

# 应急响应指南

卡巴斯基实验室



# 关于本指南

卡巴斯基实验室每年发现约 325,000 个新型恶意软件，不仅家庭用户存在风险，企业、银行、关键基础设施、政府组织以及使用自动化控制系统 ACS(Automatic Control Systems) 的制造业也同样面临风险。

本指南为安全事件响应 IR (Incident Response) 提供了一个基础说明与诠释。

本指南旨在执行下列事项：

- 将攻击周期内的所有相关信息与行为系统化，并融入安全事件响应 (IR) 过程中；
- 提供一个具有建设性的安全事件响应 (IR) 行为流程；
- 介绍一系列可用于安全事件响应 (IR) 过程的各阶段所需工具和实用程序；
- 提供安全事件响应 (IR) 的最佳实践案例。

## 致读者

本文档适用于技术专家（系统管理员）与 IT、信息安全管理负责人。

## 信息安全自主研究资源

本文档并不是执行安全事件响应的综合性操作指南。它为安全事件响应过程提供了一个基础的建议，并且描述了一个建设性的、用于响应信息安全事件的安全事件响应行为流程。

为了获得更多的安全事件响应理论及实践相关知识，建议你先熟悉下列主题：

- 安全事件响应；
- 数据取证；
- 恶意软件的深入分析与逆向工程。

卡巴斯基实验室提供一个从技术层面的、涵盖基础到高级的全面的网络安全课程。如果适用，所有人均可通过客户端、本地或本区域范围内的卡巴斯基实验办公室获得该课程。有关这个课程的更多信息，请参看：<http://www.kaspersky.com/enterprise-security/intelligence-services>。

# 术语和定义

本章提供了本指南中使用的术语及定义。这些术语均只定义在本指南范围内。

本指南将使用的术语如下：

- **APT**

高级持久性威胁（APT）是一种攻击类型，攻击者通过该类型攻击获取对组织的资产访问权，并试图隐蔽潜伏很长一段时间。APT 攻击的目标通常包括监听和窃取敏感数据。APT 攻击涉及定制的、高复杂度的软件的运用。

- **工件 (artifact)**

工件是指攻击过程中被恶意软件创建或篡改的对象。如，恶意软件程序文件、目录、系统日志文件条目、注册表分支等。

- **资产 (asset)**

资产是指属于组织的对象或实体。如，组织网络的工作站、安全控件、以及存储在工作站的数据。

- **攻击、网络攻击 (attack, cyber attack)**

攻击（网络攻击）是指由攻击者发起的试图控制、损坏或销毁一个计算机网络及系统的恶意行为。

- **攻击者 (attacker)**

攻击者是指发动网络攻击的个人或团体。攻击者通常试图获取组织资产的访问权。

- **C&C 服务器**

命令及控制服务器（C&C server）是一台计算机，用于向被攻破的计算机发送命令。

通常，一个恶意软件可向 C&C 服务器发送请求，并在响应中接收命令。

- **防御措施 (defensive measures)**

防御措施是指组织用来防御网络攻击的安全控件及过程。如，组织用于保护工作站的代理服务器、防病毒设施等。

- **终端防病毒设施 (endpoint anti-virus solutions)**

终端防病毒设施是用于保护组织工作站、抵御网络攻击的软件。如，卡巴斯基的终端安全设施。

- **事件 (event)**

事件是指涉及组织资产的任何事情。事件通常表示为可在输入流中被识别的消息、模式、值或标记。如，网络传输、报错或信号、计数等。

- **利用程序 (Exploit)**

利用程序(Exploit)是指可利用攻击者发现的安全漏洞，并提供攻击荷载(Payload)的一段代码、一块数据或一系列命令。

- **安全事件 (incident)**

安全事件是指组织的信息安全及资产因网络攻击而受到损害的事件。

- **安全事件响应 (incident response, IR)**

安全事件响应 (IR) 是指处理、管理安全事件 (如，网络攻击) 的过程。

- **攻击指示器 (indicators of compromise , IOC)**

攻击指示器 (IOC) 是指用于识别网络或系统上潜在的恶意活动的的数据片段。如，异常网络流量、多次登录失败记录、线上被恶意程序利用的文件、以及可疑的注册表或系统文件变更、字符串、URL、IP 地址以及哈希值 (hash) 等。

- **组织 (organization)**

本指南中的组织是指一个被攻击者发动攻击的公司，且该组织有信息安全团队执行安全事件响应。

- **攻击荷载 (Payload)**

攻击荷载 (Payload) 是攻击者用来达到攻击目标的软件程序。根据攻击目标，攻击荷载 (Payload) 可能包含恶意软件或正规软件，以便攻击者获得敏感数据的访问权或对组织造成损害。

- **取样样本 (软件或病毒)**

软件取样样本 (恶意软件样本) 是指一个特定实例或特定实例的一部分。恶意软件的样本是由信息安全团队从受损的资产中获取的。

- **安全控件 (security control)**

安全控件是指组织用于防御网络攻击的一个设备或一系列软件程序。

- **信息安全团队 (security team)**

信息安全团队是由组织内部员工组成的一个团队，致力于提供安全保障并执行安全事件响应。

- **安全信息与事件管理 (SIEM) 系统**

安全信息与事件管理 SIEM (Security information and event management) 系统

是一种软件程序，可收集事件与其他安全相关信息，并分析工作站、服务器、网络设备以及组织安全控件等发生的事件。

- **鱼叉式网络钓鱼** (*spear phishing*)

鱼叉式网络钓鱼是攻击者通过向组织发送恶意电子邮件等方法以达到破坏组织资产或者非授权获取组织机密数据的一种手段。

- **威胁库** (*Threat Feed*)

威胁库是指潜在或当前的网络威胁相关的数据流。威胁库包含用于识别和减轻网络威胁的攻击指示器 (IOC)，威胁库可集成到 SIEM 系统中。

- **漏洞** (*vulnerability*)

漏洞是指可被攻击者利用发动攻击的组织安全缺陷。

# 第一章 安全事件响应基础

本章介绍了用于攻击的 Kill chain 模型和对抗这些攻击的安全事件响应基本过程。

本章内容如下：

- 攻击生命周期（Kill chain）
- 安全事件响应步骤

## 第一节 攻击生命周期（Kill chain）

本节介绍了网络攻击的生命周期和 Kill chain 模型。

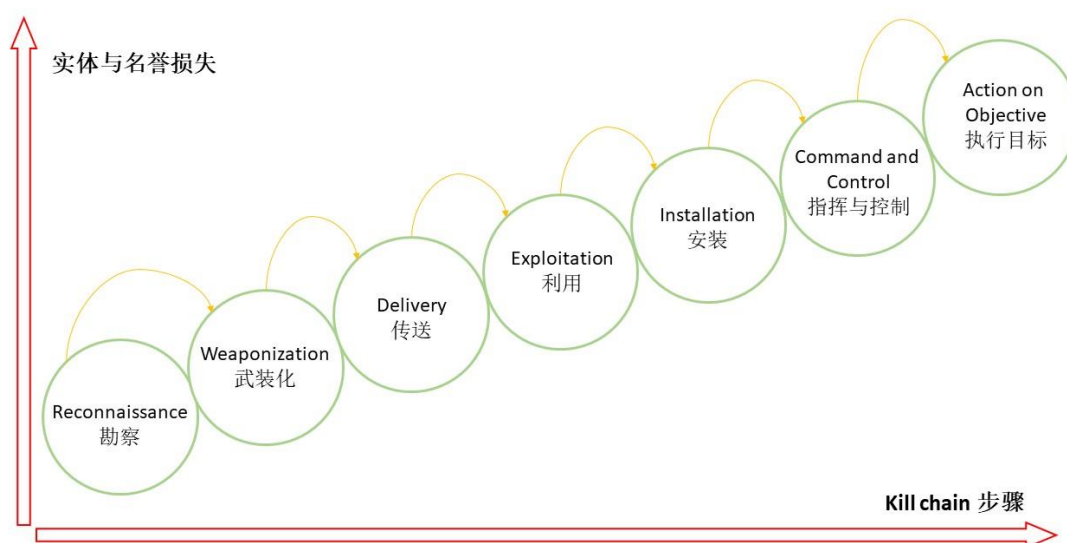
### 关于 Kill chain 模型

当攻击者发起一个网络攻击时会遵循一套结构化的行为。Kill chain 模型就是描述这一系列结构化动作的模型之一。

起初，Kill chain 这个术语是在军事上用于描述攻击结构的词汇。当防御方掌握了攻击者发动攻击时的一整套行为时，防御方可构建一个防御策略用于抵御攻击。

Kill chain 模型不仅适用于 IT 安全，也可用于描述网络攻击。与军事上运用 Kill chain 模型的方式类似，安全团队可建立一套防守策略用于抵御网络威胁。为了成功地应对威胁，安全团队须根据攻击者的行为流程建立防御策略。

当 Kill chain 模型应用到网络攻击时，Kill chain 模型定义了几个攻击阶段。在 Kill chain 模型中，攻击者必然经历这些阶段，以达到攻击的目的。如果攻击者无法执行这些阶段中的任意阶段，那么该攻击将无法成功。



Kill chain 模型定义了如下几个攻击阶段：

1. Reconnaissance 勘察
2. Weaponization 武装化
3. Delivery 传送
4. Exploitation 利用
5. Installation 安装
6. Command and Control 指挥与控制
7. Action on Objective 执行目标

网络攻击造成的实体与名誉的损失程度取决于攻击被检测出的阶段，这个阶段也决定了调查的有效性。如果一个攻击在“执行目标”阶段（最后阶段）被检测到，那么安全团队将无法抵御该攻击，制止攻击者达成目标。一个攻击越早被检测出来（如在“传达”阶段到“安装”阶段），该网络攻击造成的损失就越低。

## 阶段一：勘察（Reconnaissance）

在此阶段，攻击者搜集关于目标组织及其资产的信息。例如，攻击者将试图获取目标的组织结构、技术框架及安全措施的相关信息。攻击者也可能会考虑使用社会工程来对付组织内部员工。如，攻击者可在公共社交网络上获取到员工账户列表。

## 阶段二：武装化（Weaponization）

在此阶段，攻击者利用在“勘察”阶段搜集到的信息决定攻击手法。攻击者选择所需使用的利用程序（Exploit）、攻击荷载（Payload），以及散播这些利用程序（Exploit）、攻击荷载（Payload）的方法。

利用程序（Exploit）可以是一个软件包、一个数据块或一系列命令，它可利用“勘察”阶段发现的漏洞进行攻击荷载（Payload）的散布。攻击者可利用现有的软件或开发一个针对目标组织漏洞的新型软件。

攻击荷载（Payload）是一个软件程序，可供攻击者使用，进而达到攻击目标，根据攻击目标的不同，攻击荷载（Payload）可能包含恶意软件或正规软件，供攻击者访问敏感数据或对目标组织进行破坏。

攻击者可选择多种利用程序（Exploit）。例如，攻击者可能使用已中毒的微软文件或 PDF 文档，可移动存储设备上的恶意软件，或电子邮件附件等。攻击者也可能会诱导公司员工访问恶意的钓鱼 URL，或破坏员工访问的线上资源。

## 阶段三：传送（Delivery）

在此阶段，攻击者将向目标组织传送利用程序（Exploit）。

传送的意义通常包括使用目标公司的公共资源（如公司网站等），控制公司内部员工散播利用程序（Exploit），或破坏与目标组织一同工作的其他公司。

## 阶段四：利用（Exploitation）

在此阶段，利用程序（Exploit）可利用网络安全漏洞，在组织内网的计算机上安装恶意软件。该计算机可感染组织内网的其他计算机，并将攻击荷载（Payload）散播到所有受感染的计算机上。

## 阶段五：安装（Installation）

在此阶段，攻击荷载（Payload）感染了目标计算机，自行安装并试图隐藏行迹，以便躲避检测与被删除。



通常，攻击荷载（Payload）将试图自行安装，通过这样的方式保持其可操作性及隐蔽性，即使利用程序（Exploit）所利用的漏洞已被发现并得到修复。

例如，攻击荷载（Payload）可能包含一个后门（backdoor）。这个后门（backdoor）在受感染的计算机上自行安装，修改系统注册表，使系统在启动的同时也启动该后门。该后门（backdoor）隐藏自己的进程，防止用户在任务管理器上看到该后门（backdoor）进程。当该后门（backdoor）启动时，攻击者可通过连接它来控制受感染计算机。

