件来表示此匹配。这个新事件(event)可以被认为是一个事件触发器。

由反病毒管理系统产生的事件触发

防病毒管理系统可以汇集来自端点防病毒解决方案保护的工作站的事件。

当一个工作站或安全控制台上的端点防病毒解决方案检测到威胁时，会生成一个事件(event)并将其发送到防病毒管理系统。

并非所有这些事件(event)都是事件触发器。例如，关于检测恶意软件的事件之后可能是关于消毒这种恶意软件的事件。在这种情况下，不需要调查。

只有以下反病毒管理系统收到的事件(event)才能被视为事件触发器：

- 尝试访问已知的C&C服务器
- 尝试杀毒失败
- 在同一台电脑上重复检测到恶意软件
- 防病毒软件错误和故障导致保护级别降低

安全团队对于这些事件(event)触发器的响应应该与对在SIEM系统中接收到的带有恶意哈希或者恶意URL的事件(event)的响应相同。反病毒系统中的所有事件(event)也可以发送到SIEM系统中。

可能成为事件触发器的可疑行为

还有其他事件可能成为事件触发器。这种事件的存在需要安全小组的关注和调查。

以下是可疑事件的示例：

- 存在操作系统启动时自动运行的未知软件。
- 在系统服务列表中存在未知服务。
- 从不太可能用于运行可执行文件的目录执行文件，例如从临时目录和系统缓存执行。
- 从存在这些动态库文件的目录加载动态库是不太可能的。例如，当一件软件从软件的可执行文件所在的目录加载系统库时。
- 意外升级的用户权限。
- 存在可由攻击者使用的合法软件。此类软件的示例包括mimikatz，Windows®凭据编辑器和许多远程管理工具。

以下事件构成与网络活动相关的可疑行为：

- DNS或ICMP协议流量意外上升。
- 与频繁更改其IP地址的域的交互。这种行为可能表示攻击者使用快速通量DNS技术将C&C服务器隐藏在作为代理的受攻击的主机的网络之后。
- 与卡斯基实验室威胁情报提供的分类的网址进行互动。例如，URL可以被分类为恶意软件源或漏洞利用包登录页。
- 与卡斯基实验室威胁情报分类的IP地址进行交互。例如，IP地址可以被分类为用于扫描网络的IP地址或用作进行DDoS攻击的IP地址。
- 与具有可疑Whois信息的域的交互。

优先级准则

本节介绍事件优先级的基础知识。

时间是IR过程中可能最缺乏的资源。攻击开始与安全团队的响应之间的时间量决定攻击者是否达到攻击目标。如果安全小组一下子面临着大量的安全事件，可能没有足够的时间对所有安全事件作出反应。在这种情况下，事件必须按优先级分类。

事件优先事项必须根据以下因素确定：

- 受攻击的计算机所在的网段。
- 存储在受感染计算机上的数据的价值。
- 影响同一台电脑的其他事件的类型和数量。
- IOC与事件相关的可靠性。

最终事件优先级必须根据每个组织的具体情况确定。对于一些组织来说，最危险的事件是那些涉及ransomware（恶意软件加密受感染计算机上的数据）的事件，因为组织使用知识产权或敏感数据。由于与此软件的使用相关的声誉风险，其他组织可能将与潜在危险软件（例如色情内容）相关的事件设置更为优先。

例如，安全小组可能会使用事件的以下优先次序：

1. 与高级持续威胁（APT）相关的事件是首要任务。有关检测APT的更多信息，请参见下面的“检测高级持续威胁”小节。
2. 与恶意软件相关的事件具有第二优先。
3. 与潜在危险软件相关的事件（广告软件，色情内容等）具有第三重要性。

检测高级持续威胁

高级持续威胁（APT）是一种攻击类型，攻击者可以访问组织的资产，并尝试长时间不被发现。APT攻击的目标最常见的包括侦测和盗窃敏感数据。

要确定检测到的攻击是否必须被视为APT，请使用以下标准：

- 卡斯基实验室APT报告刊登IOC。APT报告是卡斯基威胁情报门户解决方案的一部

分。

- 与之前由另一个APT使用的C&C服务器的交互。这种互动可以通过静态和动态威胁分析来确定。

要分析威胁的行为并获取与其进行交互的URL列表，建议使用“分析工具”一节中描述的工具和实用程序。

如果在卡斯基实验室威胁情报IOC的普及程度值为2或以上，则威胁是常规的恶意软件。这种威胁不能被认定为APT。

还建议使用作为卡斯基威胁情报门户解决方案的一部分的威胁查询服务来确定威胁的普及程度。如果IOC（哈希或URL）的普及程度较低，则可能将该威胁视为APT。

在SIEM中分析事件

本节介绍在SIEM系统中分析不同类型事件的推荐操作顺序。

对于所有事件的行动

当安全小组在SIEM系统中收到事件触发器时，必须按照建议的操作顺序进行操作：

1. 确定导致SIEM生成信息事件的触发事件(event)的原始事件(event)。这个事件有SIEM检测到的IOC。
 - 如果这个威胁是通过邮件附件发送的，检查组织的邮件服务器的日志文件。
 - 如果威胁时通过网络传送的，检查组织的代理服务器，防火墙，UTM网关或者其它提供网络访问设备的日志文件。
2. 确定目前的攻击阶段。这取决于检测到的IOC的类型。例如，如果检测到与C&C服务器的交互，则攻击处于命令和控制阶段。
3. 评估存储在潜在受损资产上的信息的重要性以及与事件有关的IOC的可靠性。根据这两个因素，调整事件的优先级。
4. 根据检测到的威胁的类型执行其余操作，如以下部分所述。

如果终端防病毒解决方案检测到威胁，则仅在以下情况下需要事件响应：

- 终端防病毒解决方案没有阻止威胁。
例如，如果员工已成功下载恶意软件。
- 威胁被阻止，但事件(event)多次发生。

例如，如果组织网络中的计算机持续尝试下载恶意软件，则计算机可能会受到终端防病毒解决方案未检测到的恶意软件的感染。

如果检测到具有威胁的URL

如果检测到威胁的URL，请根据URL的类别执行操作。括号中的值是卡巴斯基实验室的威胁情报中的类别。

- 如果检测到钓鱼网址（PHISHING类别）：

1. 检查该URL导致的网页的源代码。确定员工可能向攻击者提供哪些信息。
2. 在SIEM中，分析与被攻击的员工相关的事件(event)。对于员工访问网络钓鱼URL之后的10分钟前和10分钟内的时间，应该进行此操作。
 - 如果员工发送或下载了任何文件，对于这些文件中的哈希请执行以下子节“如果检测到威胁的哈希”中描述的操作。
 - 如果员工没有发送或下载文件，请通知员工事件。根据员工披露的信息价值，可能需要额外的行动。
3. 如果有可能员工的凭据受到攻击，请更改此员工的密码。

- 如果检测到恶意URL（MALICIOUS类别）：

1. 分析代理服务器事件(event)以确定是否下载了恶意软件。
 - 如果没有下载恶意软件，那么受影响的资产不会受到威胁。这样的事件(event)不是信息事件，不必进一步调查。确保恶意URL被列入黑名单。
 - 如果下载恶意软件，请继续进行调查。
2. 确定恶意软件是否被组织的代理服务器或防病毒解决方案等防御措施阻止。
 - 如果恶意软件被阻止，并且这是此类事件的首次发生，那么受影响的资产就不会受到威胁。这样的事件(event)不是信息事件，不需要进一步调查。
 - 如果恶意软件被阻止，这不是首次发生这种事件，请继续进行调查。
 - 如果恶意软件未被阻止，请继续进行调查。
3. 获取此URL导向的恶意软件的样本。如果URL是一个网页的链接，请检查网页的源代码以确定哪些样本可能从其中下载。
4. 分析恶意软件样本。

有关分析软件样本的更多信息，请参见“分析工具”节。
5. 确定下载的恶意软件是否已执行。

6. 扫描受感染的计算机检测到的威胁的IOC。扫描相同网段中的其他计算机，从而获取检测到威胁的IOC。

包括在调查这些扫描过程中获得的新IOC。例如，通过分析恶意软件样本，可以获得新的IOC。

7. 继续进入事件响应过程的遏制阶段。

- 如果检测到Botnet C&C URL（BOTNET C&C类别）：

1. 确定尝试与C&C服务器交互的软件并对其进行分析。

有关分析软件样本的更多信息，请参见“分析工具”节。

2. 扫描受感染的计算机的恶意软件。可能通过从C&C服务器接收的命令下载该软件。

3. 分析URL

有关分析URL的更多信息，请参见“分析工具”节。

4. 扫描受感染的计算机中来获取检测到的威胁的IOC。扫描相同网段中的其他计算机，从而获取检测到的威胁的IOC。

在这些扫描中，包括在调查过程中获得的新IOC。例如，可以从分析URL获取新的IOC。

5. 继续进入事件响应过程的遏制阶段。

如果检测到僵尸网络C&C URL，则攻击已达到命令和控制阶段。这次袭击是活跃的。

- 如果检测到移动僵尸网络C&C URL（MOBILE BOTNET C&C类别）：

1. 用移动防病毒解决方案扫描受感染的手机。

2. 继续进入事件响应过程的遏制阶段。

如果检测到威胁的哈希

如果检测到威胁的哈希，则根据哈希类别执行操作。括号中的值是卡斯基实验室的情报中的类别。

- 如果检测到恶意或bot散列（MALICIOUS和BOT类别）：

1. 分析该哈希所属的恶意软件。

有关分析软件样本的更多信息，请参见“分析工具”节。

2. 扫描受感染的计算机来获取检测到的威胁的IOC。扫描相同网段中的其他计算机，以获取检测到的威胁的IOC。

在这些扫描中，包括在调查过程中获得的新IOC。例如，可以从分析恶意软件获得新的IOC。

- 如果检测到移动恶意，漫游器或木马哈希（MOBILE MALICIOUS，MOBILE BOT和MOBILE TROJAN类别）：
- 用移动防病毒解决方案扫描受感染的手机。
- 继续进入事件响应过程的遏制阶段。

