



# **SANS Institute**

## **Information Security Reading Room**

### **Detecting Crypto Currency Mining in Corporate Environments**

---

Jan D&#039;Herd

Copyright SANS Institute 2019. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Detecting Crypto Currency Mining in Corporate Environments

*GIAC (GCIH) Gold Certification*

Author: Jan D'Herdt, jan.dherdt@gmail.com  
Advisor: Richard Carbone

Accepted: January 26, 2015

## Abstract

After many discussions amongst friends and colleagues about the opportunities of mining crypto currencies, one could start wondering what kind of corporate resources can be utilized in order to do crypto currency mining, and how a company can protect against this kind of threat.

Some will say that this is not a real threat for a company; however, some believe differently, which is explained in this paper. This research was performed, because there may be a need to professionally prepare and handle the misuse of corporate assets in order to avoid losses, both financially and operationally, in corporate environments.

As the installation and usage of crypto currency mining is both easy to use and setup, it is highly likely that there are many companies that have mining applications running in their environment without their noticing or knowing the financial and operational damage they may be causing. This paper will discuss how crypto currency mining can be done in corporate environments, and how it is possible to protect and defend against them.

# 1. Introduction

Crypto currencies [1] such as Bitcoin, Dogecoin, Primecoin, Litecoin, Riecoin and many others are digital currencies that do not follow the normal set of rules for currencies as we know them. Digital currencies, such as Bitcoin, are different as they wholly replace state-backed currencies with a digital version that is tougher to forge, cut across international boundaries, and can be stored on a local hard drive instead of in a bank. However, perhaps most importantly to users, digital currencies are not subject to the inflationary whim of whatever Central Bank or government decides to print more money [2].

Currencies, such as the U.S. Dollar, were once linked to gold, with every Dollar representing a certain amount of gold. If one is lucky and has the resources, a shovel for example, and a good location, one could mine his own gold. As gold can be mined, so too can digital currencies. The digital currency value is derived through their scarcity.

Techradar.com identified that mining programs compute an encryption function (a hashing function) on a set of random numbers. Coins are awarded every ten minutes to whichever miner happens to compute a number below a certain threshold. As the network gets bigger, the hash gets more complex, and miners get fewer coins for their trouble [3].

Mining is the process of using one's own computer's processing power, such as CPU [4] and GPU [5] to calculate hashes at immense speeds. These hashes are in place to generate integrity in the crypto currency network. Originally, miners used the CPU processing power to calculate the hashes, however, a few users figured out that with GPU, it was possible to increase efficiency and get much better results. This is because a GPU can execute more instructions per clock cycle as compared to a CPU. For comparison, a mid-range graphic card, a ATI HD5770, can calculate around 230 Mhash/sec where a high-end Intel Core i7 3930k with 12 cores can calculate around 66.6 Mhash/sec, as shown in the hardware comparison table on bitcoin.it [6].

A miner confirms the transactions on the crypto currency network and writes it into a general ledger. The general ledger is a block-chain or a long list of blocks. This is used to explore all transactions made at any point on the network. When a new block is

created, it is added to the block-chain. An updated copy of the block is given to everyone who participates, so everyone knows what is going on. The general ledger has to be trusted. To ensure that the general ledger remains intact, miners apply a mathematical formula to create a hash. This hash is stored together with the block at the end of the block-chain. Every time a successful hash is created, the block-chain is updated, and everyone on the network is informed about it. The miner is also rewarded with a crypto currency coin amount; in Bitcoin this is 25 Bitcoins [7].

Miners use mining pools to increase the chances of finding blocks. It is more likely that a group finds a block than an individual. The mining pool will pay each miner a portion corresponding to how much was contributed. In other words, the profits are shared amongst the contributors, and the more one contributes, the more profits one will receive. In Appendix A, there is a list of well-known mining pools.

### **1.1. Problem statement and Risk summary**

In order to understand the risks related to crypto currency mining in corporate environments, it is important to understand what is required to do mining in the first place.

