# 案例研究

In order to test our method, a small Hadoop cluster using Virtual Box including one master node and 15 slave nodes is set up. The node environment is an i5-4590 3.3 GHz 2G Ubuntu 12.04 and Hadoop Version is 1.2.1.

为了测试我们提出的方案，在Virtual Box虚拟机上安装了有一个主节点和15个从节点的小型Hadoop群。（被动句转换为主动）这些节点配置的环境为：i5-4590 3.3GHz的CPU，2G内存版本为12.04的Ubuntu系统，版本1.2.1的Hadoop。

## 应用层面的数据泄露研究

We first conduct an investigation at the Hadoop application level. Suppose attackers stole a secret file named star-project.txt using a legal account. As we mentioned before, the Hadoop audit log cannot record the operator and there might be CSP employees who are authorized to modify the Hadoop logs and the Fsimage, so both the Hadoop logs and Fsimage may be contaminated. However, this case can be investigated based on the HProgger log, the Hadoop log, and the Fsimage according to following steps.

我们首先在Hadoop的应用层开始研究。假设攻击者使用合法帐户窃取了一个名为star-project.txt的秘密文件。像之前讲到的，由于Hadoop的审计日志无法记录操作者，并且有CSP工作人员被授权修改Hadoop日志和Fsimage的可能，这将可能会导致Hadoop日志和Fsimage被污染。（逻辑）但是，可以根据以下基于HProgger日志、Hadoop日志和Fsimage的步骤来调查这种情况。

**Step 1.** Find corresponding block IDs by file name in the Hadoop logs that come from the name node. The records show that block 8241916282566986668 belongs to the file star-project.txt.

**步骤1.** 在来自名称节点的Hadoop日志中按文件名查找相应的块id。记录显示块8241916282566986668属于文件star-project.txt。

**Step 2.** In application-level attacks, criminals access data through Hadoop commands, e.g. some Hadoop shell commands for file operations, such as CopyToLocal, so we can filter out this type of record from the HProgger logs. In this case, we can know from the filtered logs that in 21:04:28, User Alice used the CopyToLocal command to copy a file to a local machine, renamed it to abc.txt, and put it to /home/Alice. However, we cannot confirm that abc.txt is star-project.txt.

**步骤 2.** 在应用层面的攻击中，罪犯者通过Hadoop命令访问数据，比如一些用于文件操作的Hadoop shell命令，CopyToLocal就为其中之一，因此我们可以从HProgger日志中筛选出这种类型（命令）的记录。在这种情况下，我们可以从筛选的日志中得知，在21:04:28，用户Alice使用copy to local命令将文件复制到本地计算机，并将其重命名为abc.txt，然后将其放到/home/Alice目录下。但是，我们不能确定abc.txt是否为star-txt。

**Step 3.** Find the records containing the investigated file name or block IDs around the key records found in Step 2 in the HProgger logs, then obtain the timestamp of this operation. For example, we found a record showing that block 8241916282566986668 was opened in 21:04:28, and this record is just the former one of the key records we found in Step 2.

**步骤 3.** 在HProgger日志的步骤2中关键记录的周边进行搜索，找到包含所调查文件名或块id的记录，然后获取此操作的时间戳。例如，我们发现一条记录，显示块8241916282566986668在21:04:28打开，而这条记录只是我们在步骤2中找到的前一条关键记录。

**Step 4.** Search the records in the Hadoop logs according to the timestamps and block ID we found in the above steps. The results show that in 21:04:28, a HDFS\_READ was executed on block 8241916282566986668 and there were no other records at the same time. This record and the two records we found in HProgger can prove to each other that the criminal is User Alice. She copied star-project.txt to local by CopyToLocal and renamed it abc.txt.

**步骤 4.** 根据上面步骤中找到的时间戳和块ID搜索Hadoop日志中的记录。结果表明，在21:04:28，在块8241916282566986668上执行HDFS\_READ，同时没有其它（操作）记录。这个记录和我们在HProgger找到的两个记录可以相互证明罪犯是用户Alice。她通过CopyToLocal命令将star-project.txt复制到本地，并将其重命名为abc.txt。

In conclusion, Alice is the attacker. We can conduct second-stage forensics and find more information about this attack, for example, obtaining the network traffic in that node to detect whether Alice transmitted this file to another location. However, if attackers tampered with the Hadoop logs from the data node or the name node, how do we investigate such a case?

综上所述，Alice是攻击者。我们可以进行第二阶段的取证，以找到更多关于此攻击的信息，例如，通过获取该节点的网络流量去检测Alice是否将此文件传送到另一个位置。但是，如果在攻击者篡改了数据节点或名称节点的Hadoop日志的情况下我们该如何调查？

Hadoop logs from the data node are tampered with: In this case, we cannot obtain the relevant record from the Hadoop logs as was done in Step 4. However, any changes to the file or directory can be detected by HProgger. If we set HProgger to monitor /usr/local/hadoop/logs/, which is the directory where Hadoop logs are stored, we can find the illegal tampering from attackers.