## 阶段六：指挥与控制（Command and Control）

在此阶段，攻击荷载（Payload）将等待来自攻击者的命令。

接收命令最常用的方式是在目标组织内网中建立一个命令及控制服务器（C&C server）。C&C 服务器受攻击者控制。一旦连接建立后，攻击者可发送命令给攻击荷载（Payload）并采取行动达到目的。例如，攻击荷载（Payload）包含后门（backdoor）程序，攻击者可获取受感染计算机的控制权，访问这些计算机内的信息，并监听用户的行为。

如果受感染计算机不能直接访问网络，无法与 C&C 服务器建立连接，攻击者可通过提供其他恶意软件给攻击荷载（Payload）来传达命令。

## 阶段七：执行目标（Action on Objective）

在此阶段，攻击者使用攻击过程中下载的攻击荷载（Payload）和其他软件来实现攻击目标。

一旦攻击者破坏了组织内某一资产，他将试图窃取、更改或销毁已受损资产的可用数据。

例如，如果攻击目的是窃取敏感数据，并且攻击荷载（Payload）是后门（backdoor）程序，攻击者可获取受感染计算机的控制权，并搜索存储在该计算机上的所需数据。

如果数据并未存储在受感染计算机中，攻击者可使用横向转移（Lateral movement）技术。攻击者可以利用受感染的可控计算机，感染组织内网中的其他计算机，窃取用户证书，进而访问不可用的计算机，甚至通过扮演受感染计算机用户，诱骗其他员工提供所需数据。

## 第二节 安全事件响应步骤

本节介绍了安全事件响应流程的基础。

### 关于安全事件响应

安全事件响应（IR）是用于处理和管理一个事件（如网络攻击等）的规范化的流程。

安全事件响应（IR）的主要目标如下：

- 减少攻击带来的破坏
- 缩短攻击复原时间
- 制作一个操作手册和防御指南用于防止同类攻击再次发生

安全事件响应流程始于对安全事件的调查，当安全团队调查一个安全事件，须判别如下事项：

- **攻击载体 (Attack vector)**

攻击者散播攻击荷载（Payload）的手段。

- **攻击荷载 (Payload) 和利用程序 (Exploit)**

攻击者使用的恶意软件和其他工具。

- **攻击目标 (Target of the attack)**

攻击影响的网络、系统和数据。

- **破坏程度 (Damage inflicted)**

攻击造成的实物、名誉的损害程度。

- **攻击状态 (Attack state)**

当前所处的攻击阶段（攻击生命周期），即攻击者能否通过执行操作来实现目标，以及攻击者是否已经达到了攻击目标。

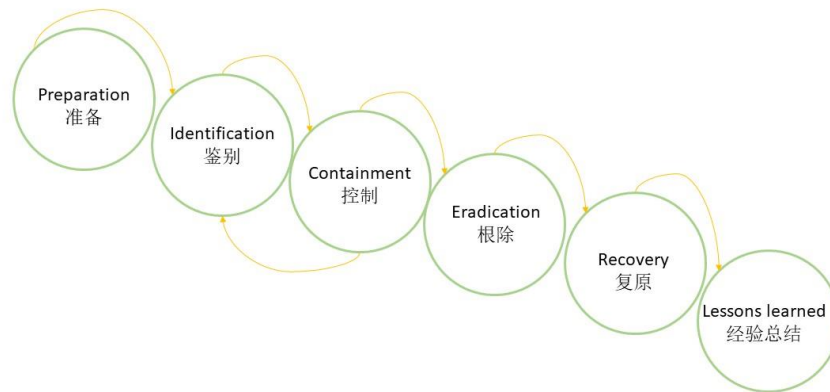
- **攻击时间表 (Attack timeline)**

攻击的起始与终止时间，被检测的时间，以及安全团队可以应对该攻击的时间。

当调查完成后，安全团队必须使用已获取的相关信息复原受损系统，并更新升级安全策略和安全事件响应（IR）计划。

## 关于安全事件响应阶段

基于攻击生命周期（Kill chain）的相关信息，安全团队可以创建一个防御策略并应用于安全事件响应中。在安全事件响应实例章节中提供了应用该策略的实例。（见 25 页）



安全事件响应流程包括如下阶段：

1. Preparation 准备
2. Identification 鉴别
3. Containment 控制
4. Eradication 根除
5. Recovery 复原
6. Lessons learned 经验总结

### 阶段一：准备（Preparation）

攻击事件发生时，安全团队必须快速精准的采取行动。这就要求有所准备。安全团队成员必须准备应对流程、工具以及有助于预防、探查和响应网络攻击的策略。

准备事项中须包含公司员工培训。所有的公司员工必须熟知公司的安全政策，并能够在发生网络攻击时清楚知晓如何应对。

负责管理并执行安全事件响应的安全团队必须通过不断获取安全事件响应领域的知识来扩展专业知识与技能。

## 阶段二：鉴别（Identification）

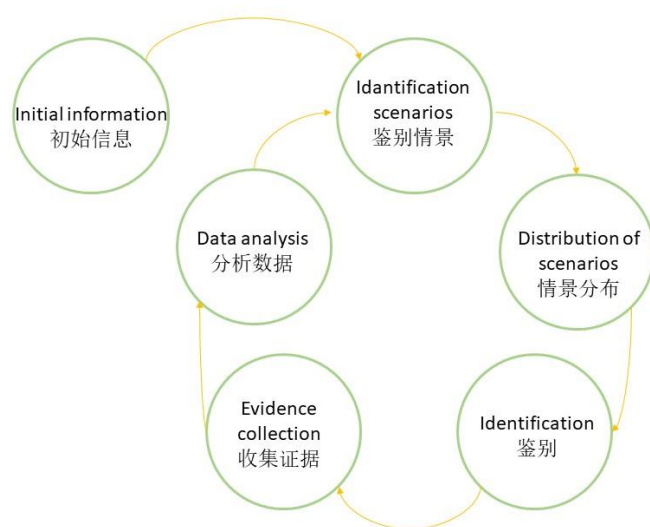
在此阶段，安全团队须判定某个事件是否是信息安全事件。为此，安全团队须将可用事件信息与已知的攻击指示器（IOC）做比较。

攻击指示器（IOC）是用于识别系统或网络中存在潜在的恶意活动的数据片段。如，IOC 包括异常的网络流量、多次登录失败行为、恶意软件使用的文件，可疑的注册表或系统变更等。

为了收集 IOC，安全团队可以从公共报告和威胁提要中获取信息，并对恶意软件进行静态、动态分析。

静态分析是在不启动软件的情况下进行的。这可用于获取多种类型的 IOC，包括网络和电子邮箱地址的软件应用和哈希（hash）文件。

动态分析需要在受保护的环境（沙箱或脱机的计算机）中使用软件。动态分析可以执行软件的行为检查和与之相关的 IOC 收集。



收集 IOC 是一个循环过程。基于攻击的初始信息，安全团队可建立监测方案。运用该方案通常可以监测到新的 IOC。新的 IOC 有助于进一步识别攻击和获取更多攻击相关信息，从而建立一个循环。

当事件被定义为安全事件时，才继续执行 IR 流程的剩余阶段。

### 阶段三：控制（Containment）

在此阶段，安全团队必须识别出受损计算机，并调整安全策略，以防止公司资产进一步遭受损坏。安全团队须重新配置组织的网络环境，以便隔离受损资产。

例如，如果组织内部的一个服务器被攻击者破坏，安全团队须在网络环境中隔离该服务器。安全团队还须调整路由策略，以防该服务器感染其他服务器。

### 阶段四：根除（Eradication）

在此阶段，安全团队须将受损资产恢复成原有的状态。通常涉及到恶意软件的清除、恢复配置以及清除恶意软件残留的组件等。

例如，如果一个计算机被后门（Backdoor）软件损坏，安全团队须删除后门（backdoor）软件，恢复受损文件和系统注册表，并删除后门（Backdoor）软件的安装文件。

### 阶段五：复原（Recovery）

在此阶段，之前被损坏的资产已经重新投入运作。一段时间内，安全团队须监控该资产的状态，以确保威胁已经完全解除。

例如，如果组织网络环境内的一个服务器被恢复了，安全团队须将其重新加入到组织网络环境中，调整路由策略使用该服务器，并在一段时间内监控服务器的行为，以确保其没有可疑行为。

### 阶段六：经验总结（Lessons learned）

在此阶段，安全团队须分析安全事件，制定措施，用于抵御类似的安全事件。并应升级应对此类安全事件的安全事件响应计划。

该措施可包含调整安全策略，变更组织的资产配置，以及对公司员工实施信息安全教育。

安全事件响应计划是一套书面指南，用于识别安全事件及其响应。即使它无法完全的抵御日后的安全事件，安全事件响应计划也将有助于缩短安全事件的识别时间并提高安全事件响应效率。

## 第二章 安全事件响应流程的建议及规则

本章介绍了执行安全事件响应和事故调查的规则和建议事项。

### 阶段一：准备（Preparation）

本节提供了安全事件响应流程中“准备”阶段的一些相关建议事项。

#### 防御措施

为了有效的对抗网络攻击，安全团队须采取保护组织资产的防御措施，建议创建多层次的防御措施，并创建一个防御边界，用于抵御来自多个攻击载体（attack vector）的网络攻击。

例如，可考虑下列防御措施：

- 在所有工作stations上安装一个终端防病毒软件；
- 在网络环境中设置入侵防御系统（IPS）；
- 互联网网关处设置防火墙保护；
- 访问互联网须通过组织的代理服务器，并需要授权；
- 组织使用 SIEM 系统跟踪事件，SIEM 系统保存完整的威胁库；
- 为网络攻击者提供一个诱导系统（又称 honeypot），该系统是分离的，且由安全团队监控。卡巴斯基实验室专家不断地开发新的安全解决方法，提供全面的保护，防止各种类型的信息安全威胁，网络和钓鱼攻击。
- 为保护工作stations抵御已知、未知以及高级威胁，卡巴斯基实验室专家开发了 Kaspersky Endpoint Security。
- 为了保护企业免受针对性的攻击和高级威胁，卡巴斯基实验室创建了 Kaspersky Anti increase Targeted Attack Platform（KATA）

想了解更多卡巴斯基实验室的企业安全解决方案，

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

## 渗透测试

渗透测试是指针对计算机系统的模拟攻击，并且可以检测出计算机中的安全漏洞。渗透测试可以由第三方组织进行，并将渗透测试结果报告给安全团队。安全团队可根据该结果修复漏洞。

## 专业技能提升

安全团队成员须持续不断提升自己在安全事件响应理论和实践方面的专业技能。

卡巴斯基实验室课程提供一个全面的课程，包含网络安全的主题和技术，以及从基础到专家层面的评估。如果适用，所有人均可通过客户端、本地或本区域范围内的卡巴斯基实验室办公室获得该课程。有关这个课程的更多信息，请参看：  
<http://www.kaspersky.com/enterprise-security/intelligence-services>

了解信息安全领域内的事件和趋势，以及新兴网络安全威胁和对抗这些威胁的防御措施相关信息是很重要的。例如，APT 报告服务，这是卡巴斯基实验室威胁情报门户解决方案（见 45 页）的一部分，它将提供与卡巴斯基实验室持续不断的连接，用于同步卡巴斯基实验室针对高识别度的网络间谍活动领域内的调查与发现。

## 收集安全事件响应相关信息

安全团队须收集安全事件以及安全事件响应流程相关信息，并准备一个安全事件响应计划。这些信息可包含安全事件报告和组织内发生的安全事件的历史日志。

## 阶段二：鉴别（Identification）

本节提供了安全事件响应流程中“鉴别”阶段的一些相关建议事项。

## 事件触发器（Incident triggers）

本节介绍了可作为事件触发器（Incident triggers）的事件。

本节所述的事件和事件触发器并不是网络攻击可疑行为的完整列表。

## 什么是事件触发器？

事件触发器（Incident triggers）是一个指示网络威胁表征的事件。当事件触发器被触发，安全团队须意识到一个网络攻击可能在发起中。事件触发器是安全团队用于区分安全事件与事件的基准。