如果检测到具有威胁的IP地址

如果检测到威胁的IP地址，请根据IP地址的类别执行操作。以下类别是将SIEM事件(event)与卡斯基实验室的威胁馈送进行匹配的结果。

- 如果检测到Tor®退出节点IP地址（TOR EXIT NODE category）：
 1. 询问员工是否使用过Tor。
 - 如果员工确认他或她使用Tor，那么这样的事件(event)不是事件，不需要进一步调查。
 - 如果员工表示他或她没有使用Tor，请继续进行调查。
 2. 扫描可以使用Tor的软件受感染的计算机。这样的软件可能是合法的软件，或者它可能是使用Tor隐藏其活动的恶意软件。扫描同一网段中的其他计算机的恶意软件。
 3. 对于检测到的软件文件重复完整的识别过程。
- 如果检测到垃圾邮件IP地址（垃圾邮件类别）：
 1. 继续进行事件响应过程的教训阶段（第35页）。
- 如果检测到恶意软件IP地址（恶意软件类别）：
 1. 确定尝试与IP地址交互的软件，并对其进行分析。

有关分析软件样本的更多信息，请参见“分析工具”节。
 2. 执行上述“检测到威胁的URL地址”小节中描述的对于恶意URL的操作。

遏制

本节为事件响应过程的遏制阶段提供建议。

遏制阶段的目标

遏制阶段主要有两个目标：

- 在保持系统可操作性的同时隔离受损资产。

- 防止删除可能用于调查的IOC。

隔离受攻击的计算机

建议将受感染的计算机放入单独的隔离网络中。安全团队必须更改路由策略，以防止受感染的计算机与组织的网络和Internet中的其他计算机进行通信。

不建议关闭受感染的计算机。某些类型的恶意软件保留在内存中，并且不会在硬盘上创建文件。如果具有这种恶意软件的计算机被关闭，则该恶意软件的IOC将会丢失。当系统收到关机信号时，其他类型的恶意软件会删除其IOC。这将使调查更加困难。

也不建议禁用受感染计算机的本地网络连接或将其与网络物理断开连接。某些类型的恶意软件跟踪受感染计算机上本地网络连接的状态。如果连接已被禁用一段时间，恶意软件可能会开始删除其存在的迹象，从而销毁了IOC。

创建内存和硬盘转储

为了继续调查，安全团队必须从受感染的计算机获取内存和硬盘备份。这些备份包含恶意软件的所有组件。

通过分析受损计算机的内存和硬盘转储，安全团队可以获取与攻击相关的恶意软件和IOC的样本，并确定攻击方法。

该信息可用于防止相同类型的进一步攻击达到发送，开发或安装阶段。通过分析恶意软件的样本，安全团队可以找到有效的根除恶意软件的方法。

如果将内存和硬盘备份发送到安全团队是非常困难的，建议先发送内存备份。安全团队分析内存备份后，团队必须决定是否还需要硬盘备份。例如，如果组织有几个地理上分开的办公室，并且安全团队只在其中一个位置，则可能会出现这种情况。

有关创建内存和硬盘备份的推荐工具的更多信息，请参见“创建备份的工具”节。有关分析内存和硬盘备份的工具的更多信息，请参见“分析内存备份的工具”和“分析硬盘备份的工具”。

硬盘的完全备份总是占用硬盘上可用的全部硬盘空间。这是因为硬盘备份还包括来自硬盘空闲（未使用）扇区的信息。例如，如果硬盘的容量为400千兆字节（GB），并且使用了50 GB的硬盘空间，则该硬盘的备份将需要400 GB。

保持可操作性

在受攻击的计算机被隔离后，系统必须保持其可操作性。例如，如果组织网络中的多台服务器遭到入侵，则安全团队必须更改路由策略，以便其他服务器承担受感染服务器的负载。

根除

本节为事件响应过程的根除阶段提供了建议。

根除阶段有两种可能的策略：

- 受损资产的完全恢复

例如，可以从工作站映像恢复工作站。

该策略非常适合于为员工工作站使用标准软件的组织。如果受影响的资产是手机或其他硬件设备，则可以使用出厂设置。

- 检测恶意软件和删除其文件及其从受损资产创建的所有组件。

例如，由后门软件感染的工作站可以通过从硬盘中删除后门和由其创建的所有文件以及将系统注册表恢复到其原始状态来恢复。

可以通过使用“分析工具”节中描述的工具和实用程序分析恶意软件来检测恶意软件创建的组件。

恢复

本节为事件响应过程的恢复阶段提供建议。

在此阶段，以前受损资产已经投入使用。安全小组必须监测资产的状况一段时间，以确保威胁得到彻底消除。

例如，如果组织网络中的其中一个服务器已恢复，则安全团队将其重新安装到组织的网络中，调整路由策略以使用此服务器，并监视服务器的行为一段时间以确保没有可疑活动。

经验学习

本节为事件响应过程的经验教训阶段提供建议。

调查完成后，安全团队必须撰写报告。此报告必须包含以下问题的答案：

- 事件是何时被谁发现的？
- 事件的范围是什么？什么资产会受到此次事件的影响？
- 遏制，消除和恢复阶段如何进行？
- 事件响应过程的哪个阶段是安全团队最有效？
- 在事件响应的哪个阶段，安全小组的行动需要改进？

根据报告和调查情况，安全团队必须制定有助于防止今后发生事件的措施，更新这类事件的事故应急方案。

措施包括调整安全政策，改变组织资产配置，对公司员工进行信息安全培训。在事件响应过程中获得的IOC可以由安全小组使用，以便在将来发现其他类似的攻击。

事件响应计划必须包括一组书面指示，以便识别事件并作出响应。即使不可能在将来完全防止事件发生，事件响应计划也将有助于尽可能减少事件发现所需的时间，提高事件响应的有效性。

事件响应示例

本章提供了一个网络攻击的例子和安全小组进行的事件响应的例子。

攻击计划

本节提供了计划的网络攻击的示例。在这个例子中，犯罪者试图获得对银行ATM控制系统（ATM网关）的控制，以便从ATM终端提款。

攻击目标，载荷，漏洞利用和发送方式

袭击的目标是从ATM终端提款。当攻击者获得对ATM网关的控制并损害ATM终端时，实现目标。

这种攻击的载荷是加载软件。在它被发送后，装载程序软件将下载，安装和运行bot软件（如下所述）。之后，装载机软件将继续监控机器人软件。如果机器人软件被铲除，装载机软件将再次下载并安装。例如，端点防病毒解决方案可能会消除bot软件，但是加载程序软件会一次又一次的安装。

bot软件将允许攻击者通过从C&C服务器发送命令来远程控制受感染的计算机。机器人软件具有后门软件功能，允许攻击者控制受感染的计算机。

攻击者将使用备用软件窃取用户凭据。他或她选择mimikatz软件，这是可以用于此目的的合法软件。bot软件与C&C服务器建立连接后，bot软件将从C&C服务器提供的URL下载mimikatz软件。将在此次攻击中使用的最后一块软件是由攻击者开发的定制软件，以危及位于ATM网关后面的ATM终端。一旦攻击者获得对ATM网关的访问，该软件将被bot软件下载。

这种攻击的利用是包含加载程序软件的PDF文件。通过利用Adobe®Acrobat®Reader软件中的漏洞，漏洞利用将在打开文档时运行加载程序软件。

攻击者使用钓鱼来发送这些漏洞利用。漏洞利用将附加到发送给目标组织的员工的电子邮件中。

第一阶段：侦察

攻击者获取攻击ATM终端的方式的信息。为此，攻击者必须控制一个银行的ATM网关，这是一个受到重点保护的资产。

攻击者创建使用相同类型的ATM网关的银行列表。然后，攻击者收集有关每家银行采取的安全措施的信息。攻击者分析可用信息并选择目标。通过使用社会工程，攻击者获得银行雇员和企业电子邮件地址列表。

第二阶段：武器化

因为破坏银行安全边界是不太可能成功的，所以攻击者选择通过对组织的员工进行一次钓鱼。

攻击者通过上文“攻击目标，载荷，漏洞利用和发送方式”中描述的攻击目标，载荷，漏洞利用和发送方式。

第三阶段：发送

攻击者进行钓鱼攻击时。他或她通过社会工程获得的雇员名单向并且几名雇员发送电子邮件。攻击者根据他们基于员工的一些漏洞组织钓鱼。例如，财务部门的员工可能是这种攻击的有用目标。