数据节点中的Hadoop日志被篡改：在这种情况下，我们无法像步骤4中所做的那样从Hadoop日志中获取相关记录。但是，HProgger可以检测到对文件或目录的任何更改。如果我们设置HProgger作为监视器去监控/usr/local/hadoop/logs/这个存储hadoop日志的目录，我们就可以找到来自攻击者的非法篡改。

Hadoop logs from the name node are tampered with: In this case, we cannot obtain the block ID based on file name as was done in Step 1. Fortunately, we can obtain this relation from the Fsimage. That is why the data collector collects the Fsimage from each node.

名称节点中的Hadoop日志被篡改：在这种情况下，我们不能像在步骤1中那样基于文件名获取块ID。幸运的是，我们可以从Fsimage中获得这种关系。这就是数据采集器从每个节点收集Fsimage的原因。

The Fsimage is broken: If the Hadoop logs and the Fsimage both cannot be trusted, how do we investigate such a case? In this situation, we can first obtain the Fsimage from the secondary name node, which is the backup for the name node and synchronizes with it periodically in most Hadoop environments. Second, we can use the old version of the Fsimage that was saved by the Fsimage file manager.

Fsimage已损坏：如果Hadoop日志和Fsimage都不可信，我们如何调查这种情况？在这种情况下，我们可以首先从次级名称节点获取Fsimage，它是名称节点的备份，并周期性地在大多数的Hadoop环境中同步。其次，我们可以使用Fsimage文件管理器保存的Fsimage的旧版本。

In conclusion, even if the Hadoop logs and Fsimage files are tampered with, the investigator can still find the attackers based on our method.

总之，即使Hadoop日志和Fsimage文件被篡改，调查者仍然可以根据我们的方法找到攻击者。

## 操作系统层面的数据泄露研究

In this section, we conduct an investigation at the operating system level. Suppose an attacker knew the location of a secret file companyA.7z from the name node logs or some other way. Then they could read this file directly from these data nodes by logging in to the host OS. Such an operation cannot be monitored by the Hadoop audit mechanism, but we can find this attacker based on the HProgger logs, the Hadoop logs, and the Fsimage according to the following steps.

在本节中，我们将在操作系统的层次进行研究。假设攻击者从名称节点日志或者通过其他方式知道机密文件companyA.7z的位置。然后他们可以通过登录主机操作系统直接从这些数据节点读取该文件。因为Hadoop的审查机制无法监控此类操作，所以我们需要通过基于HProgger日志、Hadoop日志和Fsimage的方法去找到此攻击者。（逻辑）

**Step 1.** Find the corresponding block IDs by file name in the Hadoop logs that are from the name node. Different from the first experiment, we obtained three block IDs, i.e., 4067922487609870000, 6299596445748830000 and 7132029012670650000. That is because companyA.7z is larger than 64 Mb, so it is divided into three blocks by Hadoop.

**步骤 1.** 在来自名称节点的Hadoop日志中按文件名查找相应的块id。与第一次实验不同，我们得到了4067922487609870000、6299596445748830000和7132029012670650000三个块id。这是因为companyA.7z大于64Mb，所以它被Hadoop分成三个块。

**Step 2.** Find the HProgger records by block ID. These records show that User Alice copied block 5255825402 465249432 from the Hadoop system directory to home/alice at 11:41:44. We find Alice did the same thing to two other blocks that belonged to companyA.7z, but in different data nodes. That is to say, Alice copied all the blocks of companyA.7z directly from the operating system in different machines. We can conclude that Alice stole companyA.7z. We can conduct a second-stage forensic investigation and find more information about this attack, e.g., obtain the network traffic in that node to detect whether Alice transmitted this file to another location.

**步骤 2.** 按块ID查找HProgger记录。这些记录显示，用户Alice在11:41:44将块5255825402465249432从Hadoop系统目录复制到home/Alice目录下。我们发现Alice对另外两个属于companyA.7z的块做了相同的操作，但是是在不同的数据节点中。也就是说，Alice直接从不同机器上的操作系统中复制了companyA.7z的所有块。我们可以得出结论Alice窃取了companyA.7z。我们可以进行第二阶段的调查，找到有关此攻击的更多信息，例如，通过获取该节点中的网络流量去检测Alice是否将此文件发送到另一个位置。

Similar to the first experiment, if the Hadoop logs cannot be trusted, we can obtain the mapping between the file and the block through the Fsimage, and if the Fsimage is broken, we can obtain the old version from the secondary name node or the Fsimage file manager.