## 关于事件源（event sources）

事件可以有很多起源头，这类事件可能是 Anti-APT 系统，蜜罐诱饵，入侵防御系统、很多其他安全控件和手段。

就本指南而言，事件被认作是来自事件源的单一类别-SIEM 系统和用于管理公司网络环境内终端防病毒设施及系统。

## SIEM 系统触发的事件触发器

SIEM 系统能汇总大范围内软、硬件安全控件的相关信息。包括代理服务器和防火墙。

在 SIEM 系统汇总出的事件中，与安全控件中可构成威胁库（Threat Feed）的事件相匹配的事件可被认为是事件触发器。安全控件可检测出这类来自威胁库的攻击指示器（IOC），以及事件表征信号。

就本指南而言，假定卡巴斯基实验室的 Data Feeds 已应用于匹配 SIEM 事件。Data Feeds 是卡巴斯基威胁情报门户的一部分（见 45 页）。

例如，组织网络环境内的计算机的恶意软件试图连接恶意 URL。与常规的 URL 一样，组织的代理服务器利用恶意 URL 生成一个事件，并将该事件发送给组织的 SIEM 系统。SIEM 系统试图将该 URL 和卡巴斯基威胁库（Threat Feed）匹配。如果这是一个卡巴斯基威胁库中收录的恶意 URL，那么本次匹配是成功的。SIEM 系统将接收到关于本次匹配的事件信号。这个事件将被认作是一个事件触发器。

## 防病毒管理系统触发的事件触发器

防病毒管理系统可汇总用于保护工作站的终端防病毒设施（endpoint anti-virus solutions）的相关事件。



当工作站或安全控件的一个终端防病毒设施检测出一个威胁，将生成一个事件并发送给防病毒管理系统。

所有这类事件并不都能构成事件触发器。例如，一个检测恶意软件的事件可能伴随着一个消除恶意软件的事件。这种情况不需要进一步调查。

防病毒管理系统接收的下列事件可被认作是事件触发器：

- 企图连接一个已知的 C&C 服务器；
- 终端防病毒设施尝试删除恶意软件失败；
- 同一个计算机上反复检测到恶意软件；
- 防病毒报错和失败导致保护级别降低。

安全团队须对这些事件触发器（Incident triggers）做出响应，就如同接收到 SIEM 系统判定恶意哈希值（hash）和恶意 URL 的事件一样，对其做出响应。防病毒管理系统的所有事件均可被收录到 SIEM 系统。

## 可判定为事件触发器的可疑行为

一些其他事件也可被认作是事件触发器。这些事件的表征需要安全团队关注和调查。

可疑事件的示例如下：

- 操作系统启动时自动执行的未知软件；
- 系统服务列表中有未知的服务项；
- 任务目录里执行着不可用于运行可执行文件的异常文件。如，临时目录和系统缓存；
- 从目录中加载的动态库，某些动态库文件极不可信。例如，一个软件从软件可执行文件所在的目录中加载系统库；
- 用户权限突然升级；
- 可被攻击者利用的正规软件。如 mimikatz，Windows Credentials Editor 和很多远程管理工具等。

与网络活动相关的可构成事件的可疑行为如下：

- DNS 或 ICMP 的协议流量异常大量上升；
- 频繁改变自己 IP 地址的域名。这种行为可能标志着攻击者使用快速通量 DNS 技术，隐藏受损主机背后的 C&C 服务器；
- 与卡巴斯基实验室威胁库收录的 URL 交互。例如，一个被归类为恶意软件源或利用

程序包（Exploit）登录页面的 URL；

- 与卡巴斯基实验室威胁库收录的 IP 交互。例如，一个被归类为扫描网络的 IP 地址，或一个被归类为进行 DDoS 攻击的 IP 地址；
- 与一个具有可疑 Whois 信息的域交互。

## 优先级指南

本节主要介绍了安全事件的优先级相关基础。

时间是在安全事件响应（IR）流程中供应最短的资源。

从攻击开始到安全团队响应的时间长度决定着攻击者能否达到攻击目标。如果安全团队同时面对大量的安全事件，他们可能没有充足的时间去应对所有事件。因此，安全事件须划分优先级。

安全事件优先级须以下列因素为基础定义：

- 受感染计算机所在网段；
- 受感染计算机内存储的数据价值；
- 影响同一计算机的其他安全事件的类型和数量；
- IOC 相关安全事件的可靠性。

最终的安全事件优先级须依据每个组织的特性定义。对于一些组织而言，最危险的安全事件是勒索（加密受感染计算机内数据的恶意软件）相关的，因为这些组织的工作涉及到知识产权或敏感数据。其他组织可能优先考虑与潜在风险软件（如 pornware）相关的安全事件，因为使用这些软件可能会存在信誉风险。

例如，安全团队可参考使用下列安全事件优先级分级标准：

1. 高级持续性威胁（APT）相关安全事件为最高优先级。有关检测 APT 相关的更多信息，见后续“检测高级持续威胁”。
2. 恶意软件相关安全事件为第二优先级。
3. 潜在危险的软件（adware, pornware 等等）为第三优先级。

## 检测高级持续性威胁

高级持续性威胁（APT），攻击者企图在该攻击中获取对组织资产的访问权，并试图隐藏停留很长一段时间。

APT 攻击的目标普遍包含搜集和窃取敏感数据。

定义一个被检测的攻击是否是 APT，可参考下列标准：

- 卡巴斯基实验室 APT 报告中的 IOC。APT 报告是卡巴斯基实验室威胁情报门户解决方案的一部分（见 45 页）；
- 与曾经用于其他 APT 的 C&C 服务器交互。这种交互可通过静态和动态威胁分析确定。

为了检测威胁行为，并获取与之交互的 URL 列表，建议使用工具和“分析”阶段介绍的的工具和功能（见 44 页）。

如果威胁的 IOC 在卡巴斯基实验室的威胁库中有 2 个或者更多，那么该威胁可被看作是恶意软件，这类威胁不可被看作是 APT。

建议使用卡巴斯基实验室威胁情报门户解决方案（见 45 页）中的威胁检索服务，可用于定义普遍的威胁。如果普遍的 IOC（hash 或 URL）很低，那么该威胁可被看作是 APT。

## 分析 SIEM 的安全事件

本节介绍了用于分析不同类型的 SIEM 系统事件的执行建议。

### 所有事件的应对行为

当安全团队接收到来自 SIEM 系统的事件触发器，建议遵照下列流程执行：

1. 确定引发 SIEM 生成事件触发的最初事件。该事件的 IOC 已被 SIEM 检测。
  - 如果威胁是由电子邮件附件引发的，检查组织电子邮件服务器的日志文件。
  - 如果威胁是由互联网引发的，检查组织代理服务器、防火墙、UTM 网关或其他提供网络访问设备的日志文件。
2. 确定当前攻击阶段，这取决于被检测到的 IOC 类型。例如，如果检测到一个与 C&C 服务器交互的行为，那么该攻击处于“鉴别”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，以及与事件相关的 IOC 的可靠性。依据这两个标准，调整事件的优先级。
4. 根据检测到的威胁类型执行其余操作，如下列各节所述。

如果威胁被终端防病毒设施检测到，仅在下列情况下需要执行安全事件响应：

- 威胁未被终端防病毒设施阻断。如，一个已经被员工下载的恶意软件；

- 威胁已被阻断，但事件发生多次。如，组织网络环境内的一个计算机试图下载恶意软件，该计算机极有可能未被终端防病毒设施检测到存在恶意软件感染。

## 检测出威胁相关的 URL

如果检测出威胁相关的 URL，须依据 URL 的类型执行相关操作。（括号中的值是卡巴斯基实验室威胁库中定义的类别）

### ► 检测出一个钓鱼 URL (PHISHING category):

1. 检查该 URL 指向的 Web 页面源代码。确认可能已被员工提供给攻击者的信息。
2. 在 SIEM 系统，分析被攻击员工的相关事件。这需要在员工访问钓鱼网站前的十分钟到访问后十分钟之间完成。
  - 如果员工发送或下载了任何文件，执行了下一步（如果检测到威胁的哈希值）描述的操作。
  - 如果并未发送或下载文件，告知员工事件的相关情况。根据员工提供的信息的价值，可能需要采取额外的行动。
3. 如果员工的凭证可能已经遭到破坏，那么需要变更员工的密码。

### ► 检测出恶意的 URL (MALICIOUS category):

1. 通过分析代理服务器上的事件，判定恶意软件是否已经被下载了。
  - 如果恶意软件并未被下载，那么受影响的资产就没有遭受破坏的危险。这样的事件并不是一个威胁事件，且不需要进一步调查。确保将该恶意的 URL 添加到黑名单中即可。
  - 如果恶意软件已被下载，那么须继续调查该事件。
2. 确认恶意软件是否被防御措施拦截，如，组织内部的代理服务器或防病毒设施。
  - 如果恶意软件被拦截，且类似的事件是第一次发生，那么受影响的资产并没有遭受破坏的危险。这样的事件并不是一个威胁事件，且不需要进一步调查。
  - 如果恶意软件被拦截，且类似的事件不是第一次发生，那么须继续调查该事件。
  - 如果恶意软件未被拦截，继续调查该事件。
3. 获取该 URL 指向的恶意软件样本，如果该 URL 指向一个网页，检查该网页的源代码，以便确认从该处下载的样本。
4. 分析恶意软件样本。

关于分析恶意软件样本的更多信息，请见章节“分析工具介绍”。

5. 确认被下载的恶意软件是否执行了。
6. 扫描被破坏的计算机，以获取所检测到的威胁的 IOC。扫描与其在同一网段的其他计算机，并获取所检测到的威胁的 IOC。包括调查扫描期间获得的新 IOC。如，通过对恶意软件样本的分析，获得新的 IOC。
7. 继续进入安全事件响应流程的“控制”阶段。

#### ► 检测出僵尸网络的 C&C URL (BOTNET C&C category)

1. 确认试图与 C&C 服务器交互的软件，并分析该软件。

关于分析软件样本的更多信息，请见章节“分析工具介绍”。

2. 扫描被破坏的计算机及其恶意软件。该软件可能通过来自 C&C 服务器的指令被下载。
3. 分析 URL。

关于分析 URL 的更多信息，请见章节“分析工具介绍”。

4. 扫描被破坏的计算机，以获取所检测到的威胁的 IOC。扫描与其在同一网段的其他计算机，并获取所检测到的威胁的 IOC。包括调查扫描期间获得的新 IOC。如，通过对 URL 的分析，获得新的 IOC。
5. 继续进入安全事件响应流程的“控制”阶段。

如果检测到僵尸网络的 C&C URL，那么攻击已经到达“命令和控制”阶段。目前，攻击行动很活跃。

#### ► 检测出移动终端的僵尸网络的 C&C URL (MOBILE BOTNET C&C category):

1. 通过移动终端版的防病毒软件扫描被破坏的移动电话或可移动设备。
2. 继续进入安全事件响应流程的“控制”阶段。

### 检测出威胁的哈希值 (hash)

如果检测出威胁的哈希值，需依据哈希值的类别执行操作。（括号中的值是由卡巴斯基实验室提供的威胁类别）

#### ► 检测出恶意软件或 BOT 的哈希值 (MALICIOUS and BOT categories):

1. 分析该哈希值所属的恶意软件

关于分析软件实例的更多信息，请见章节“分析工具介绍”。

2. 扫描被破坏的计算机，以获取所检测到的威胁的 IOC。扫描与其在同一网段的其他计算机，并获取所检测到的威胁的 IOC。这些扫描包含调查期间发现的新 IOC，例如，这些新 IOC 可用于分析恶意软件。

► **检测出一个移动端的恶意软件、BOT 和木马病毒的哈希值**

(MOBILE MALICIOUS, MOBILE BOT, and MOBILE TROJAN categories):

1. 使用移动端防病毒软件扫描被破坏的移动终端。
2. 继续进入安全事件响应流程的“控制”阶段。

## 检测出威胁的 IP 地址

如果检测到一个威胁的 IP 地址，需依据 IP 地址的类别执行操作。以下类别由 SIEM 事件与卡巴斯基实验室提供的威胁类别匹配的结果确定的。

► **检测出一个 Tor 出口节点 IP 地址 (TOR EXIT NODE category):**

1. 询问确认员工是否使用过 Tor。
  - 如果员工确认其使用过 Tor，那么这样的事件就不是安全事件，不需要进一步调查。
  - 如果员工确定其并未使用过 Tor，需继续调查。
2. 扫描被破坏的计算机，并确认使用 Tor 的软件。这类软件可能是正规软件，或是通过 Tor 隐藏其行为的恶意软件。扫描与其在同一网段的其他计算机，进而排查恶意软件。
3. 针对检测出的软件文件，重新执行一整套鉴定流程。