According to Forbes.com, crypto currencies seek to fashion a new currency out of little more than cryptography, networking, and open-source software [2]. Bitcoin.org states “mining is the process of spending computing power to process transactions, secure the network, and keep everyone in the system synchronized together. It can be perceived as the crypto currency data center except that it has been designed to be fully decentralized with miners operating in most countries and no individual having control over the network”. This process is referred to as "mining" as an analogy to gold mining because it is also a temporary mechanism used to issue new crypto currency coins. Unlike gold mining, mining of crypto currency provides a reward in exchange for useful services required to operate a secure payment network. Bitcoin.org argues that anybody can become a miner by running software with specialized hardware. The mining software listens for transactions broadcast through the peer-to-peer network, and performs appropriate tasks to process and confirm these transactions.

Miners perform this work because they can earn transaction fees paid by users for faster transaction processing, and newly created coins issued into existence according to a fixed formula. For new transactions to be confirmed, they need to be included in a block along with a mathematical proof of work. Such proofs are very hard to generate because there is no way to create them other than by trying billions of calculations per second. This requires miners to perform these calculations before their blocks are accepted by the network, and before they are rewarded [8].

Based on this information, the requirements for mining are a device with computing power with sufficient power supply, the ability to run an application, and active connection to the Internet.

Currently, mining of crypto currency is no longer a good return on investment, as the market is saturated. In other words, if one does it at home with a standard home computer, be it either CPU or GPU mining, the costs of electricity are higher than what one earns out of it. And therein lies the monetary risk and potential financial loss for any corporate environment. The electricity, Internet, and possible hardware costs in case something breaks due to long-term high-loads of computing, are costs for the company, whereas the profits are for the person who configures or sets up the mining application.

However, that is not the only risk related to mining. In order to perform mining one needs to install a client that calculates the blocks and that has access to the Internet. The tools and applications used for mining are not properly built, making them not trustworthy. The tools and applications may have vulnerabilities that can be exploited, or have backdoors implemented by the creators. Deploying these applications and tools in corporate environment could potentially lead to serious impacts on the confidentiality, integrity, and availability of the corporate environment. What is also worrying is that the user who sets up the mining does this to earn money at the expense of the corporate environment. As such, the user may intentionally bypass corporate security settings.

Finally, most miners mine at full capacity thereby indicating that these devices have no free computing capacity as everything is being used for mining. Depending on the purpose of the device, this can lead to performance problems and even total failure of corporate applications, network, and systems, which can be a high risk for any company

that requires sustainability and availability of services. The impact of the risks depends on the environment and organization. A risk assessment can be made to help decide which risks have priority.

The following table provides a summary of the risks mentioned in this section:

**Table 1 - Risks crypto mining on corporate environment**

Risk	
1	Costs of Electricity, Internet and hardware
2	Circumvention of corporate security
3	Usage (and installation) of vulnerable applications and tools
4	Performance and Stability problems
5	(Total) Failure of corporate applications and/or networks and/or systems.

## 2. Detection and Prevention

Protecting from and detecting crypto currency mining has to be done throughout all layers of the environment. In this section, several ways on how one can protect and defend against it are described in more detail. In order to simplify the section it is split up into four layers or groups:

- Physical (2.1)
- Network (2.2)
- Host (2.3)
- Personnel (2.4)

### 2.1. Physical

The physical layer is especially important in environments with high computing power devices (e.g. data centers and server rooms). To protect these devices it is important to consider limiting the ability of accessing their BIOS settings, data center and server rooms in order to avoid installing and running software and booting from portable

media such as USB sticks and CD/DVDs. There are devices on the market that boot from a USB stick to automatically start up a miner; for example, Hex Fury and YellowJacket [9]. It is also possible to create this oneself by loading one's favorite UNIX distribution on a USB stick. There are already custom-made UNIX distributions available, such as LiteCoin BAMT Unix [10] and SMOS Linux [11]. On various websites, it is also possible to purchase specialty USB sticks created specifically for crypto mining. An example is AntMiner [12], a USB stick created with the sole purpose of mining Bitcoins.

Access to the data center or server room has to be restricted to authorized employees. It is also a best practice to record all entries and exits. The hardware that is allowed to go inside these locations has to follow a delivery process and to be checked by the team leader or the person responsible (Separation of Duties, section 2.4.2.) before the equipment can be brought into the data center or server room. It is recommended that all of these actions be documented and recorded. Moreover, employees that go into the data center or server room should not be allowed to bring in any hardware that has not been controlled and approved. The documentation and records resulting from these actions can help to investigate incidents and events.