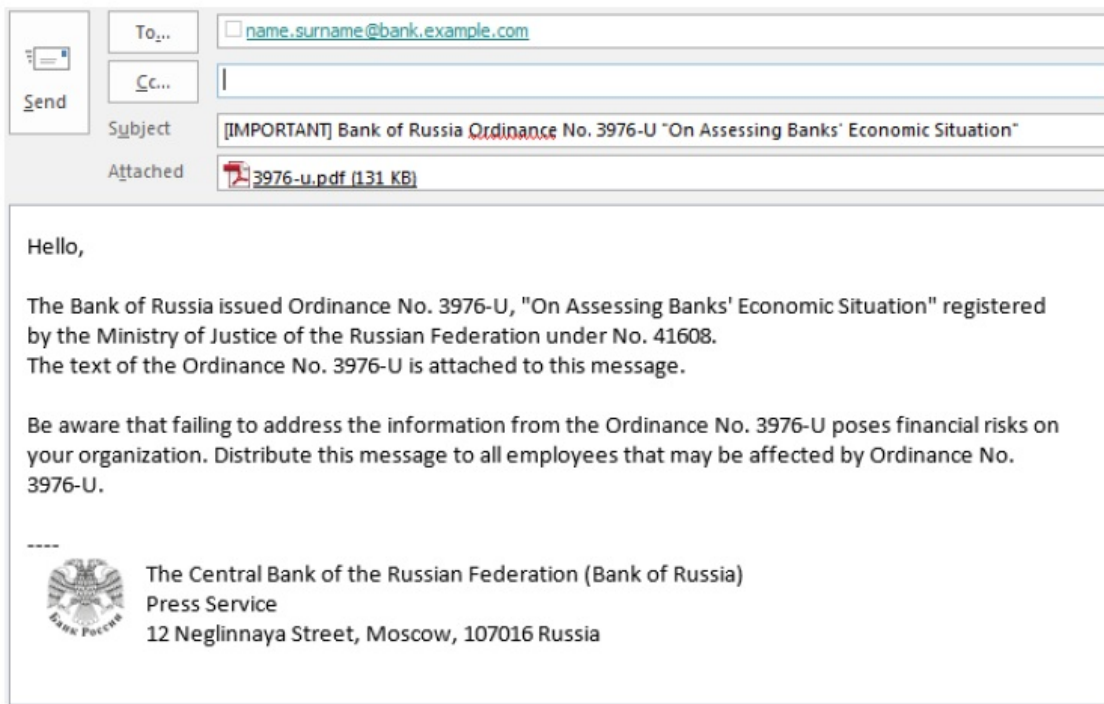


Figure 4: The spear phishing attack is conducted by means of email messages

电子邮件似乎来自该国的金融监管机构（俄罗斯央行）。这些电子邮件的文字是用来诱导雇员打开附件的PDF文件。

第四阶段：漏洞利用

雇员在Acrobat Reader中打开PDF文件后，将加载程序软件的文件复制到员工的计算机硬盘，并将加载程序软件添加到操作系统上的启动程序列表中。

第五阶段：安装

在受影响的计算机的下次启动时，操作系统将运行加载程序软件。加载软件将下载bot软件，安装它，并将其添加到启动程序列表中。完成这些操作后，加载程序软件将监控机器人软件的状态。如果系统中不存在bot软件，装载软件将重复安装步骤。

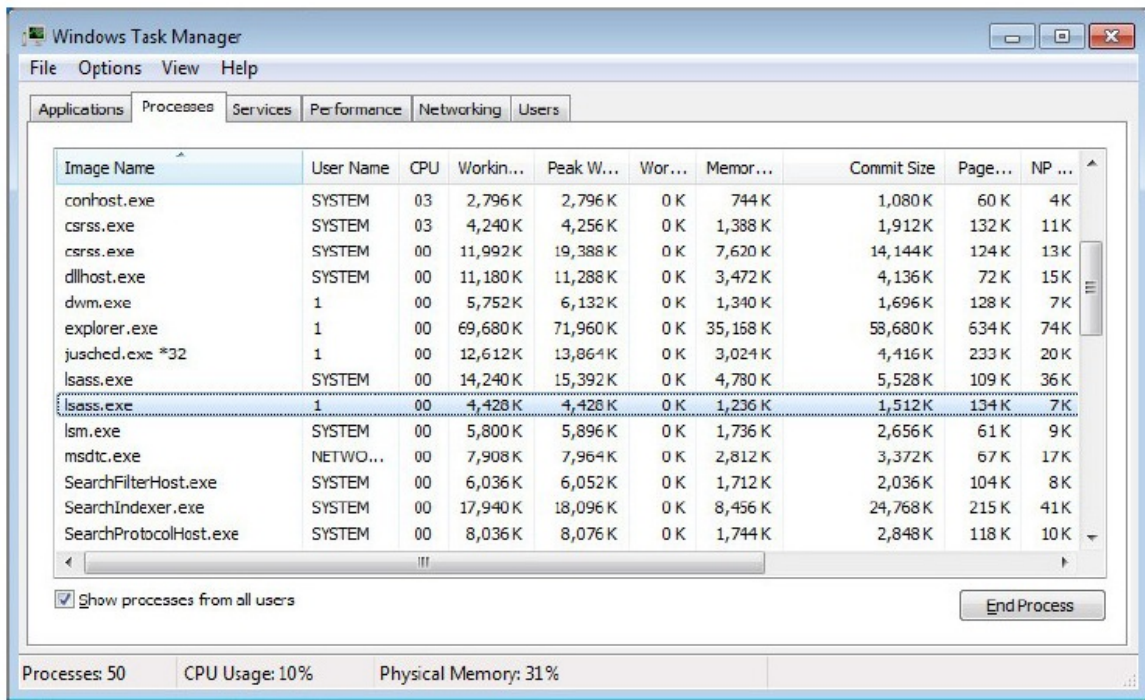


Figure 5: The bot software disguises itself as lsass.exe

bot软件试图通过伪装成已知的合法系统进程lsass.exe（本地安全认证服务器）来隐藏用户的存在。该软件始终存在于Windows操作系统上的进程列表中。

第六阶段：命令和控制

bot软件建立与攻击者控制的C&C服务器的连接。

第七阶段a：对于目标的操作（横向活动）

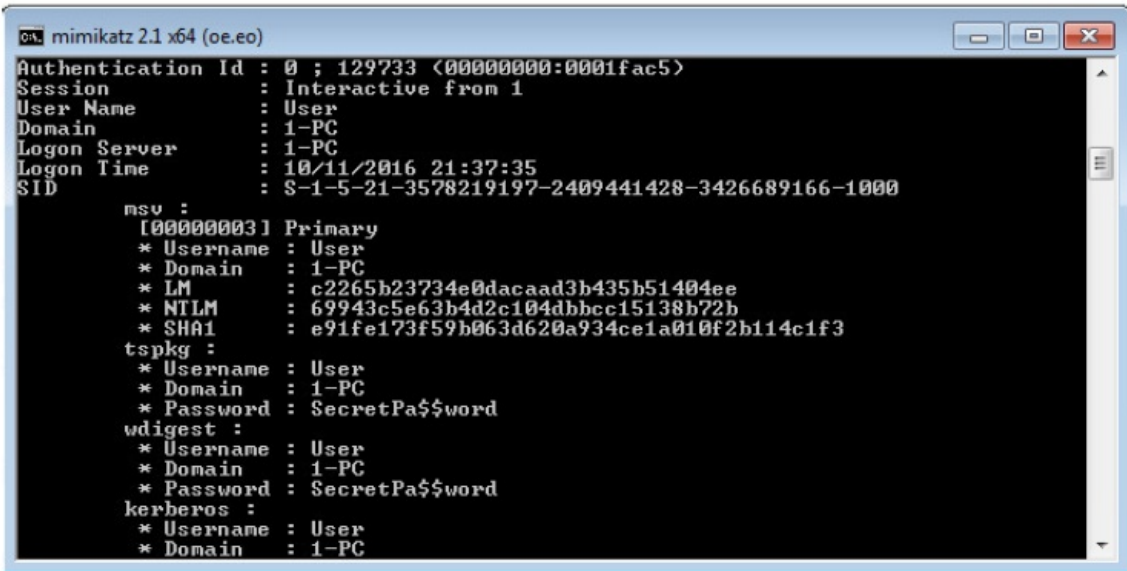
攻击者向bot软件提供的第一个命令是感染组织网络中的其他计算机。

僵尸软件使用受攻击的计算机的访问权限和用户权限以及已知的漏洞将漏洞利用到其他计算机。攻击者还可以选择受攻击组织内部使用的其他PDF文档。

此步骤的目标是危及上次操作系统启动后管理员帐户已登录的计算机。

第七阶段b：对于目标的操作（盗用凭据）

当一台计算机（管理员帐户登录后）被发现并遭到入侵时，机器人软件将下载mimikatz并运行它。



```

c:\mimikatz 2.1 x64 (oe.eo)
Authentication Id : 0 ; 129733 (00000000-0001fac5)
Session          : Interactive from 1
User Name        : User
Domain           : 1-PC
Logon Server     : 1-PC
Logon Time       : 10/11/2016 21:37:35
SID              : S-1-5-21-3578219197-2409441428-3426689166-1000

msv :
[00000003] Primary
* Username : User
* Domain   : 1-PC
* LM       : c2265b23734e0dacaad3b435b51404ee
* NTLM     : 69943c5e63b4d2c104dbbcc15138b72b
* SHA1     : e91fe173f59b063d620a934ce1a010f2b114c1f3

tspkg :
* Username : User
* Domain   : 1-PC
* Password : SecretPa$$word

wdigest :
* Username : User
* Domain   : 1-PC
* Password : SecretPa$$word

kerberos :
* Username : User
* Domain   : 1-PC

```

Figure 6: The mimikatz software is used by the attacker to steal user names and passwords

攻击者将使用mimikatz程序获取自上次操作系统启动以来在此计算机上登录的所有用户的用户名和密码（包括Microsoft®ActiveDirectory®用户凭据）。攻击者在此阶段的目标是获取Active Directory管理员帐户的密码。

第七阶段**c**：对于目标的操作（攻击ATM网关）

攻击者命令bot软件来访问ATM网关。bot软件使用前一阶段获得的管理员凭据来获取对ATM网关的控制。达成攻击目标。

当ATM网关受到控制时，bot软件下载并运行攻击者开发的定制软件来危及ATM终端。此操作可以成功，因为ATM网关不再阻止攻击者访问ATM终端。攻击者可以通过从C&C服务器进行控制，从受损的ATM终端提取资金。例如，攻击者可以模拟某个ATM终端的取款操作，并迫使终端分配现金托盘的内容。