► **检测出垃圾邮件的 IP 地址 (SPAM category):**

1. 继续进入安全事件响应流程的“经验总结”阶段。

► **检测出恶意软件的 IP 地址 (MALWARE category):**

1. 确认并分析试图与该 IP 地址交互的软件。

关于分析软件实例的更多信息，请见章节“分析工具介绍”。
2. 执行“检测出威胁相关的 URL”部分中描述的操作。

## 阶段三：控制 (Containment)

本节提供了安全事件响应流程中“控制”阶段的一些相关建议事项。

## 控制阶段的目标

控制阶段有两个主要目标：

- 在保障系统可操作性的基础上，隔离受损资产
- 防止用于调查的 IOC 被删除

## 隔离受感染的计算机

建议将受感染的计算机移至单独的隔离网络环境。安全团队须变更路由策略，以防受感染计算机与组织内网中的其他计算机互通，并防止其访问互联网。

不建议将受感染计算机关机。有些恶意软件会将其自身保存在内存中，且并不在硬盘上创建文件。如果感染此类恶意软件的计算机关机，此类恶意软件的 IOC 将会遗失。当系统收到关机指令时，有些类型的恶意软件将会删除其 IOC。这会使调查更加困难。

不建议禁用受感染计算机的本地网络或采用物理手段限制其网络连接。有些类型的恶意病毒会监听受感染计算机的本地网络连接状态。如果网络连接被禁用一段时间，恶意软件将开始删除其存在的痕迹，以毁坏其 IOC。

## 创建内存和硬盘的副本（Dump）

为了继续调查，安全团队须获取内存和硬盘的副本（Dump）。这些副本包含恶意软件的所有组件。

通过分析受感染计算机的内存和硬盘的副本，安全团队可获取恶意软件的样本和攻击相关的 IOC，并确认攻击载体（Attack vector）。

这些信息可用于防止同类攻击进一步升级到“传送”、“利用”、或“安装”阶段。通过分析恶意软件的样本，安全团队可以找到一种有效地根除该恶意软件的方法。

如果很难将内存和硬件的副本（Dump）传送至安全团队，那么建议先将内存副本（Dump）传送过去。安全团队分析完内存副本（Dump）后，再决定是否需要硬件副本（Dump）。例如，一个组织可能拥有多个物理环境分离的办公区，但该组织只有一个安全团队。

关于创建内存和硬盘副本（Dump）的工具的更多信息，请见章节“创建副本（Dump）的工具介绍”（见 42 页）。关于分析内存和硬件副本（Dump）的工具的更多信息，请见章节“分析内存副本（Dump）的工具介绍”和“分析硬盘副本（Dump）的工具介绍”（见 47 页）。

硬盘的全部副本（Dump）通常占用硬盘上可用的全部空间。这是因为硬盘副本（Dump）还包括来自硬盘空余（未使用）扇区的信息。例如，如果一个硬盘有 400G 的存储空间，已使用 50G，那么该硬盘副本（Dump）将占据 400G 的空间。

## 保持可操作性

受感染计算机被隔离后，系统须保持其可操作性。例如，如果组织网络环境内的多个服务器被感染，那么安全团队须变更路由策略，以便其他服务器可分担受感染服务器的负载。

## 阶段四：根除（Eradication）

本节提供了安全事件响应流程中“根除”阶段的一些相关建议事项。

“根除”阶段有两个可行策略：

- 完全复原受损资产

例如，一个工作站可通过一个工作站镜像复原。

这个策略适用于员工工作站使用标准软件集的组织。如果受损资产是个手机或其他硬件设备，可采取恢复出厂设置。

- 检测受损资产中的恶意软件、删除其文件以及其创建的工件。

例如，一个被后门软件感染的工作站，可通过删除后门软件和其创建在硬盘上的文件，以及还原系统注册表来复原。

恶意软件所创建的工件的检测，可通过使用工具、以及章节“分析工具介绍”中描述的相关设施进行恶意软件分析实现。

## 阶段五：复原（Recovery）

本节提供了安全事件响应流程中“复原”阶段的一些相关建议事项。

在这个阶段，曾受损的资产会被重新投入使用。安全团队须监控该资产一段时间，以确保该威胁已经被彻底根除。

例如，如果组织中的一个服务器被复原，安全团队已将其移至组织网络环境中，调整其路由策略并启用该服务器。那么须监控该服务器的行为，以确保其没有可疑的行为。



## 阶段六：经验总结（Lessons learned）

本节提供了安全事件响应流程中“经验总结”阶段的一些相关建议事项。

调查完全结束后，安全团队须拟定报告。该报告需包含下列要素：

- 安全事件由谁在什么时候发现的？
- 安全事件的影响范围？有哪些资产受到影响？
- “控制”阶段、“根除”阶段及“复原”阶段是如何执行的？
- 安全事件响应的哪个阶段安全团队执行的最高效？
- 安全事件响应的哪个阶段安全团队需要加强优化？

根据这个报告和调查期间获取到的信息，安全团队须强化安全措施，以防止此类安全事件再次发生。并且针对此类安全事件，升级安全事件响应计划。

该措施可能包含安全策略调整，组织资产的配置变更，以及开展员工信息安全培训等。

安全事件响应过程中获取的 IOC 可供安全团队使用，以便将来发现此类攻击。

安全事件响应计划须包含一系列的书面操作指南，用于识别安全事件并做出响应。即使将来该计划无法完全防止安全事件，但可缩短安全事件的鉴别用时，并且提升安全事件响应的效率。

## 第三章 安全事件响应实例

本章提供了一个网络攻击的实例，以及安全团队进行安全事件响应的实例。

### 第一节 攻击计划（实例）

本节提供了一个网络攻击计划的实例。本实例中，罪犯试图获取一家银行的 ATM 控制系统的控制权限，进而从 ATM 终端取款。

### 攻击目的、攻击荷载（Payload）、利用程序（Exploit）以及传送方式

本次攻击的攻击目的是从 ATM 终端取款。当攻击者获取对 ATM 网关的控制权，并入侵 ATM 终端时，该目的就达成了。

本次攻击的攻击荷载（Payload）是装载软件（Loader Software）。装载软件传送完毕后，该装载软件将下载、安装并运行 BOT 软件。之后，装载软件将继续监控 BOT 软件。如果 BOT 软件被清除，装载软件会重新下载并安装 BOT 软件。例如，终端防病毒设施可能会清除 BOT 软件，但是装载软件将会不断重复安装 BOT 软件。

BOT 软件可根据攻击者的 C&C 服务器发送的命令来远程控制受感染的计算机。BOT 软件具备后门软件的功能，允许攻击者获取受感染计算机的控制权。

攻击者将使用补充软件进一步窃取用户凭证。攻击者会选择可实现这一目的的正规软件，如 Mimikatz 软件。BOT 软件与 C&C 服务器建立连接后，BOT 软件会从 C&C 服务器提供的 URL 中下载 Mimikatz 软件。

本次攻击用到的最后一个软件是攻击者自主开发的自定义软件。用于破坏位于 ATM 网关后面的 ATM 终端。一旦攻击者获取到了 ATM 网关的访问权，该软件将被 BOT 软件下载。

本次攻击的利用程序（Exploit）是包含装载软件的 PDF 文件。通过利用 Adobe Acrobat Reader 软件的漏洞，当文件被打开时，利用程序会触发执行装载软件。

攻击者通过鱼叉式钓鱼攻击（Spear Phishing）传送利用程序（Exploit）。该利用程序（Exploit）会被附加到发送给目标组织的员工的电子邮件中。

## 步骤一：勘察（Reconnaissance）

攻击者获取有关入侵 ATM 终端的信息。为了做到这一点，攻击者须获取银行 ATM 网关的控制权，这是个受高度保护的资产。

攻击者将创建一个使用同一类型 ATM 网关的银行列表。之后，攻击者会收集每个银行的安全措施的相关信息。攻击者将分析出有价值的信息并选择目标。通过使用社会工程的手段，攻击者可获取银行员工及其公司电子邮件地址列表。

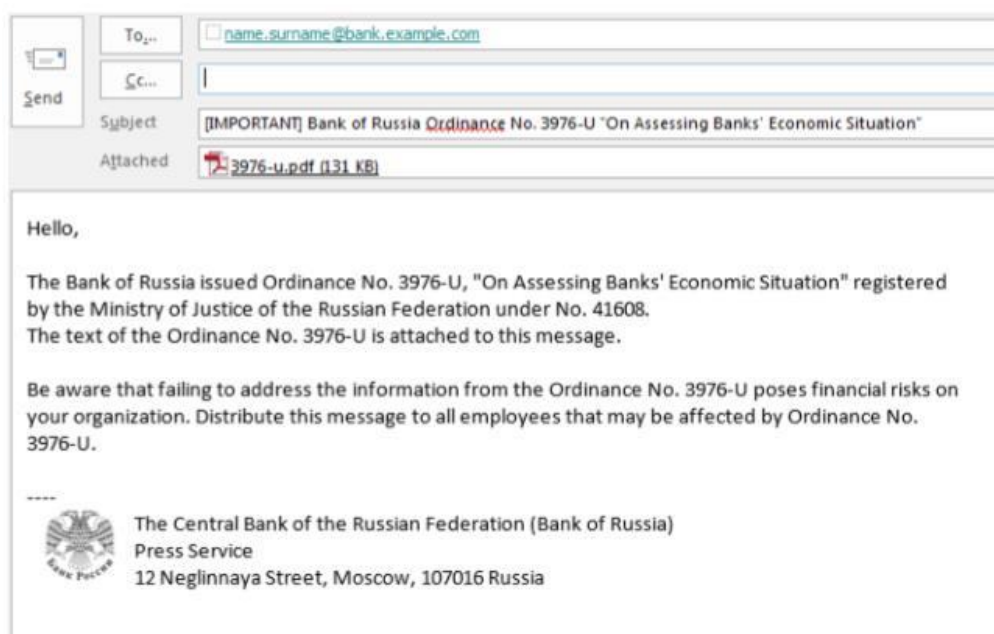
## 步骤二：武装化（Weaponization）

由于破坏银行安全边界（Security Perimeter）的工作不大可能成功，攻击者选择通过向组织内部员工发起鱼叉式钓鱼攻击（Spear Phishing）的方式执行内部攻击。

攻击者选择攻击荷载（Payload）、利用程序（Exploit）以及传送方式。如上一节“攻击荷载（Payload）、利用程序（Exploit）以及传送方式”所述。

## 步骤三：传送（Delivery）

攻击者发起鱼叉式钓鱼攻击（Spear Phishing）。攻击者从利用社会工程手段获取的员工列表中筛选出多名员工并向他们发送电子邮件。攻击者根据员工在鱼叉式钓鱼攻击（Spear Phishing）中的漏洞选择员工。例如，财务部门的员工可能是此类攻击的有利目标。