与第一个实验类似，如果Hadoop日志不可信，我们可以通过Fsimage获取文件和块之间的映射，如果Fsimage被破坏，我们可以从次级名称节点或Fsimage文件管理器获取旧版本。

We have shown how to find attackers when the only clue is the name of the file that was stolen, but how do we find which file was stolen? Earlier an automatic detection algorithm was proposed. In order to test its efficiency, we run the algorithm every five minutes in our cluster (the frequency can be customized). Figure 3 and Figure 4 show the monitoring results of companyA.7z during a period of 30 minutes.

我们已经展示了如何在唯一线索是被盗文件名的情况下找到攻击者，但是如何寻找被盗的文件？早期提出了一种自动检测算法。为了测试它的效率，我们每五分钟在我们的集群中运行一次算法（频率可以定制）。图3和图4显示了companyA.7z在30分钟内的监控结果。

Figure 3 shows that all three dimensions of the file companyA.7z changed from 21:20 to 21:55, and all values of the three dimensions are greater than their normal value. For other files, the values of all dimensions remained unchanged the entire time.

图3显示从21:2至21:55，文件companyA.7z的所有的三个维度都改变，并且三个维度的所有的值都大于其正常值。对于其他文件，所有维度的值始终保持不变。

Figure 4 shows the AO values of all three blocks of the file companyA.7z growing to 7 or 8, both greater than the normal value 6. For the blocks of the other files, the values remained at 6 all the time. Hence, suspicious operations must have happened to companyA.7z during 21:20 to 21:55. So the detailed suspicious HProgger logs were found, which showed that Alice copied block 6299596445748830000 and block 713202901267065000 from /app/hadoop/tmp/ dfs/data/ current to /home/abc/, and she copied block 40679224 87609870000 to home/Alice and then to home/abc. All the blocks of companyA.7z were stolen by Alice.

图4显示了文件companyA.7z中所有三个块的AO值都增长到7或8，都大于正常值6。对于其他文件的块，值始终保持在6。因此，在21:20到21:55期间，companyA.7z中一定发生了可疑的操作。对此，我们发现了可疑的HProgger日志，其中显示Alice从/app/hadoop/tmp/dfs/data/current目录向/home/abc/目录复制了6299596445748830000块和713202901267065000块，并将40679224 87609870000块复制到home/Alice，之后将其复制到home/abc。至此companyA.7z所有的块都被爱丽丝窃取了。

# 结论

This article presents a forensic framework including an on-demand data collection method and an automatic analysis method for data leakage attacks in Hadoop. It collects data from the machines in the Hadoop cluster to our forensic server and then analyzes them. With the automatic detection algorithm, it can find out whether there exist suspicious data leakage behaviors and give warnings and evidence to users. This collected evidence can be used to find the attackers and reconstruct the attack scenarios. Some simulated investigating cases have shown its efficiency.

本文提出了一种基于Hadoop的检测框架，包括按需数据的采集方法和数据泄漏攻击的自动分析方法。它从Hadoop集群中的机器中收集数据到我们的判别服务器，然后对它们进行分析。利用自动检测算法，可以发现是否存在可疑数据泄露行为，并向用户发出警告和证据。收集到的证据可用于寻找攻击者和攻击场景的重建。一些仿真调查案例显示了其有效性。

# 翻译总结

1. 专业词汇、专有名词多

例如：Fsimage（Hadoop的日志镜像文件），Ubuntu（操作系统）

1. 论文句式简单，无复杂的长难句，但是句子间内涵逻辑联系。

As we mentioned before, the Hadoop audit log cannot record the operator and there might be CSP employees who are authorized to modify the Hadoop logs and the Fsimage, so both the Hadoop logs and Fsimage may be contaminated.

像之前讲到的，由于Hadoop的审计日志无法记录操作者，并且有CSP工作人员被授权修改Hadoop日志和Fsimage的可能，这将可能会导致Hadoop日志和Fsimage被污染。

（因为审计日志无法记录操作者，因此工作人员的修改操作导致日志被污染。）

In application-level attacks, criminals access data through Hadoop commands, e.g. some Hadoop shell commands for file operations, such as CopyToLocal, so we can filter out this type of record from the HProgger logs.

在应用层面的攻击中，罪犯者通过Hadoop命令访问数据，比如一些用于文件操作的Hadoop shell命令，CopyToLocal就为其中之一，因此我们可以从HProgger日志中筛选出这种类型（命令）的记录。

（e.g. 与such as 均为例如，但是两者之间存在从属关系。）

1. 主句从句之间合并翻译。

However, if attackers tampered with the Hadoop logs from the data node or the name node, how do we investigate such a case?

但是，如果在攻击者篡改了数据节点或名称节点的Hadoop日志的情况下我们该如何调查？

（将从句整合进主句）

1. 主被动转换

In order to test our method, a small Hadoop cluster using Virtual Box including one master node and 15 slave nodes is set up.

为了测试我们提出的方案，在Virtual Box虚拟机上安装了有一个主节点和15个从节点的小型Hadoop群。（被动句转换为主动）