第七阶段**d**：对于目标的操作（销毁证据）

达到攻击目标后，攻击者命令bot软件销毁任何攻击的证据。这个阶段的目标是推迟这次攻击的识别，使调查更加困难。bot软件将从受感染的计算机中删除自身，加载程序软件和mimikatz软件。bot软件还将尝试删除其创建的组件，例如受损的PDF文档。

事件响应

本节提供了对网络攻击的事件响应的示例。在这个例子中，受到攻击的银行的安全团队试图对抗攻击者试图获得对银行ATM控制系统（ATM网关）的控制。

准备（示例）

本节介绍银行为防范网络攻击而采取的防御措施。

银行的企业网络设计包含对于安全的考虑。

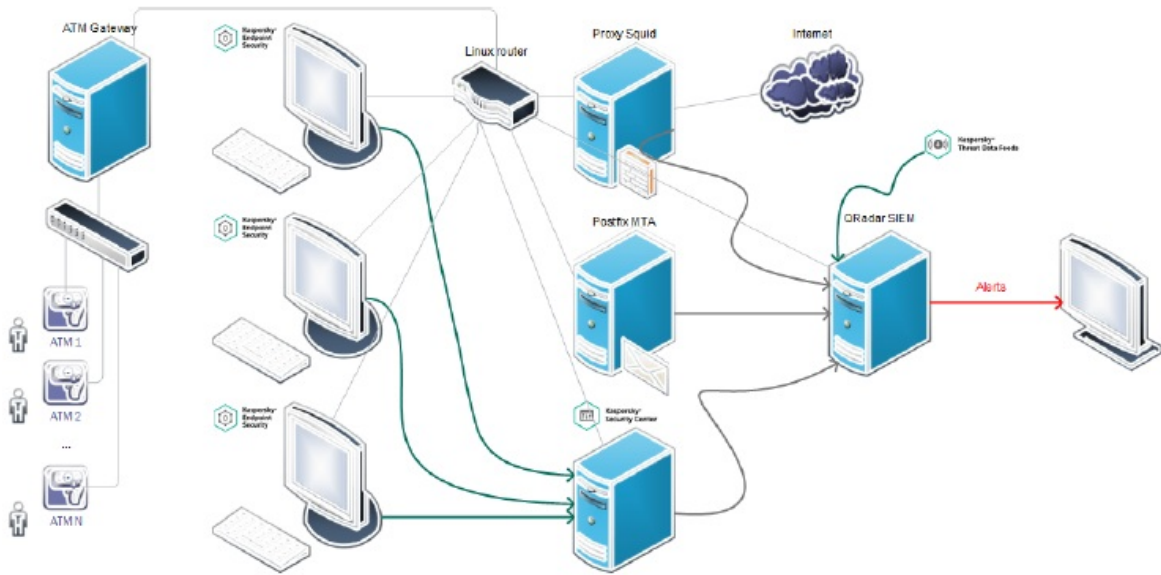


Figure 7: Corporate network of the bank

银行采取以下防御措施来打击网络攻击。该银行使用IBM®QRadar®SIEM系统跟踪事件。卡斯基实验室威胁情报集成在SIEM系统中。

- 来自组织网络的Internet访问只能通过Squid代理服务器进行访问。代理服务器配置为向SIEM系统发送事件(event)。
- 银行使用Postfix邮件传输代理(MTA)来传输组织的电子邮件。Postfix MTA还将事件(event)发送到SIEM系统。这些事件(event)具有来自电子邮件标题的信息，包括“已接收”标题。
- 由卡斯基安全中心控制的卡斯基端点安全保护银行网络中的所有工作站。卡斯基安全中心的所有警报都将发送到SIEM系统。
- 银行的路由器在Linux®操作系统上运行。ATM网关和ATM终端位于隔离网络中。只允许少数用户访问该网络。
- 该银行积极订阅卡斯基威胁情报门户解决方案。

识别（示例）

本节介绍事件响应示例的识别阶段。

可能会发生什么

由于银行使用SIEM系统，所有从员工计算机访问的URL和尝试与组织网络交互的所有IP地址与威胁情报相匹配。终端防病毒解决方案会扫描工作站上的所有下载文件。终端防病毒解决方案还将这些文件的哈希信息发送到SIEM系统，并将其与威胁情报进行匹配。

这次袭击可能会在以下阶段中被确认：

- 攻击者用来发送钓鱼邮件服务器的IP地址将与威胁情报中的IP信誉匹配。在这种情况下，攻击在发送阶段被识别。
- 下载僵尸软件请求将与恶意URL威胁情报匹配。在这种情况下，攻击在安装阶段被识别。
- 连接到C&C服务器的请求将与Botnet C&C URL威胁情报匹配。在这种情况下，攻击在命令和控制阶段被识别。
- mimikatz软件将被保护工作站的卡斯基端点安全解决方案检测和删除。在这种情况下，攻击是在对于目标操作的阶段中确定的。

攻击不太可能成功，因为防止攻击者在攻击生命周期（kill chain）中任何阶段执行来阻止攻击。

SIEM中监测到的Botnet C&C URL

为了这个例子的目的，假定攻击达到命令和控制阶段。

当安全团队的成员在SIEM系统中接收到事件触发时，IR过程的识别阶段开始。

Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP
KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2	1	Oct 13, 2016, 7:22:0...	Botnet Address	10.65.65.65
KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2	1	Oct 13, 2016, 7:21:5...	Botnet Address	10.65.65.65

Figure 8: Requests to the Botnet C&C URLs are detected in the SIEM system

在这种情况下，对C&C服务器的请求是从组织的网络进行的。安全团队的成员将此事件(event)分类为事件触发器，因为“事件响应指南”指出，这些事件(event)始终是事件触发器。

遏制（示例）

本节提供了进行事件响应过程的遏制阶段的示例。

识别受感染的计算机

对C&C服务器的请求是主动攻击的标志。在这种情况下，第一个优先事项是识别受感染的计算机，并将其隔离在不能访问组织的网络和Internet的单独网络中。

为了识别受感染的计算机，安全团队在SIEM系统中搜索与Botnet C&C URL的请求相关的所有事件(event)。组织网络中提出此类请求的所有网络计算机都受到影响。

如事件响应步骤部分所述，收集IOC是一个循环过程。在此示例的后面，安全团队使用卡斯基威胁情报门户解决方案的威胁查询服务分析 Botnet C&C URL。安全团队获得与此 Botnet URL相关的恶意软件的哈希。这些哈希是额外的IOC，可用于确定其他受感染的计算机。下一步是通过获取具有这些哈希的恶意软件访问的所有URL的列表来获取更多的IOC并识别更多受感染的计算机。这些额外的网址可能是其他恶意网址和Botnet C&C网址。

隔离受感染的计算机

安全团队使用组织路由器上的iptables程序隔离受感染的计算机。

例如，受感染的计算机的IP地址是192.168.0.3。在组织的路由器上执行以下命令可以防止受感染的计算机通过网络发送和接收任何数据：

```
iptables -A FORWARD -s 192.168.0.3 -j DROP
```

安全团队还将受感染计算机访问的Botnet C&C URL添加到黑名单中。如果组织网络中还有其他受损的计算机尚未识别，则无法与C&C服务器进行交互。

识别攻击方法

为了识别攻击方法，安全团队将分析与QRadar SIEM系统中受感染计算机相关的所有事件(event)。

	Event Name	Log Source
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
	KL_Malicious_URL	KL_Threat_Feed_Service_v2
	KL_Malicious_URL	KL_Threat_Feed_Service_v2
	KL_IP_Reputation	KL_Threat_Feed_Service_v2

Figure 9: All events that are related to compromised computers and that match threat feeds from Kaspersky Lab

在此示例中，最早的事件与IP信誉威胁情报(KL_IP_Reputation)的匹配。攻击者使用的钓鱼邮件邮件的服务头包含与卡巴斯基实验室威胁情报匹配的IP地址。IP信誉威胁情报包含与垃圾邮件和网络钓鱼攻击相关联的IP地址。这意味着攻击开始于向银行雇员发送电子邮件。

通常，与此IP地址的通信将被组织使用的防御措施之一所阻止，但为了本例的目的，假设对此事件没有反应。

进一步调查事件后，安全团队会发现攻击者发送的电子邮件。现在，安全团队可以分析这些电子邮件的附件，以调查攻击者使用的漏洞。此外，通过查找电子邮件的所有收件人，安全小组可能能够确定其他受到攻击的计算机（可能受到攻击的影响），并阻止员工激活漏洞。

分协议软件

在受攻击的计算机被隔离后，安全小组继续进行调查并分析受攻击的计算机。

安全团队可以使用卡巴斯基威胁情报门户解决方案的威胁查询服务获取与Botnet C&C URL地址相关的信息。这样的信息包括与该URL相关的恶意软件文件的散列以及与该URL相关的软件描述。

出于本例的目的，假定安全团队没有使用卡巴斯基威胁情报门户解决方案的威胁查询服务。相反，安全团队将尝试通过使用Microsoft Sysinternals和“Volatility 工具”中的“自动运行”实用程序分析受感染的计算机，获取攻击者使用的恶意软件的信息。