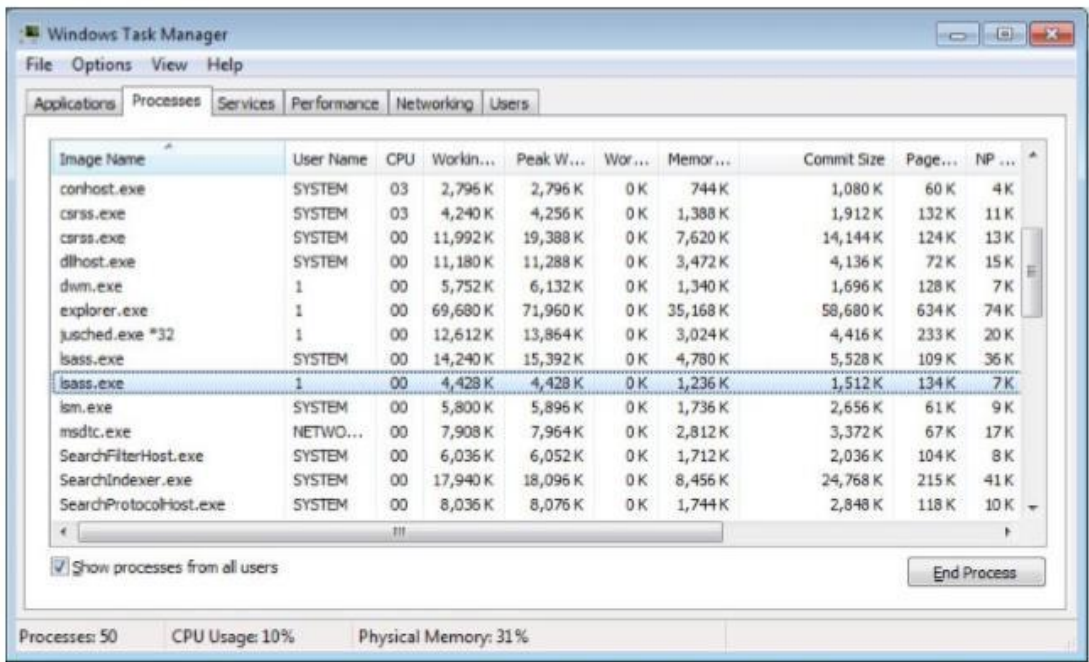
这封电子邮件看似是来自国家金融监管局（Bank of Russia）。这封电子邮件的正文措辞是为了欺骗诱使员工打开附件中的 PDF 文件。

## 步骤四：利用（Exploitation）

员工使用 Acrobat Reader 打开该 PDF 文件后，文件中的装载软件（Loader Software）会复制到员工计算机的硬盘中，并且该装载软件会被添加到操作系统中的启动程序列表中。

## 步骤五：安装（Installation）

受感染计算机下次启动的时，该操作系统将启动并运行装载软件。该装载软件将下载、安装 BOT 软件，并将其添加到操作系统中的启动程序列表中。这一系列的操作都完成后，装载软件会监控 BOT 软件的状态。如果 BOT 软件不在系统中，装载软件将重复执行“安装”步骤。



BOT 软件通过把自己伪装成一个已知的正规系统程序 lsass.exe（本地安全身份认证服务器，Local Security Authentication Server），从而试图隐藏自己的存在。此类软件通常存在于 Windows 操作系统的进程列表中。

## 步骤六：指挥与控制（Command and control）

BOT 软件会与攻击者控制的 C&C 服务器建立连接。

## 步骤七 A：执行目标（lateral movement）

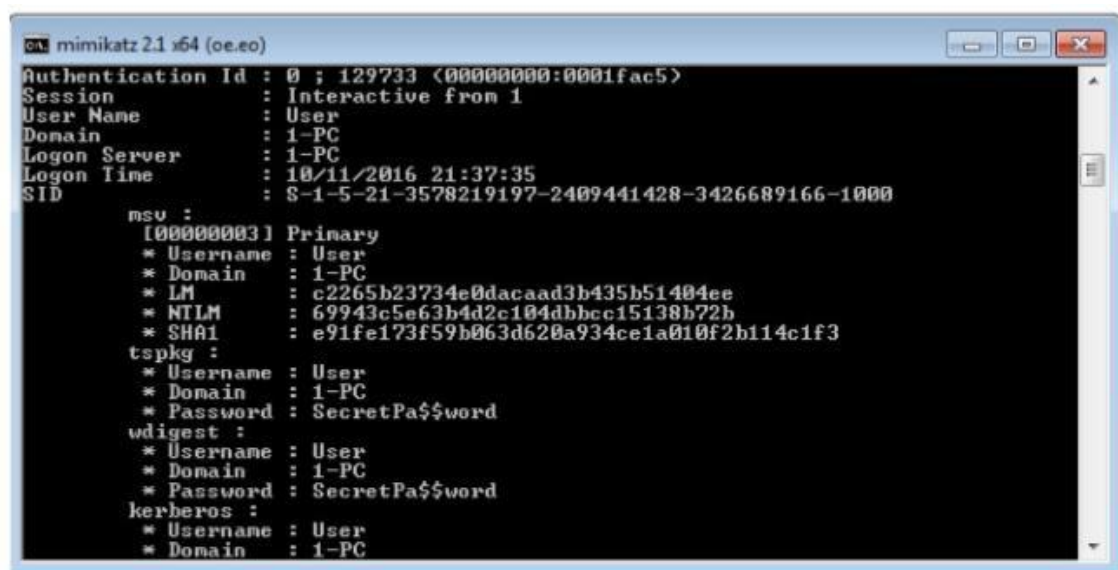
攻击者给 BOT 软件下达的第一个指令是感染组织网络环境内的其他计算机。

BOT 软件利用受感染计算机的访问权限、用户特权以及已知的漏洞，将利用程序（Exploit）传送给其他计算机。攻击者也可能会选择感染组织内部使用的其他 PDF 文件。

这个步骤的目的是为了感染那些自上次操作系统启动后使用管理员账号登录的计算机。

## 步骤七 B：执行目标（theft of credentials）

当计算机（使用管理员账号登录）被发现并被感染，BOT 软件将下载并运行 mimikatz。



```
mimikatz 2.1 x64 (oe.oe)
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
```

攻击者通过 mimikatz 获取所有自上次操作系统启动后使用管理员账号登录的计算机的用户名和密码（包括 Microsoft Active Directory 用户凭证）。这个阶段攻击者的目的是为了获取 Active Directory 的管理员凭证密码。

## 步骤七 C：执行目标（compromising the ATM gateway）

这个阶段攻击者命令 BOT 软件获取 ATM 网关的访问权。BOT 软件通过使用上一步骤中得

到的管理员凭证，进而获取 ATM 网关的控制权。这个攻击的目的达成了。

当 ATM 网关被控制，BOT 软件将下载并安装攻击者自主开发的自定义软件，从而感染 ATM 终端。这一操作是成功的，因为 ATM 网关已经不能阻止攻击者访问 ATM 终端。之后，攻击者可通过 C&C 服务器控制受感染的 ATM 终端并取款。例如，攻击者可模拟某一 ATM 终端取款操作，并迫使终端分发现金。

## 步骤七 D：执行目标（destroying the evidence）

攻击目的达成后，攻击者命令 BOT 软件销毁攻击痕迹。这个阶段的目的是延缓攻击识别和加大调查难度。BOT 软件会从受感染计算机中销毁自身、装载软件（Loader Software）以及 mimikatz 软件。BOT 软件也会试图删除其创建的工件，如受感染的 PDF 文件等。

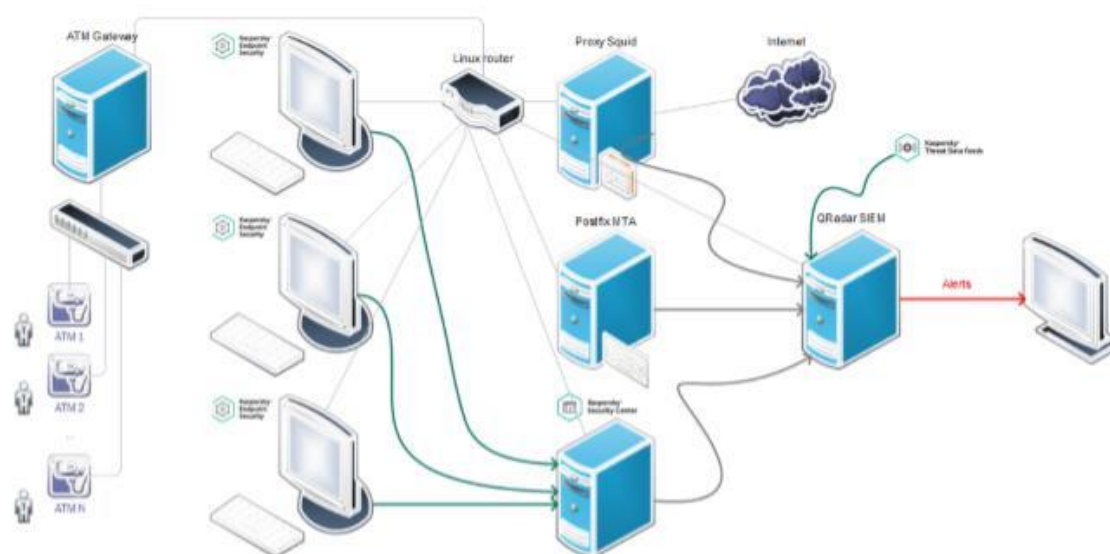
## 第二节 安全事件响应（实例）

本节提供了一个网络攻击事件响应的实例。在本实例中，受攻击的安全团队试图反击攻击者企图控制银行 ATM 控制系统（ATM 网关）的意图。

### 步骤一：准备（Preparation）

本节介绍了银行为防止网络攻击而采取的防御措施。

银行内部网络是结合信息安全层面的考量而设计的。



银行采取下列防御措施来应对网络攻击。银行使用 IBM QRadar SIEM 系统跟踪事件。卡

巴斯基实验室威胁库已集成到了该 SIEM 系统中：

- 组织内部网络访问互联网只能通过 Squid 代理服务器进行。该代理服务器通过配置将事件（Event）发送给 SIEM 系统；
- 银行使用 Postfix 邮件传输代理（MTA）传输组织内部的电子邮件。Postfix MTA 也会将事件发送给 SIEM 系统。这些事件包含来自邮件的报头（Header）信息，也包含“接收”的报头信息；
- 银行内部的所有工作站均受卡巴斯基安全终端（Kaspersky Endpoint Security）保护，由卡巴斯基的安全中心（Kaspersky Security Center）监控；
- 银行路由器的操作系统是 Linux 系统。ATM 网关和 ATM 终端位于隔离网络环境中。仅有少数用户允许访问该网络环境；
- 银行订阅了卡巴斯基威胁情报门户解决方案（Kaspersky Threat Intelligence Portal solution）。（见 45 页）。

## 步骤二：鉴别（Identification）

本节介绍了安全事件响应阶段中的“鉴别”阶段实例。

### 可能发生什么？

因为银行使用 SIEM 系统，员工计算机访问的所有的 URL 和试图与组织内部网络产生交互的 IP 地址都会与威胁库进行匹配。工作站下载的所有文件都会使用终端防病毒设施（endpoint anti-virus solution）进行扫描。当这些信息与威胁库相匹配时，终端防病毒设施会将这些文件的哈希值（hash）发送给 SIEM 系统。

攻击可能在下列这些阶段中的一个阶段被识别出来：

- 攻击者用于发送钓鱼邮件的服务器 IP 与 IP 威胁库相匹配。这种情况下，攻击会在“传送”阶段被识别；
- 下载 BOT 软件的请求信息与恶意 URL 威胁库相匹配。这种情况下，攻击会在“指挥与控制”阶段被识别；
- 连接 C&C 服务器的请求信息与 Botnet C&C URL 威胁库相匹配。这种情况下，攻击会在“指挥与控制”阶段被识别；。
- Mimikatz 软件被用于保护工作站的卡巴斯基安全终端（Kaspersky Endpoint

Security) 发现并删除。这种情况下, 攻击会在“执行目标”阶段被识别;

因为阻止了攻击者执行攻击生命周期 (Kill chain) 中的任意阶段, 所以攻击基本不会成功。

## Botnet C&C URL 被 SIEM 系统监测

就本实例而言, 假设攻击已经到了“指挥与控制”阶段。

当安全团队中的成员接收到了来自 SIEM 系统的安全事件触发器, 安全事件响应进入“鉴别”阶段。

Event Name	Log Source	Event Count	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

这种情况下, 组织内部网络向 C&C 服务器发送请求。安全团队的成员应将该事件归类为安全事件触发器, 因为应急响应指南中介绍了此类事件基本上都是安全事件触发器。

## 步骤三：控制（Containment）

本节介绍了安全事件响应阶段中的“控制”阶段实例。

## 鉴别受感染计算机

向 C&C 服务器发送请求是一种主动攻击的表征。这种情况下, 最首要的是鉴别受感染计算机并将其隔离在一个与组织内部网络和互联网分离的网络环境中。

为了鉴别受感染计算机, 安全团队须在 SIEM 系统中搜索所有与 Botnet C&C URL 发送请求相关的事件。组织网络环境内所有发出这种请求的计算机都可以被判断为受感染。

正如安全事件响应步骤所述 (见 8 页), 收集 IOC 是个循环过程。在本实例的后面, 安全团队会使用卡巴斯基威胁情报门户解决方案 (Kaspersky Threat Intelligence Portal solution) 的哈希服务来分析 Botnet C&C URL。安全团队获取该恶意软件的哈希值 (hash), 并与该 Botnet URL 关联起来。这些哈希值 (hash) 是补充 IOC, 用于确定其他受感染计算机。下一步需要获取更多的 IOC, 并通过已获取的 Botnet URL 列表和恶意软件的哈希值 (hash) 鉴别更多受感染的计算机。这些额外附加的 URL 可能是其他恶意 URL 和 Botnet C&C 的 URL。



## 隔离受感染计算机

安全团队可在组织的路由器上使用防火墙（iptables），隔离受感染计算机。

例如，受感染计算机的 IP 地址是 192.168.0.3。在组织的路由器上执行下列命令，可防止受感染计算机在网络中发送和接收任何数据。

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

安全团队会将受感染计算机访问的 Botnet C&C URL 地址添加到黑名单中。如果组织网络环境中仍存在其他未被识别到的受感染计算机，它们也无法与 C&C 服务器建立连接。

## 鉴别攻击载体（attack vector）

为了鉴别攻击载体（attack vector），安全团队应分析 QRadar SIEM 系统里所有与受感染计算机相关联的事件（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

在本实例中，最早发生的事件是与 IP 威胁库（KL\_IP\_Reputation）做比对。攻击者用于发起鱼叉式钓鱼攻击的邮件的服务报头中包含一个 IP 地址，该 IP 地址与卡巴斯基实验室的威胁库中的内容相匹配。IP 威胁库包含与垃圾邮件和钓鱼邮件相关的 IP 地址。这就意味着本次攻击会以发送钓鱼邮件给银行内部员工的方式开始。

通常，与这些 IP 地址的通信会被组织的防御措施阻断。但就本实例而言，假定并未对该事件（event）进行响应。

对事件进行进一步调查后，安全团队发现了攻击者的邮件。现在安全团队可以分析这些邮件并进一步调查攻击者使用的利用程序（Exploit）。不仅如此，安全团队还可以通过寻找这些邮件的所有收件人，确认其他可能受感染的目标计算机，并防止员工创建利用程序（Exploit）。

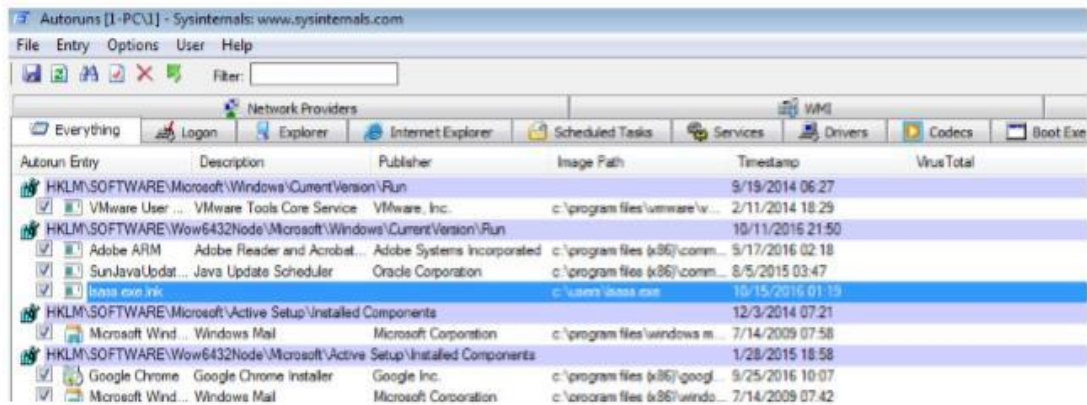
# 分析恶意软件

受感染计算机被隔离后，安全团队应继续进行调查并分析该受感染计算机。

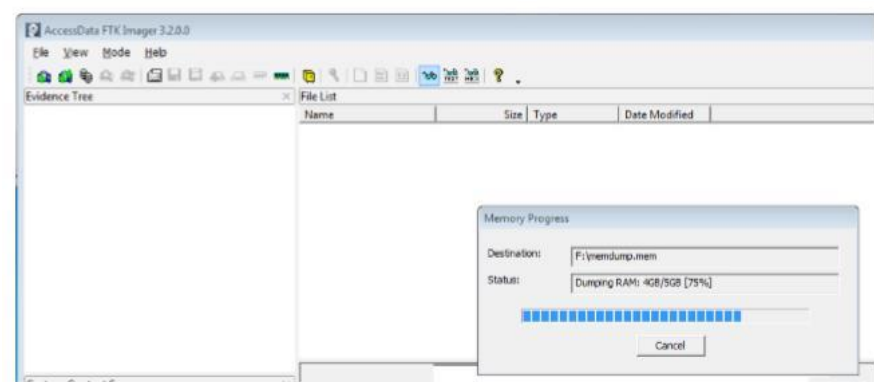
安全团队可以使用卡斯基威胁情报门户解决方案（Kaspersky Threat Intelligence Portal solution）的威胁检索服务来获取与 Botnet C&C 地址相关的信息。这些信息包括与这些 URL 相关联的恶意软件的哈希值（hash）和描述。

就本实例而言，假定安全团队并没有使用卡斯基威胁情报门户解决方案（Kaspersky Threat Intelligence Portal solution）的威胁检索服务。相反，安全团队试图通过 Microsoft Sysinternals 和 Volatility 工具中的 Autoruns 获取被攻击者利用的恶意软件相关的信息。（见 47 页）

如果安全团队可以直接访问受感染的计算机，那么安全团队成员会运行 Autoruns 工具。



Autoruns 工具帮助安全团队成员在 C 盘 user 目录下找到了一个可疑的文件 lsass.exe。这类启动项的存在极有可能不是银行员工应用于工作站的。如果安全团队无法直接访问受感染计算机，那么应由具有访问权限的员工遵照安全团队的指示创建受感染计算机的内存副本，并发送给安全团队。AccessData Forensic Toolkit（见 43 页）可用于创建内存副本。



安全团队获取了内存副本之后，安全团队成员应使用 Volatility 工具（见 47 页）获取

受感染计算机的进程列表。

```
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
0xffffffff8004ca9b30	lsass.exe	516	404	8	847	0
0xffffffff8004cadb30	lsass.exe	524	404	10	189	0
0xffffffff8005b37660	explorer.exe	1976	1916	33	992	1
0xffffffff8005ce4b30	lsass.exe	2336	1976	10	231	1
0xffffffff8005ceab30	svchost.exe	2348	508	14	334	0

Volatility 工具输出显示两个 lsass.exe 进程。其中一个 lsass.exe 进程的 PID 是 516，PPID 是 404，这意味着该进程是由 wininit.exe 启动的。另一个 lsass.exe 进程的 PID 是 2336，PPID 是 1976，这意味着该进程是由 explorer.exe 启动的。第二个 lsass.exe 进程非常可疑，因为 explorer.exe 进程是 Windows Explorer 的一部分，并不是用来运行系统进程的。

一旦恶意软件（lsass.exe）被识别，安全团队须确保该软件的确是用来响应 C&C 服务器的。安全团队成员应对恶意软件进行静态分析，并使用 Strings 功能查找 lsass.exe 文件对应的 C&C 服务器 URL。

Strings 功能的参数之一是符号的长度。安全团队成员应使用 lsass.exe 文件的不同值进行扫描，以便从该文件中获取 ASCII 和 Unicode 字符串。

通过使用 Strings 功能的具体参数，安全团队成员可获得下列输出（fragment）：

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

f:\dd\vc\tools\crt\crtw32\dllstuff\atexit.c

>"g/

BSJB

v4.0.30319

#Strings

#GUID

#Blob

~,#
```