如果安全团队可以直接访问受感染的计算机，则安全团队的成员就可以运行Autoruns实用程序。

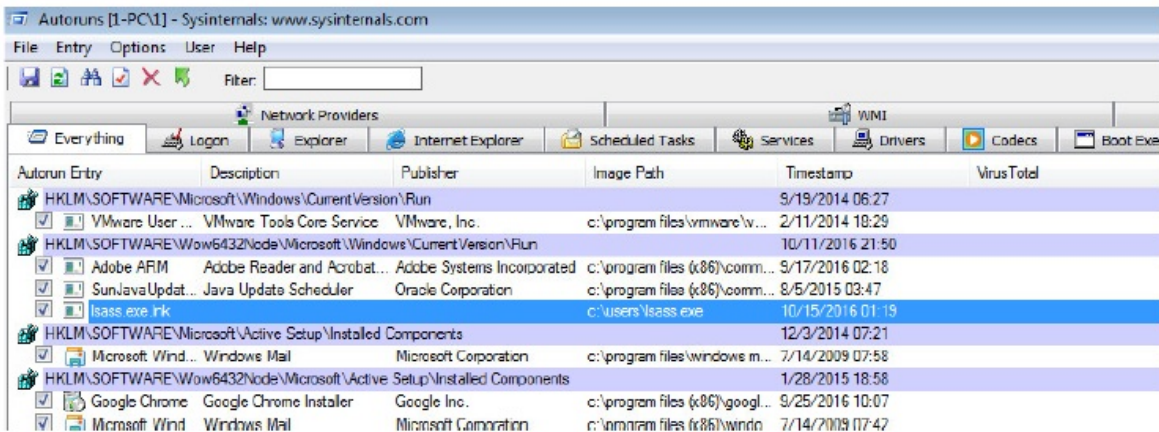


Figure 10: Analyzing startup programs with Autoruns

Autoruns工具可以帮助安全性成员检测位于c:\users目录中的可疑文件lsass.exe。在银行职员使用的标准工作站上，这种启动计划的存在是不太可能的。如果安全团队无法直接访问受感染的计算机，那么有权访问的员工将遵循安全团队的指示来创建受感染计算机的内存转储并将其发送给团队。AccessData取证工具包用于创建内存转储。

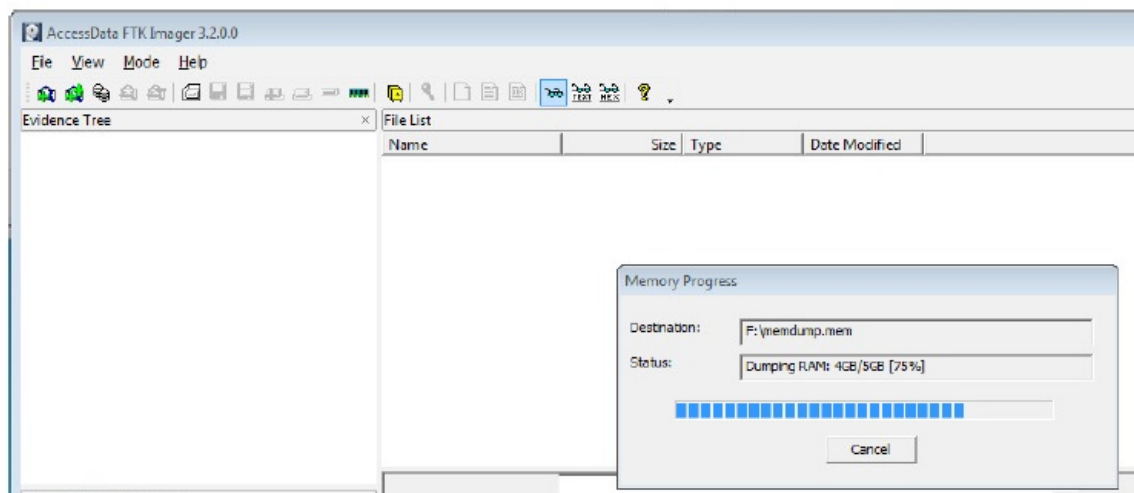


Figure 11: Creating a memory dump of the compromised computer with the FTK Imager utility

在安全团队获取内存转储后，安全团队的成员使用Volatility工具获取受感染计算机上的进程列表。

```
C:\Users\User\volatility_2.5>volatility.exe pslist -f C:\Users\User\Memdump\1-PC.mem
--profile=Win7SP0x64

Volatility Foundation Volatility Framework 2.5

Offset (V)          Name                      PID  PPID  Thds  Hnds  Sess
-----
0xffffffff8003c6c890 System                    4    0    96   2276  -----
0xffffffff8004400950 smss.exe                 264   4     2    29  -----
0xffffffff80048e3b30 csrss.exe                352  344    9   620    0
0xffffffff8004b57420 wininit.exe              404  344    3    76    0
0xffffffff8004b45b30 csrss.exe                412  396   10   280    1
0xffffffff8004b7a6a0 winlogon.exe             448  396    3   108    1
0xffffffff8004bcc2e0 services.exe              508  404    7   224    0
```

Volatility 工具输出显示两个lsass.exe进程。具有PID 516的lsass.exe进程具有PPID 404（父PID），这意味着它由wininit.exe进程（PID 404）启动。具有PID 2336的其他lsass.exe进程具有PPID 1976，这意味着它由explorer.exe进程启动（PID 1976）。第二个lsass.exe进程是高度可疑的，因为explorer.exe进程是Windows资源管理器的一部分，它不用于运行系统进程，如lsass.exe。

一旦识别出恶意软件（lsass.exe），安全团队必须确保该软件确实用于向C&C服务器发出请求。安全团队的成员对恶意软件执行静态分析。他或她使用Strings工具集搜索lsass.exe文件的C&C服务器URL。

其中一个Strings工具集参数定义了符号的长度。安全团队的成员使用该参数的不同值扫描lsass.exe文件，以从文件中获取ASCII和Unicode字符串。

通过使用具有默认参数的Strings工具集，安全团队的成员获得以下输出（片段）：

```
$ strings -a 'lsass.exe'

f:\dd\vctools\crt\crtw32\dllstuff\atosexit.c

>"g/

BSJB

v4.0.30319

#Strings

#GUID

#Blob

~,#
```

然后安全性团队成员搜索Unicode字符串，用-e l参数指定16位字符串。输出结果如下（fragment）：

```
$ strings -a -e l 'lsass.exe'

*.msg

__native_startup_state == __initialized

_controlfp_s(((void *)0), 0x00010000, 0x00030000)

http://subbotnet-domain_19.botnet-domain.example.com/page/c

find_proxy

{0}: {1}

--- Start of primary exception ---
```

http://subbotnet-domain_19.botnet-domain.example.com/page/c是由SIEM系统检测到的Botnet C&C URL。

分析恶意软件的最后一步是将样本发送给防病毒软件公司。在这个例子中，安全团队将恶意软件样本发送到卡巴斯基实验室。

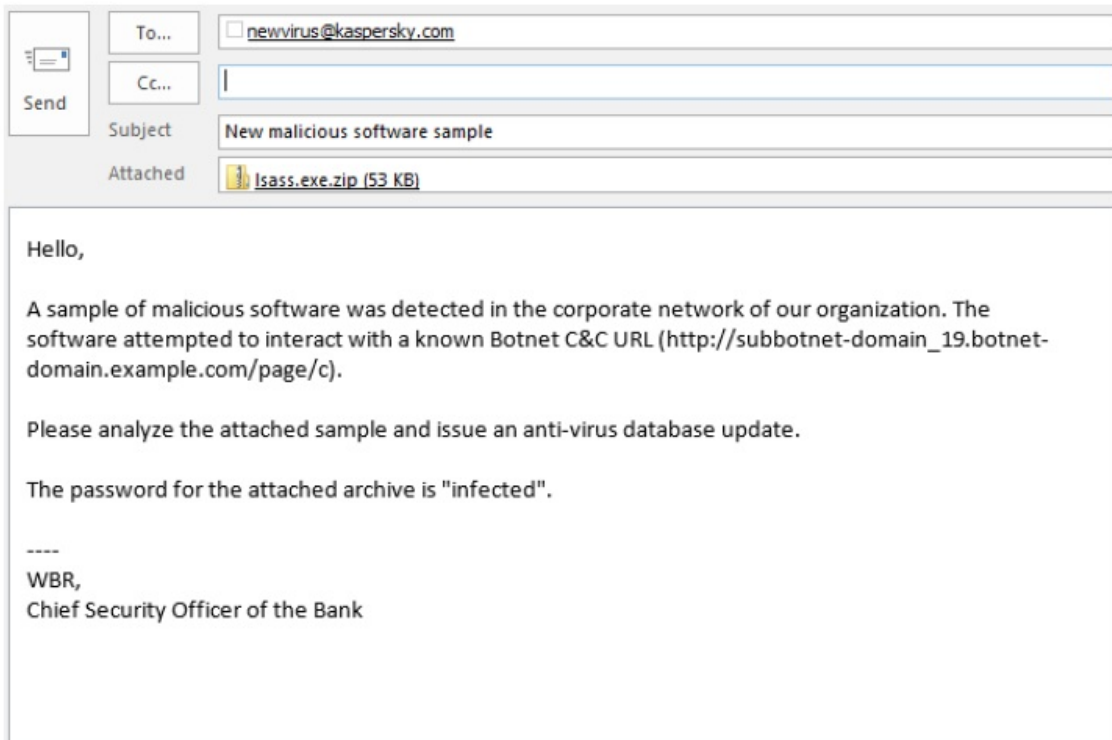


Figure 12: Sending the malicious software sample to Kaspersky Lab

卡巴斯基实验室专家将分析收到的样本，并且在终端点防病毒解决方案的数据库对此进行更新。这将有助于保护其他计算机免受此软件的影响。

动态分析利用和载荷

安全团队在检测到利用的时候还必须分析攻击方法。

安全团队从攻击者使用的电子邮件分析附件。安全团队的成员使用卡巴斯基威胁情报门户解决方案的沙箱服务（第60页）执行利用漏洞的动态分析。作为替代，他或她可以使用隔离的虚拟机来执行动态分析。

漏洞的动态分析有助于确定漏洞的行为。漏洞利用程序安装加载程序软件，并尝试下载恶意软件。

安全团队还可以分析漏洞利用下载的恶意软件。该分析将确认恶意软件尝试访问C&C服务器。

结果

通过隔离受攻击的计算机，安全团队能够阻止攻击。进一步分析受攻击的计算机和恶意软件有助于安全小组重建攻击计划：

- 攻击是通过钓鱼邮件进行的。
- 漏洞利用是通过安装加载软件危及计算机的PDF文档。
- 装载程序软件尝试下载僵尸软件。
- 恶意软件尝试向C&C服务器发出请求。这些请求被安全团队检测到，C&C服务器URL被列入黑名单。