安全团队成员通过 EL（expression Language）表达式作为参数查找 Unicode 字符串、指定 16 位字符串。其结果为下列输出（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 ---
```

这个地址（[http://subbotnet-domain\\_19.botnet-domain.example.com/page/c](http://subbotnet-domain_19.botnet-domain.example.com/page/c)）是被 SIEM 系统检测到的 Botnet C&C URL。

分析恶意软件的最后一步是将恶意软件的样本发送给防病毒软件公司。在本实例中，安全团队将恶意软件样本发送给卡巴斯基实验室。

Send	To...	<input type="checkbox"/> newvirus@kaspersky.com
	Cc...	
	Subject	New malicious software sample
	Attached	lsass.exe.zip (53 KB)

Hello,

A sample of malicious software was detected in the corporate network of our organization. The software attempted to interact with a known Botnet C&C URL ([http://subbotnet-domain\\_19.botnet-domain.example.com/page/c](http://subbotnet-domain_19.botnet-domain.example.com/page/c)).

Please analyze the attached sample and issue an anti-virus database update.

The password for the attached archive is "infected".

----

WBR,  
Chief Security Officer of the Bank

卡巴斯基实验室的专家将分析接收到的样本，进而更新终端防病毒设施的数据库。这将有助于保护其他计算机将来免于感染此类软件。

## 动态分析利用程序（Exploit）和攻击荷载（Payload）

当攻击载体（attack vector）被识别出来时，利用程序（Exploit）一定会被安全团队发现。

安全团队分析攻击者使用的邮件附件，安全团队成员可使用卡巴斯基威胁情报门户解决方案（Kaspersky Threat Intelligence Portal solution）的沙箱服务（见 46 页）动态分析利用程序（Exploit）。作为备选，他们可以使用隔离的虚拟机执行动态分析。

动态分析利用程序（Exploit）有助于确定利用程序（Exploit）的行为。利用程序（Exploit）安装装载软件并试图下载恶意软件。

安全团队也会分析被利用程序（Exploit）下载的恶意软件。该分析可确认恶意软件试图访问 C&C 服务器的行为。

## 结果

通过隔离受感染计算机，安全团队能够终止攻击。对受感染计算机和恶意软件的进一步分析，有助于安全团队重建攻击防御计划：

- 本次攻击是通过鱼叉式钓鱼邮件发起的；
- 利用程序（Exploit）是 PDF 文件，它通过安装装载软件感染计算机；
- 装载软件试图下载 BOT 软件；
- 恶意软件试图与 C&C 服务器建立连接。这类连接被安全团队发现并添加到 C&C 服务器 URL 黑名单中；

结果，攻击被终止了，并未造成任何损失。银行管理层决定没必要向执法部门报备这起攻击事件。安全团队进入“根除”阶段。

## 步骤四：根除与复原（Eradication and Recovery）

本节介绍了安全事件响应阶段中的“根除”与“复原”阶段实例。

安全团队从受感染计算机中移除恶意软件。组织网络环境中的所有计算机均须使用安全

团队发现的 IOC 进行扫描检查。这次扫描并未发现其他受感染的计算机。

组织的路由器被重新配置,以便之前受感染计算机可以从银行网络和互联网上发送和接收数据。

例如,恢复该受感染计算机在银行网络环境内的 IP 地址,可执行下列命令:

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

## 步骤五：经验总结（Lessons learned）

安全团队汇总关于本次安全事件的报告。所有本次安全事件响应过程中获取的 IOC（IP 地址、URL、哈希值等）均须汇总并添加到组织的安全控件的黑名单中。安全团队应以银行员工为对象,针对不可信来源邮件处理的安全规程,开展信息安全培训。

## 第四章 推荐的工具与功能

本章介绍了用于安全事件响应的实用工具与功能。

本章介绍的工具与功能并不是所有用于安全事件响应的总列表。根据安全事件，其他的安全软件也可被应用于调查。

本章介绍的工具与功能是由第三方公司开发的。卡巴斯基实验室并不负责第三方软件的可操作性和质量。这些工具与功能的详情可再第三方公司的网站查询。

### 第一节 搜集 IOC 的工具介绍

本节介绍了用于搜集 IOC 的工具与功能。

#### Sysinternals

Sysinternals 是一套用于管理和监控计算机上 Microsoft Windows 运行状况的工具。Sysinternals 组件包含超过 60 个功能。

建议使用 Sysinternals 搜集 IOC 和分析受感染计算机。

Sysinternals 功能可从本地地址下载：

<https://technet.microsoft.com/en-us/sysinternals/default.aspx>

#### PsTools

PsTools 是由一套命令行组成的功能，可用于远程执行进程（PsExec），列出进程的详细信息（PsList），通过名字和进程 ID 终止进程（PsKill），查看和控制服务（PsService）。PsTools 也包含重启和关闭计算机的功能，副本系统事件记录和任务。

#### Process Monitor

Process Monitor 是个实时监控进程的功能。该功能可监控注册表和文件系统的活动，并获取进程、网络活动和输入/输出（I/O）操作的相关信息。



## Process Explorer

Process Explorer 是用于控制进程并实时获取进程活动信息的工具。

Process Explorer 可执行下列操作:

- 获取当前活动进程的详细信息；
- 终止、暂停、恢复进程；
- 获取进程打开或加载的句柄（handle）和动态链接库（dynamic-link libraries, DLL）信息；
- 创建内存副本（memory dump）并保存成文件。

## Autoruns

Autoruns 功能用于展示那些在系统启动和登录时执行的程序，也包括 Windows 内置的应用程序，如 Internet Explorer、Windows Explorer 和 media player 等。本功能还可以启动或禁用这些程序的自主运行。

本功能支持对自主运行对象（VirusTotal）的哈希值（hash）的检查。未知文件可被送至防病毒软件公司进行分析。

**AVZ**

AVZ 功能可用于分析和恢复。

	File	Startup method	Description	Type
Autostart				
Autostart folders				
All users, Common	C:\Program Files\Microsoft Windows\CurrentVersion\Autostart\AllUsersCommon	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Autostart\AllUsersCommon	Registry key
All users, Common	C:\Program Files\Microsoft Windows\CurrentVersion\Autostart\AllUsersCommon	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Autostart\AllUsersCommon	Registry key
Users, Startup	C:\Program Files\Microsoft Windows\CurrentVersion\Autostart\UsersStartup	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Autostart\UsersStartup	Registry key
Users, AllStartup	C:\Program Files\Microsoft Windows\CurrentVersion\Autostart\UsersAllStartup	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Autostart\UsersAllStartup	Registry key
Registry				
Run*	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
System keys	C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE15\msoext.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Service/Service	C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE15\msoext.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Terminal/Server	C:\Program Files (x86)\Kaspersky Lab\Kaspersky EndPoint Security 10 for Windows\Kaspersky.exe	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Shared Task Scheduler	C:\Program Files (x86)\Microsoft Office\Office15\NAMEEXT.DLL	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Shell/Execute/Hot	C:\Program Files (x86)\Microsoft Office\Office15\NAMEEXT.DLL	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Applet/Tools	C:\Program Files\7-zip\7-zip.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Windows Script	C:\Program Files\Microsoft Office\Office15\msoext.dll	Registry key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
File	C:\Program Files\Realtek\Audio\DRIVER\RealtekAudio.exe	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Network	C:\Program Files\Windows Sidebar\sidebar.exe	Registry key	HKEY_USERS\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Remote/Access	C:\Program Files\Windows Sidebar\sidebar.exe	Registry key	HKEY_USERS\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Time/Providers	C:\Windows\COMSMG\GFC.exe	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
Win/True	C:\Windows\Microsoft.NET\Framework64\6.0.60728\aspnet_regapi.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\ASP.NET\2.0.50728\64	Registry key
Open/CD/Drivers	C:\Windows\Microsoft.NET\Framework64\6.0.60728\aspnet_regapi.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\ASP.NET\4.0.30319\64	Registry key
Device/32	C:\Windows\Microsoft.NET\Framework64\6.0.60728\aspnet_regapi.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\ASP.NET\2.0.50728\64	Registry key
Device/32/Terminal	C:\Windows\Microsoft.NET\Framework64\6.0.60728\aspnet_regapi.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\ASP.NET\4.0.30319\64	Registry key
ASIR	C:\Windows\Microsoft.NET\Framework64\6.0.60728\aspnet_regapi.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
ASIR	C:\Windows\Microsoft.NET\Framework64\6.0.60728\aspnet_regapi.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key
ASIR	C:\Windows\Microsoft.NET\Framework64\6.0.60728\aspnet_regapi.dll	Registry key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Registry key

在安全事件响应过程中获取信息时建议使用 AVZ 功能。本功能包含下列模块：

- 进程管理器 (Process manager)



- 服务与驱动管理器 (Services and drivers manager)
- 内核模块 (Kernel space modules)
- Winsock SPI (LSP, NSP, TSP)管理器 (Winsock SPI (LSP, NSP, TSP) manager)
- 分析开放式 TCP 和 UDP 端口的模块 (Module for analyzing open TCP and UDP ports)
- 自启动管理器 (Autoruns manager)
- IE 扩展管理器 (Internet Explorer extensions manager)
- Windows Explorer 扩展管理器 (Windows Explorer extensions manager)
- Microsoft Windows Control Panel (CPL) 程序管理器 (Microsoft Windows Control Panel (CPL) applets manager)
- 打印系统扩展管理器 (Printing system extensions manager)
- 任务调度作业管理 (Task Scheduler jobs manager)
- 注入 DLL 管理器 (Injected DLLs manager)
- 协议和处理程序管理器 (Protocols and handlers manager)
- Windows 活动安装管理器 (Windows Active Setup manager)
- 主机文件管理器 (Hosts file manager)
- 共享资源和网络会话管理器 (Shared resources and network sessions manager)

AVZ 功能可从本地址下载:

<http://www.z-oleg.com/secur/avz/download.php>

## GMER

GMER 是个发现并移除后门程序 (rootkits) 的功能。

GMER 主要扫描的内容如下:

- 隐藏进程 (Hidden processes)
- 隐藏线程 (Hidden threads)
- 隐藏模块 (Hidden modules)
- 隐藏服务 (Hidden services)
- 隐藏文件 (Hidden files)
- 隐藏磁盘扇区 (Hidden disk sectors)

- 隐藏注册表键值 (Hidden registry keys)
- 内核模式驱动 hook (Kernel mode driver hooks)

GMER 功能可从本地址下载:

<http://www.gmer.net>

## YARA

YARA 是用于帮助病毒研究人员分析和分类恶意软件样本的工具。YARA 是一个多平台的解决方案,可运行在 Windows、Linux 和 Apple Mac OS X 系统上。YARA 可通过命令行接口和 Python 脚本与 YARA Python 扩展配合使用。

运用 YARA,病毒研究人员可基于文本和二进制模式创建恶意软件的相关描述。每个描述(也称为规则)是由决定该恶意软件的逻辑的一组字符串和布尔表达式组成。

下面是一个 YARA 规则的实例。任意文件中只要包含三个字符串中的一个,就必须报告为一个威胁。

```
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 功能可从本地址下载:

<http://virustotal.github.io/yara>

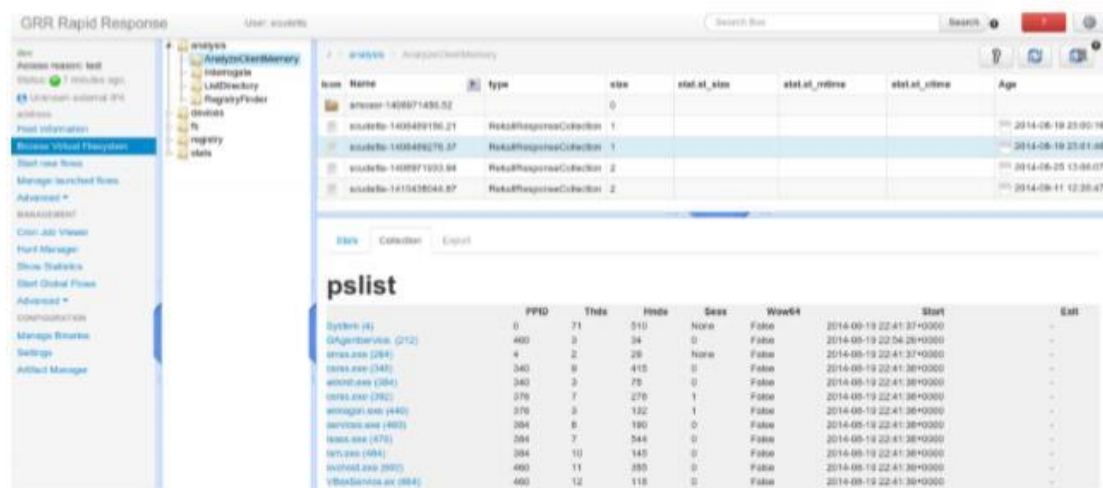
## 第二节 创建副本 (Dump) 的工具介绍

本节介绍了用于创建内存和硬盘副本的工具与功能。

## GRR Rapid Response

GRR Rapid Response 在安全事件响应过程中用于远程现场取证。

GRR Rapid Response 采用 CS 结构。客户端安装在工作站，并用于采集数据。服务器端用于存储和分析采集到的数据。



GRR 的主要功能如下：

- 运用 ReKall 功能远程分析 Windows 操作系统的内存和系统注册表。
- 运用 Sleuth Kit 功能远程分析硬盘空间

GRR Rapid Response 功能可从本地址下载：

<https://github.com/google/grr>

## Forensic Toolkit

Forensic Toolkit (FTK) 是一套数字取证的工具。Forensic Toolkit 包含 FTK 镜像功能，可用于创建内存和硬盘的副本。

FTK 支持多种查看硬盘副本的选项。例如，有一个“Spreadsheets”功能，可展示所有电子表格清单和每个电子表格的相关描述及本地位置。FTK 有一个用于查找 IOC 的关键字列表。

Forensic Toolkit (FTK) 功能可从本地址下载：

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

## DD

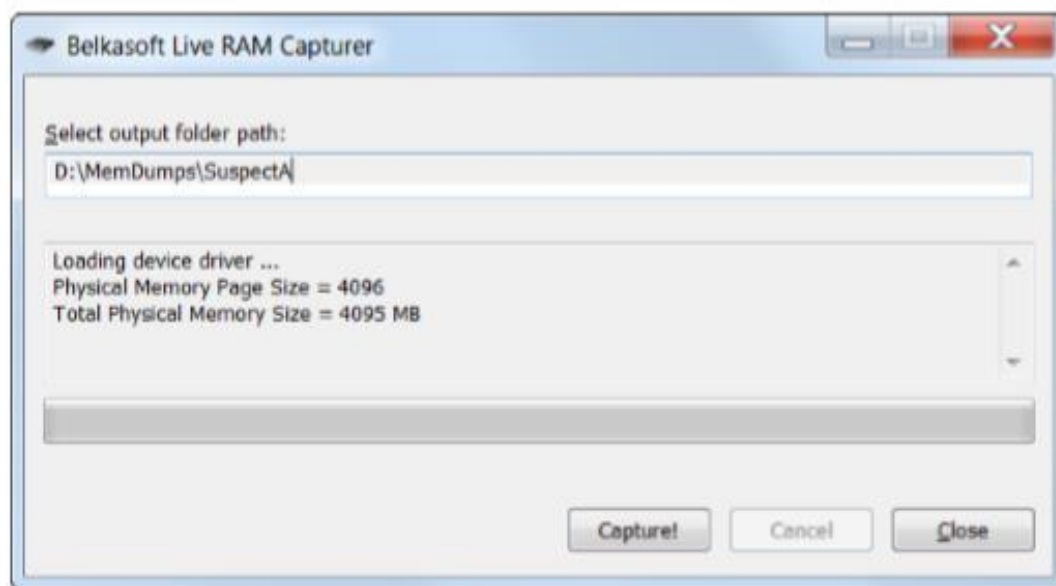
DD (dataset definition) 工具是适用于 Unix 和 Unix-like 操作系统的一个命令行功能。主要目的是转换和复制文件。

DD 工具可用于复制硬盘扇区，其中包含未被操作系统使用的扇区空间。例如，你可以使用 DD 工具做一个硬盘启动扇区的备份。

DD 工具适用于所有 Linux 系统的发行版本。DD 工具可植入到微软的 Windows 系统作为 Cygwin 的一部分。可从本地址下载：<https://cygwin.com>

## Belkasoft RAM Capturer

Belkasoft RAM Capturer 是个免费的取证工具，适用于创建微软的 Windows 系统的内存副本。所创建的内存副本会以文件的形式保存下来。



Belkasoft RAM Capturer 分为 Windows 32 位 64 位两个版本。这两个版本运行在内核模式下，并且允许获取受保护进程所使用的内存区域。

Belkasoft RAM Capturer 可从本地址下载：

<http://belkasoft.com/ram-capturer>

## 第三节 分析的工具介绍

本节介绍了用于分析潜在威胁和软件样本的工具与功能。

威胁分析需要大量的专业知识与实践。建议使用本节推荐的工具进行初步分析。然而，如果是个 ATP 攻击，最好交由专家分析。

### 卡巴斯基威胁情报门户（Kaspersky Threat Intelligence Portal）

卡巴斯基威胁情报门户是集成多个卡巴斯基实验室服务的安全设施。

- **威胁检索**

卡巴斯基威胁检索服务提供了卡巴斯基实验室获取的有关网络威胁及与其相关的所有知识，并汇集成一个强大的服务。目的在于为安全团队提供尽可能多的数据，在对组织造成影响前，防止网络攻击。本项服务可检索与威胁相关的最新详细情报。如，网址、域名、IP 地址、哈希值、威胁名称、统计与行为数据、查询数据和 DNS 数据。检索结果包含全球最新出现的威胁信息，有助于提高安全事件响应的有效性，从而更好的保护组织免遭攻击。

- **Whois 追踪**

本项服务通过特定的 WHOIS 数据搜索条件查找域名和 IP 地址。这类条件可能是域名联系人或域名创建日期。WHOIS 数据的特定领域可自动定期提交满足搜索条件的搜索记录。通过自动邮件通知的形式，可将 WHOIS 数据库中满足搜索条件的新纪录发送给特定的收件人。

- **APT 报告**

本项服务有助于提高对高知名度网络间谍活动相关的认知与相关知识。并且可提供综合性的卡巴斯基实验室实践报告。

- **数据库（卡巴斯基实验室威胁库）**

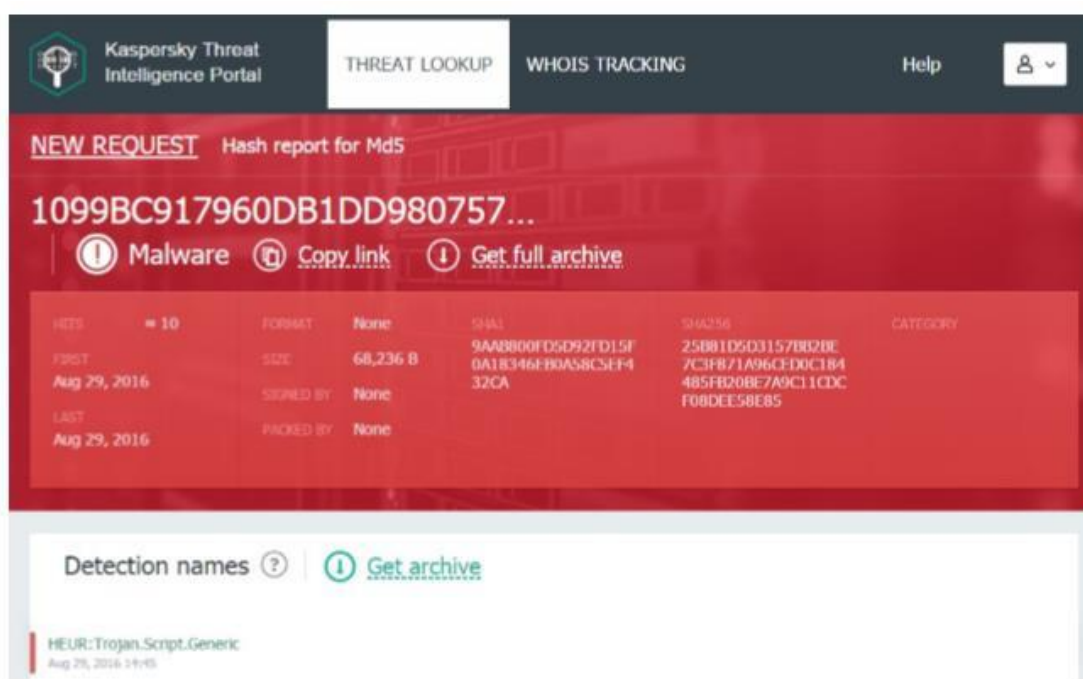
卡巴斯基实验室持续提供并更新威胁情报资料给组织和客户。以便更高效的减小威胁程度，在威胁发生前做好防范。数据库是由 JSON、CSV、OpenIOC、STIX 格式构成。并可接入 SIEM 系统。如，Splunk、HPE ArcSight、IBM QRadar、EMC RSA NetWitness、LogRhythm、McAfee Enterprise Security Manager (ESM)。

- **Sandbox**

本项服务是一个创新的、全自动化的文件分析系统，用于检测未知和高级的威胁。该服务可将文件上传至安全环境并进行深入动态分析，从而进一步调查收集综合的文件行为日志。本技术的优点不仅仅是可以分析潜在的恶意代码、采取创新的方式解决不同类型的迂回技术，还可以直观的提供 SOC、CERT 和 DFIR 的相关报告，以便提高安全事件响应的效率。

## Threat Lookup

威胁检索是卡巴斯基威胁情报门户的一部分。该服务提供网络攻击相关的威胁情报，以及网络攻击、正规对象和 IOC 之间的关联。



威胁检索服务支持执行下列事项：

- 通过向安全团队提供威胁相关的有效信息来改进并提升安全事件响应和取证能力，从而全面的洞察到目标攻击背后隐藏的信息。安全事件可以越来越高效的被诊断和分析；
- 通过人工威胁校验的方式对 IOC（如 IP 地址、恶意 URL、文件的哈希值等）进行更深入的检索。可根据攻击事件的优先级进行 IT 工作人员和相关资源分配；
- 通过调整防御策略和反击目标攻击，依据至关重要的威胁情报，加强安全体系结构。

通过使用威胁检索，安全团队可以获取 IOC 相关的更多信息。这些信息可用于监测尚未被录入到安全控件的威胁。例如，一个未知的恶意软件可以被监测到，因为与之协作的 C&C

服务器的 URL 是已知的。

## Sandbox

卡巴斯基威胁情报门户（TIP）提供了一项功能，可在沙箱环境中动态分析威胁和软件样本。该功能可以监测威胁、报告其行为并从中获取新的 IOC。

通过向威胁情报门户（Threat Intelligence Portal）发送相关的文件、URL 和哈希值等信息，TIP 沙箱中的软件样本可被进行深入分析。该软件分析可产生行为报告以及分析过程的相关信息。这些信息包括用于分析样本网络活动的 PCAP 文件和由样本修改、创建的文件。

## APT 报告

卡巴斯基实验室的 ATP 报告可用于防御 APT 攻击。

订阅 APT 报告可以持续访问卡巴斯基实验室进行的调查及其相关信息，包括每个 APT 的各种格式的完整技术数据。（包括 YARA 和 OpenIOC 格式）。

## 获取卡巴斯基威胁情报门户

获取卡巴斯基威胁情报门户，可联系 [intelligence@kaspersky.com](mailto:intelligence@kaspersky.com) 或访问 <http://www.kaspersky.com/enterprise-security/intelligence-services>。

## 第四节 分析内存副本的工具介绍

本节介绍了用于分析内存副本的工具与功能。

### Volatility

Volatility Framework 是从内存样本中取证的一个功能。该功能适用于 Linux、Windows 和 Mac OS X 操作系统。

Volatility 支持下列内存副本类型：

- 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 的发行包大约有 150 个插件。通过使用这些插件，安全团队可以获取进程加载的调用树和 DLL 的相关信息。例如，Devicetree 插件可用于获取所有设备和相关驱动件的列表。通过这个列表可以查找到 rootkit 使用的驱动。

下面的实例演示了 Volatility 是如何获取到 DLL 模块列表。

```
$ 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 工具可以从内存副本中将进程保存成可执行文件。这些文件可进行静态或动态分析。例如，在卡巴斯基威胁情报门户的沙箱中进行动态分析。利用 Strings 功能进行静态分析。

Volatility Framework 功能可从本地址下载：

<http://www.volatilityfoundation.org>

## Rekall

Rekall 是一个内存分析工具。



Rekall 有三个接口: 命令行, 基于 IPython 的交互式命令行和 web 接口。如同 Volatility, Rekall 有很多插件。例如, pslist 插件可以输出系统中运行的所有进程列表; hooks\_inline 插件可以查找到所有存在 Hook (截获的函数调用) 的库。Windows 操作系统里的内存副本可以通过 Rekall 中的 winpmem 功能进行创建。

Rekall 既可以分析内存副本也可以分析运行中的操作系统内存。这意味着 Rekall 不需要创建内存副本也可以进行分析。

下面的实例演示了 Rekall 是如何分析内存副本。

```
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 功能可从本地址下载:

## 第五节 分析硬盘副本的工具介绍

本节介绍了用于分析硬盘副本的工具与功能。

### The Sleuth Kit (TSK)

The Sleuth Kit (TSK)是将命令行工具和 C 语言库相结合工具，用于分析硬盘副本并从中复原文件。

TSK 的命令行工具可用于执行下列操作：

- 列出分配、删除的 ASCII 和 unicode 文件名；
- 显示所有 Windows NT 文件系统属性相关的详情；
- 展示文件系统和元数据结构详情；
- 创建文件活动的时间轨迹 (time-line)，可以将其导入到扩展表中，以便创建图表和报表；
- 在哈希 (hash) 数据库中查找文件哈希值；
- 根据文件类型组织规划文件。页面缩略图可以制成图像用于快速分析。

Autopsy 是 TSK 中基于 GUI 的程序。它为 TSK 功能提供 GUI。

TSK 功能可从本地址下载：

<http://www.sleuthkit.org/sleuthkit/>

Autopsy 可从本地址下载：

<http://www.sleuthkit.org/autopsy/>

### RegRipper

RegRipper 是用于注册表分析的取证工具。

RegRipper 用于提取特定的注册表键、数值和硬盘副本中的数据。RegRipper 包含大约 300 个插件。

下面的实例演示了 RegRipper 获取的有用信息。

```

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 功能可从本地址下载:

<https://github.com/keydet89/RegRipper2.8>

## Strings utility

Strings 是应用于 Unix 和 Unix-like 操作系统的命令行功能。Strings 可用于搜索二进制文件中的 Unicode 和 ASCII 字符串。这类字符串可用于 IOC 和软件样本行为的静态分析。

本项功能可以在副本文件中搜索字符串，以获取样本软件的更多信息。

Strings 功能可植入到微软的 Windows 系统作为 Cygwin 的一部分。可从本地址下载:

<https://cygwin.com>

## 第六节 根除的工具介绍

本节介绍了用于“根除”阶段的工具与功能。

## Kaspersky Virus Removal Tool

Kaspersky Virus Removal Tool 是款用于扫描和查杀恶意软件的免费工具，适用于微软的 Windows 操作系统。该工具可通过命令行使用。

Kaspersky Virus Removal Tool 有如下功能：

- 检测和根除恶意软件；
- 检测可能侵害计算机或窃取敏感数据的广告软件及其他正规软件。

本项功能无法持续的执行保护。Kaspersky Virus Removal Tool 并不更新其自身的防病毒数据库。为了使用最新的数据库，须下载最新版本的 Kaspersky Virus Removal Tool。

受感染计算机被 Kaspersky Virus Removal Tool 查杀完毕后，需要安装卡巴斯基安全终端进行持续保护。

Kaspersky Virus Removal Tool 功能可从本地址下载：

<https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool>

用于根除多种类型的恶意软件的其他免费功能，可访问本地址：

<http://support.kaspersky.com/viruses/utility?CID=acq-freekasp->

USA&\_ga=1.198229483.57166196 7.1434556259

## Kaspersky Rescue Disk

Kaspersky Rescue Disk 可用于扫描、查杀、复原受感染操作系统。也适用于无法启动操作系统的情况。

Kaspersky Rescue Disk 可以高效的删除恶意软件，因为操作系统无法启动且恶意软件无法获取系统的控制权限。

Kaspersky Rescue Disk 功能可从本地址下载：

<https://support.kaspersky.com/viruses/rescuedisk>