结果，这次攻击已经停止而不会造成任何破坏。银行管理层决定没有必要通知执法部门关于这次攻击。安全小组继续进行根除阶段。

根除和恢复（示例）

本节提供了事件响应过程的根除和恢复阶段的示例。

安全团队从受感染的计算机中删除恶意软件。扫描组织网络中的所有计算机，以便安全小组检测到IOC。该扫描显示没有额外的受感染计算机。

组织的路由器被重新配置为允许先前受到感染的计算机从银行的网络和从互联网发送和接收数据。

例如，要将IP地址为192.168.0.3的受感染计算机返回组织的网络，可以执行以下命令：

```
iptables -D FORWARD -s 192.168.0.3 -j DROP
```

经验学习（示例）

安全小组撰写有关事件的报告。在事件响应过程（IP地址，URL，哈希）过程中获得的所有IOC都被放在组织使用的安全控制的黑名单上。安全团队会对银行员工对于处理不信任来源的电子邮件时进行有关安全实践的培训。

推荐的工具和程序

本章提供了可用于事件响应的工具和程序的说明。

本章中描述的工具和工程序不构成可用于事件响应的完整软件列表。根据事件，其他软件也可能用于进行调查。

本章中描述的工具和程序由第三方公司开发。卡斯基实验室不对第三方软件的可操作性或质量负责。在第三方公司的网站上提供了对工具和实用程序的完整描述。

收集IOC工具

本节提供了用于收集IOC的工具和实用程序的说明。

Sysinternals 工具集

Sysinternals是一组用于管理和监视运行Microsoft Windows的计算机的工具。Sysinternals套件包括60多个实用程序。

建议使用Sysinternals实用程序来收集IOC并分析受感染的计算机。可用于事件响应的最重要的Sysinternals 工具集将在以下小节中介绍。

Sysinternals 工具集可以从 <https://technet.microsoft.com/en-us/sysinternals/default.aspx> 下载。

PsTools

PsTools是一组命令行实用程序，可用于远程执行进程(PsExec)，列出有关进程(PsList)的详细信息，通过名称或进程ID(PsKill)来杀掉进程，以及查看和控制服务(PsService)。PsTools还包括重新启动和关闭计算机，转储系统事件日志记录和许多其他任务的工具集。

Process Monitor

Process Explorer是一个用于控制进程并获取有关进程活动的实时信息的工具。

Process Explorer允许您执行以下操作：

- 获取有关所有当前活动进程的详细信息。
- 杀死，暂停和恢复进程的执行。
- 获取有关进程打开或加载的句柄和动态链接库(DLL)的信息。
- 创建内存转储并将其保存到文件。

Autoruns

Autoruns实用程序显示哪些程序配置为在系统启动或登录时运行，并且启动各种内置Windows应用程序（如Internet Explorer®，Windows资源管理器和媒体播放器）时。该实用程序还启用或禁用这些程序的自动执行。

该实用程序支持使用VirusTotal检查自动运行对象的散列。未知文件可以发送到防病毒软件公司进行分析。

AVZ

AVZ实用程序可用于分析和恢复。

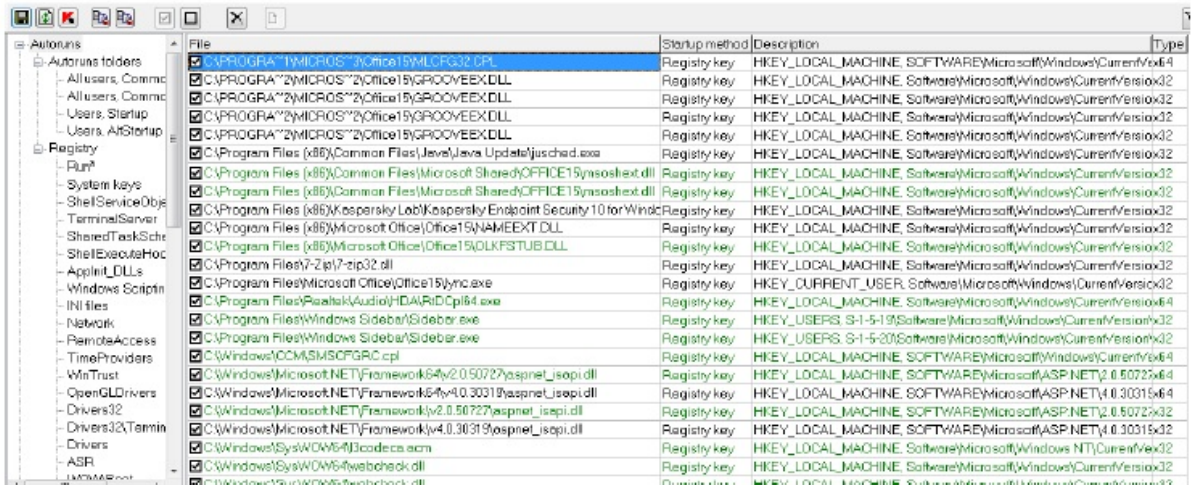


Figure 13: Autorun manager of the AVZ utility

建议在事件响应期间使用AVZ实用程序获取信息。该实用程序具有以下模块：

- 进程管理
- 服务和驱动管理器
- 内核空间模块
- Winsock SPI (LSP, NSP, TSP) 管理器
- 分析开放的TCP和UDP端口
- Autoruns 管理器
- Internet Explorer 拓展管理器
- Windows Explorer 拓展管理器
- Microsoft Windows Control Panel (CPL) applets 管理器
- 打印系统拓展管理器
- 任务调度作业管理器
- 被注入的DLLs管理器
- 协议和句柄管理器
- Windows Active Setup 管理器
- Hosts file 管理器
- 共享资源和网络会话管理器

AVZ实用程序可从 <http://www.z-oleg.com/secur/avz/download.php> 下载。

GMER

GMER是一个检测和删除rootkit的实用程序。

它扫描：

- 隐藏的进程
- 隐藏的线程
- 隐藏的模块
- 隐藏的服务
- 隐藏的文件
- 隐藏磁盘扇区（MBR）
- 隐藏的注册表项
- 内核模式驱动程序挂接

GMER实用程序可从 <http://www.gmer.net> 下载。

YARA

YARA是一种工具，旨在帮助恶意软件研究人员识别和分类恶意软件样本。YARA是一种多平台解决方案，可在Windows，Linux和Apple®Mac®OSX®上运行。它可以通过其命令行界面或使用yara-python扩展名的Python脚本来使用。

使用YARA，恶意软件研究人员可以根据文本或二进制模式创建恶意软件的描述。每个描述（也称为规则）由一组字符串和一个布尔表达式组成，用于确定其逻辑。

以下是YARA规则的示例，任何包含三个字符串之一的文件必须报告为威胁。

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true
        strings:
            $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
            $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
            $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
        condition:
            $a or $b or $c
}
```

YARA实用程序可从<http://virustotal.github.io/yara>下载。

创建转储的工具

本节介绍用于创建内存和硬盘转储的工具和实用程序。

GRR快速响应

GRR快速反应是一个专注于远程实时取证的事件响应框架。

GRR使用客户端 - 服务器架构。客户端应用程序（代理）安装在工作站上，用于收集数据。服务器应用程序用于存储和分析收集的数据。

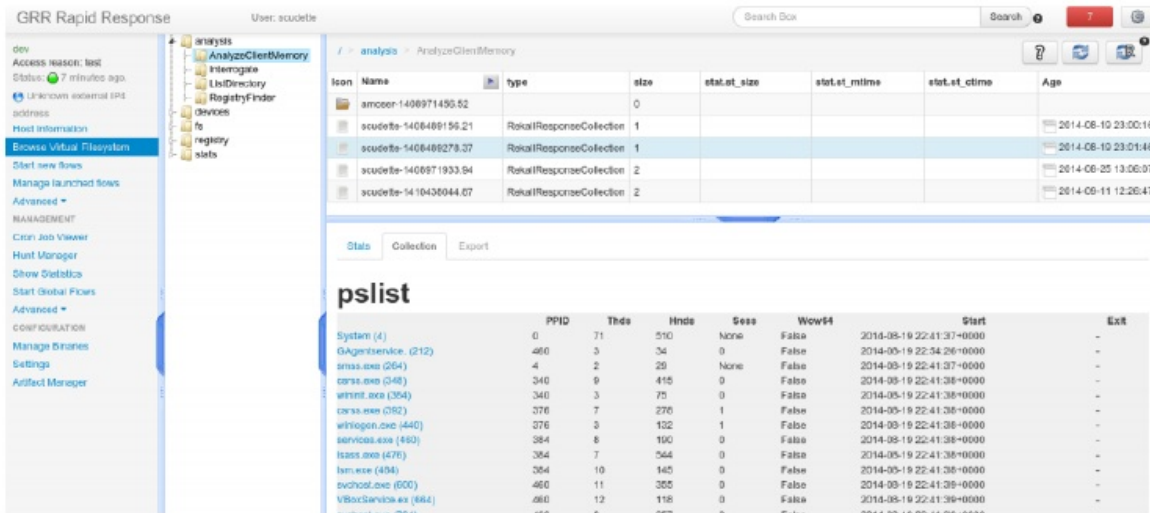


Figure 14: GRR Rapid Response

GRR的主要特性：

- 使用Rekall实用程序远程分析Windows操作系统上的内存和系统注册表。
- 使用The Sleuth Kit远程分析硬盘空间。

GRR Rapid Response可从<https://github.com/google/grr>下载。

Forensic Toolkit

取证工具包（FTK）是一套用于数字取证的实用工具。取证工具包包括FTK Imager实用程序，可用于创建硬盘和内存转储。

FTK支持查看硬盘转储的几个选项。例如，有一个名为“电子表格”的选项，其中显示了所有电子表格文件的列表，以及每个电子表格的详细说明和位置。FTK具有可用于搜索IOC的关键词列表。

FTK可从<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk?/solutions/digital-forensics/ftk>下载。

dd utility

dd（数据集定义）工具是用于Unix和类Unix操作系统的命令行实用程序，其主要目的是转换和复制文件。

该实用程序可用于复制硬盘的扇区，包括操作系统未使用的扇区。例如，您可以使用dd实用程序制作硬盘引导扇区的备份副本。

所有主要的Linux系统发行版都提供了dd实用程序。dd实用程序作为Cygwin的一部分移植到Microsoft Windows。它可以从<https://cygwin.com>下载。

Belkasoft RAM Capturer

Belkasoft RAM Capturer是在运行Microsoft Windows的计算机上创建内存转储的免费取证工具。创建的内存转储将保存到文件。

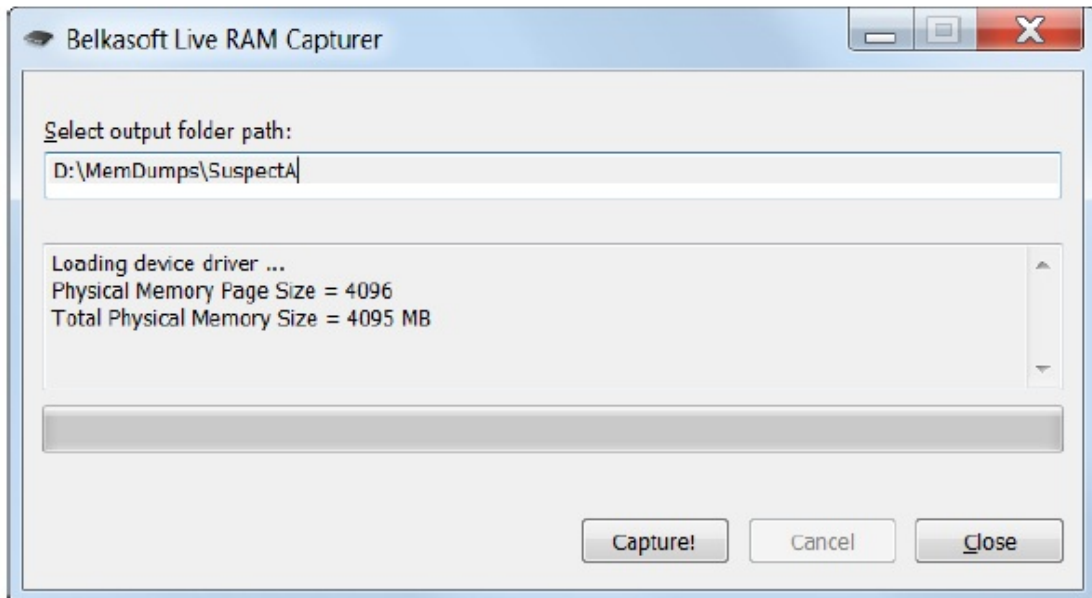


Figure 15: Belkasoft RAM Capturer

Belkasoft RAM Capturer具有32位和64位版本的Windows的独立模块。这些模块在内核模式下工作，并允许捕获受保护进程使用的内存区域。

Belkasoft RAM Capturer可以从 <http://belkasoft.com/ram-capturer> 下载。

分析工具

本节提供用于分析潜在威胁和软件样本的工具和实用程序的说明。

威胁分析需要大量的专业知识和实践。建议使用本节中描述的工具进行初步分析。但是，如果有可能发生APT攻击，最好让专家进行分析。

卡巴斯基威胁情报门户

卡巴斯基威胁情报门户是一个集合了几个卡巴斯基实验室服务的解决方案：

- 威胁查询

卡巴斯基威胁查询提供卡巴斯基实验室收集的关于网络威胁及其关系的所有知识，汇集成一个强大的服务。目标是为安全团队提供尽可能多的数据，防止网络攻击在影响组织之前。该服务检索关于URL，域，IP地址，哈希，威胁名称，统计和行为数据，WHOIS

数据和DNS数据的最新详细的威胁情报。结果是全球可见的新兴和新兴威胁，有助于提高事件响应的有效性和组织的保护再次攻击。

- whois追踪

此服务通过特定的WHOIS数据搜索条件查找域和IP地址。此类标准可能是域名联系人，域名创建日期。可以提交WHOIS数据的特定领域，以便定期和自动搜索符合指定标准的记录。关于WHOIS数据库中符合搜索条件的新记录的电子邮件通知可以自动发送到指定的收件人列表。

- APT报告

这项服务有助于通过卡巴斯基实验室的全面，实用的报告来提高对于高级的网络间谍活动的意识和知识。

- 数据情报（来自卡巴斯基实验室的威胁资讯提供）

卡巴斯基实验室提供不断更新的威胁智能数据情报，以向组织和客户通报与网络威胁相关的风险和影响，有助于更有效地减轻威胁，并在发起攻击之前防御攻击。数据情报可以使用JSON，CSV，OpenIOC和STIX™格式，并提供有SIEM的连接器，包括Splunk，HPE ArcSight，IBM QRadar，EMC®RSA®NetWitness®，LogRhythm®和McAfee®Enterprise Security Manager（ESM）。

- 沙箱

该服务是一种创新和全自动的文件分析系统，用于检测未知和高级威胁。它允许将文件提交到安全的环境中进行深入的动态分析，并接收全面的文件活动日志以供进一步调查。该技术的优点不仅是分析休眠代码和创新的方法来解决不同的逃避技术，而且还包括SOC，CERT和DFIR团队使用直观的报告来提高事件响应。

威胁查询

威胁查询是卡巴斯基威胁情报门户解决方案的一部分。它提供有关网络威胁的威胁情报，网络威胁，合法对象以及富含语境的IOC之间的互连。

Kaspersky Threat Intelligence Portal

THREAT LOOKUP WHOIS TRACKING Help

NEW REQUEST Hash report for Md5

1099BC917960DB1DD980757...

Malware Copy link Get full archive

HITS	FORMAT	SHA1	SHA256	CATEGORY
~ 10	None	9AAB800FD5D92FD15F 0A18346EB0A58C5EF4 32CA	25B81D5D3157B82BE 7C3F871A96CED0C184 485FB20BE7A9C11CDC F08DEE58E85	
FIRST Aug 29, 2016	SIZE 68,236 B	SIGNED BY None		
LAST Aug 29, 2016	PACKED BY None			

Detection names ? Get archive

HEUR:Trojan.Script.Generic
Aug 29, 2016 14:45

Figure 16: Threat Lookup — Kaspersky Threat Intelligence Portal

威胁查询服务允许您执行以下操作：

- 通过为安全团队提供关于威胁的有意义的信息，以及对目标攻击背后的原因进行全球洞察，改进和加速事件响应和取证能力。可以更有效，高效地诊断和分析安全事件。
- 对IOC进行深入的搜索，例如IP地址，恶意URL或具有人为验证的威胁上下文的文件散列，从而允许攻击的优先级，并帮助IT人员和资源分配决策。
- 通过适应防御性策略来抵御有针对性的攻击，增强战术和战略威胁情报的安全基础设施。
- 通过使用威胁查询，安全团队可以获取有关IOC之间关系的信息。此信息可用于检测攻击时安全控制未知的威胁。例如，可以检测到未知的恶意软件，因为它与已知的C&C服务器URL进行交互。

沙箱

卡斯基威胁情报门户（TIP）解决方案提供了在沙箱环境中对威胁和软件样本进行动态分析的功能。因此，可以检测威胁，生成有关其行为的报告，并获得有关事件报告的新IOC。

可以通过将文件，直接URL或对象的散列传递给卡斯基威胁情报门户（TIP）解决方案在TIP沙箱中分析软件样本。分析产生行为报告和有关与分析样本有关的工件的信息。此类信息包括PCAP文件，其中包含有关由样本修改或创建的分析样本和文件对象的网络活动的信息。

APT报告

卡斯基实验室的APT报告可用于对高级持续威胁（APT）的主动防御。

订阅APT报告可以持续访问卡巴斯基实验室的调查和发现，包括各种格式（包括YARA和OpenIOC格式）的每个APT的完整技术数据。

访问卡巴斯基威胁情报门户

要访问卡巴斯基威胁情报门户解决方案，请联系intelligence@kaspersky.com或访问<http://www.kaspersky.com/enterprise-security/intelligence-services>。

分析内存转储的工具

本节介绍可用于分析内存转储的Volatility和Rekall实用程序。

Volatility

Volatility Framework是从RAM样本中提取数字组件的内存取证框架。该实用程序具有在Linux，Windows和Mac OS X操作系统上进行内存转储的配置文件。

Volatility 支持以下转储类型：

- Raw / padded physical memory
- FireWire® (IEEE 1394)
- Expert Witness (EWF)
- 32-bit and 64-bit Windows Crash Dump
- 32-bit and 64-bit Windows Hibernation
- 32-bit and 64-bit Mach-O files
- Virtualbox Core Dumps
- VMware™ Saved State (.vmss) and Snapshot (.vmsn)
- HPAK format (FastDump)
- LiME (Linux Memory Extractor)
- QEMU VM memory dumps

Volatility Framework的发行套件有大约150个插件。通过使用这些插件，安全团队可以获取有关进程加载的进程调用树和DLL的信息。例如，`devicetree`插件可用于获取与这些设备相关联的所有设备和驱动程序的列表。该列表可用于搜索rootkit使用的驱动程序。

以下示例演示如何使用Volatility获取加载的DLL模块的列表。

```
$ python vol.py -f stuxnet.vmem --profile=WinXPSP2x86 dlldump -memory -D stuxout/
Volatility Foundation Volatility Framework 2.5
Process(V) Name          Module Base Module Name  Result
-----
0x820df020 smss.exe      0x048580000 smss.exe    OK: module.376.22df020.48580000.dll
0x821a2da0 csrss.exe    0x075b40000 CSRSRV.dll  OK: module.600.23a2da0.75b40000.dll
0x821a2da0 csrss.exe    0x077f10000 GDI32.dll   Error: DllBase is paged
0x821a2da0 csrss.exe    0x075b60000 winsrv.dll  OK: module.600.23a2da0.75b60000.dll
0x81da5650 winlogon.exe 0x001000000 winlogon.exe OK: module.624.1fa5650.10000000.dll
```

Volatility工具可以将进程从内存转储保存到可执行文件中。这些文件可以静态或动态分析。例如，可以使用沙盒卡巴斯基威胁智能门户解决方案进行动态分析；可以使用Strings实用程序执行静态分析。

Volatility框架可以从<http://www.volatilityfoundation.org>下载。

Rekall

Rekall是一个内存分析框架。

Rekall有三个接口：基于IPython的命令行，交互式控制台和Web界面。像Volatility一样，Rekall有大量的插件。例如，pslist插件可以输出系统上运行的所有进程的列表；hooks_inline插件可以搜索具有挂钩（拦截的函数调用）的所有库。可以使用Rekall附带的winpmem utility创建Windows操作系统上的内存转储。

Rekall允许在运行的操作系统上分析内存转储和内存。这意味着Rekall在不创建内存转储来进行分析。

以下示例演示如何使用Rekall分析内存转储。

```
user@computer:~/rekall$ rekall -f ~/images/win7.elf

-----

The Rekall

Memory Forensic framework 1.1.0 beta (Buchenegg).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.

-----

win7.elf 12 47 07> pslist

-----> pslist()

  _EPROCESS   Name      PIO PPID Thds Hnds Sess Wow64 Start
-----
0xfa80008959e0 System 4      0  84  511 -   False 2012-10-01 21:39:51+0000

[1] zeus.vmem 00:10:03> hooks_inline proc_regex="services"

-----> hooks_inline(proc_regex="services")

Pid Proc          DLL          Name          Hook          Disassembly
-----
676 services.exe ntdll.dll NtCreateThread 0x7e3b47 0x7c90d7d2 e97063ed83 jmp..
                                         0x7c90d7d7 ba0003fe7f mov..
                                         0x7c90d7dc ff12      call.
                                         0x7c90d7de C22000   ret..
                                         0x7c90d7e1 90       nop
                                         0x7c90d7e6 90       nop
                                         0x7c90d7e7 b836000000 mov..
```

Rekall可从<http://www.rekall-forensic.com>下载。

分析硬盘转储工具

本节介绍可用于分析硬盘转储的Sleuth Kit (TSK) 和RegRipper工具。

The Sleuth Kit (TSK)

Sleuth Kit (TSK) 是一组命令行工具和一个C库，可以分析硬盘转储并从中恢复文件。

TSK附带的命令行工具可以完成以下：

- 列出分配和删除的ASCII和Unicode文件名。
- 显示所有Windows NT文件系统属性的详细信息和内容。
- 显示文件系统和元数据结构的详细信息。
- 创建文件活动的时间线，可以导入到电子表格中以创建图形和报告。
- 在哈希数据库中查找文件哈希值。
- 根据文件类型整理文件。缩略图页面可以由图形图像进行快速分析。

Autopsy是针对The Sleuth Kit的基于GUI的程序。它为TSK实用程序提供GUI。

Sleuth Kit可从<http://www.sleuthkit.org/sleuthkit/>下载。Autopsy可从<http://www.sleuthkit.org/autopsy/>下载。

RegRipper

RegRipper是注册表分析的取证工具。

RegRipper可用于从硬盘转储中提取特定的注册表项，值和数据。RegRipper的分发包含大约300个插件。

以下示例演示了RegRipper的使用信息。

```
C:\RR>rip.exe
Rip v.2.8_20130801 - CLI RegRipper tool
Rip [-r Reg hive file] [-f plugin file] [-p plugin module] [-l] [-h]
Parse Windows Registry files, using either a single module, or a plugins file.

-r Reg hive file...Registry hive file to parse
-g .....Guess the hive file (experimental)
-f [profile].....use the plugin file (default: plugins\plugins)
-p plugin module...use only this module
-l .....list all plugins
-c .....Output list in CSV format (use with -l)
-s system name.....Server name (TLN support)
-u username.....User name (TLN support)
-h.....Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
C:\>rip -r c:\case\ntuser.dat -p userassist
C:\>rip -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.
```

RegRipper可从<https://github.com/keydet89/RegRipper2.8>下载。

字符串实用工具

字符串是用于Unix和类Unix操作系统的命令行实用程序，可用于在二进制文件中搜索Unicode和ASCII字符串。这样的字符串可以用作IOC或静态分析软件样本行为。

该实用程序可以在转储文件中搜索字符串，以获取有关开发分析样本，URL，IP地址，电子邮件地址和分析样本和其他IOC访问的注册表项中使用的软件的信息。

Strings实用程序作为Cygwin的一部分移植到Microsoft Windows。它可以从<https://cygwin.com>下载。

根除工具

本节提供了用于事件响应过程的根除阶段的工具和实用程序的说明。

卡巴斯基病毒删除工具

卡巴斯基病毒删除工具是一个免费的解决方案，可用于扫描恶意软件和消毒运行Microsoft Windows的计算机。该工具可以从命令行工作。

卡巴斯基病毒删除工具可以：

- 检测和根除恶意软件。
- 检测广告软件和其他合法的软件，可以被罪犯用来伤害计算机或窃取敏感数据。

该实用程序不是为持久保护而设计的。卡巴斯基病毒删除工具不会更新其防病毒数据库。必须下载新版本的卡巴斯基病毒删除工具才能使用最新的数据库。

卡巴斯基病毒删除工具用于对受感染的计算机进行消毒后，必须安装终端防病毒解决方案（如卡巴斯基端点安全）以实现持久保护。

卡巴斯基病毒删除工具可以从 <https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool> 下载。

可以从 http://support.kaspersky.com/viruses/utility?CID=acq-freekasp-USA&_ga=1.198229483.571661967.1434556259 获得用于消除几种恶意软件的其他免费工具。

卡巴斯基拯救盘

卡巴斯基拯救盘旨在扫描，消毒和恢复受感染的操作系统。当无法启动操作系统时可以使用它。

卡巴斯基拯救盘可以有效地消除恶意软件，因为操作系统未启动，恶意软件无法控制系统。

卡巴斯基拯救盘可从<https://support.kaspersky.com/viruses/rescuedisk>下载。

卡巴斯基实验室

卡巴斯基实验室是世界知名的系统供应商，可以保护计算机免受数字威胁，包括病毒和其他恶意软件，未经请求的电子邮件（垃圾邮件）以及网络和黑客攻击。

2008年，卡巴斯基实验室被评为世界四大领先的最终用户信息安全软件解决方案供应商（IDC全球终端安全收入供应商）。卡巴斯基实验室是俄罗斯家庭用户计算机保护系统的首选供应商（IDC Endpoint Tracker 2014）。

卡巴斯基实验室于1997年在俄罗斯成立，已发展成为国际集团公司，在33个国家设有38个办事处。公司拥有3000多名熟练人才。

产品 卡巴斯基实验室产品为家庭电脑到大型企业网络的所有系统提供保护。

个人产品系列包括桌面，笔记本电脑和平板电脑，智能手机和其他移动设备的安全应用程序。

该公司为工作站和移动设备，虚拟机，文件和Web服务器，邮件网关和防火墙提供保护和控制解决方案和技术。该公司的产品组合还提供专门的产品，防止DDoS攻击，保护工业控制系统和预防金融欺诈。与集中管理工具结合使用，这些解决方案可确保针对计算机威胁的任何大小的公司和组织提供有效的自动化保护。卡巴斯基实验室产品经过主要测试实验室的认证，与不同供应商的软件兼容，并经过优化，可在许多硬件平台上运行。

卡巴斯基实验室病毒分析师全天候工作。每天他们发现成千上万的新计算机威胁，创建检测和消毒的工具，并将其签名包含在卡巴斯基实验室应用程序使用的数据库中。

技术 现在已经有许多现代反病毒工具技术的一部分，最初是由卡巴斯基实验室开发的。许多其他开发商在其产品中使用卡巴斯基反病毒引擎并不是巧合，包括：阿尔卡特朗讯，Alt-N，华硕，BAE系统，Blue Coat，Check Point，Cisco Meraki，Clearswift，D-Link，Facebook，通用动力公司，H3C，瞻博网络，联想，微软，NETGEAR，Openwave Messaging，Parallels，高通，三星，Stormshield，东芝，Trustwave，Vertu和ZyXEL。该公司的许多创新技术都获得专利。

成就 多年来，卡巴斯基实验室在打击电脑威胁方面赢得了数百项服务奖。卡巴斯基实验室在2014年由著名的奥地利测试实验室AV-Comparatives进行的测试和研究后，以获得的高级+证书数量排在前两名供应商中，并最终获得最高评级证书。但卡巴斯基实验室的主要成就就是全球用户的忠诚度。该公司的产品和技术保护了4亿多用户，其企业客户数量超过27万。

卡巴斯基实验室网站：

<http://www.kaspersky.com>

病毒百科全书：

<http://www.securelist.com>

病毒实验室：

<http://newvirus.kaspersky.com>

（用于分析可疑文件和网站）

卡斯基实验室的网页论坛：

<http://forum.kaspersky.com>