Protecting laptops, desktops, and portable devices is not so easy. To protect these systems, one will need to look at additional layers of enhanced protection to prevent their misuse as one cannot limit the physical access of employees to these devices. In the following sections, ideas can be found on how to protect these devices.

Additionally, there are devices available that have mobile modems in them to connect to the Internet by themselves, for example, mobile devices. Mobile devices also have the option to mine; there is even an app available on the Google store [13]. The speed and performance of mobile device miners is not comparable to servers or high-performance computers. Combining many computing devices can outperform a few extremely fast ones, such as super computers, and can result in faster overall calculating speed. In addition, the impact of losing one device will not be as significant as losing one super computer.

Standalone devices like Pwnie Express' PWN Plug [14] can be used in order to bypass standard network firewalls and proxies to facilitate crypto currency mining on

corporate infrastructures and at the same time completely break all security layers setup by corporate security. The only thing it needs is power, which is the most expensive element over the long-term, as these systems need to be powered on and working at high capacity in order to perform mining.

Protecting the infrastructure and the building is a very important thing to do in this layer. A regular physical check of the equipment on the premises can be highly useful as some people might bring unauthorized devices into the corporate environment. Performing this exercise on a regular basis will not only detect unauthorized hardware used for mining purposes but also detect unauthorized hardware brought into the corporate environment. Comparing the results of the control with the asset inventory and reviewing delivery processes and records will provide an approach to detect unauthorized hardware and prevent it from being deployed.

The following table provides a summary of the recommendations found in this section:

**Table 2 - Recommendations Physical Layer**

Recommendations	
1	Limit the abilities to access bios settings
2	Limit the abilities to access data centers and server rooms
3	Limit the abilities to access corporate premises
4	Perform regular physical audits and checks for unauthorized equipment
5	Setup delivery and deployment processes

## 2.2. Network

Mining requires an active connection to either mining pools or the crypto currency network in order to perform mining activities. In other words, one needs to be online and connected to the Internet in order to perform mining.



### 2.2.1. Mining pools

In the Introduction, it was mentioned that miners often use mining pools where profits are shared with all miners, based on the amount of mining that they have performed. Mining applications connect and communicate to the mining pools; most mining pools communicate over ports 8080 and 8081. With detailed network analysis and capturing, it is possible to determine which ports are in use and which connections are established. One of the recommendations is to block any inbound and outbound connections to well-known mining pools. In Appendix A, a list of well-known mining pool sites can be found.

This action will block access to these mining pools; however, a user might setup tunnels and other methods of communication. Alternatively, a user can also setup a miner without the use of a mining pool.

Users and attackers can make use of secure encrypted communication channels that will not be detected during network analysis; for example, by using an SSH [15] tunnel or TOR network [16]. By applying this method, it will not be possible to detect communication to the mining pools or network; instead, it will create encrypted or strange traffic that may be legitimate. However, it will give an indication that something strange or different is ongoing on the network, which should lead to questions such as “What is this secure communication?” and “Is this normal?” These basic questions should be asked when looking into the network traffic.

To make network detection more difficult, mining applications do not communicate much with the mining pools, as shown in Figure 1. Inspecting IP addresses and DNS requests may provide clues; however, it is important to note that DNS requests are done only at the beginning of a mining session. Based on the examined network mining applications, the communication between the clients and server occurs cyclically, often between 30-100 seconds. The first thing that occurs is a DNS request followed by TCP communication. The TCP communication in Figure 1 is utilizing port 10034, which is the default port for the mining pool (ypool.net).

It is possible to configure the miners to avoid real-time traffic detection and analysis. The operational monitoring team, analyzing and monitoring the traffic, can

detect abnormal network traffic when special attention is given to encrypted traffic and mining pool addresses, as described in this section. The detected network traffic then needs to be investigated to determine if the traffic is “normal”; however, if it is “abnormal”, it is to be blocked. Figure 1 provides an excerpt using Wireshark that is analyzing a pool mining communication.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.129	192.168.1.1	DNS	69	Standard query 0xacd4 A ypool.net
2	0.025006000	192.168.1.1	192.168.1.129	DNS	85	Standard query response 0xacd4 A 128.65.210.244
3	0.025522000	192.168.1.129	128.65.210.244	TCP	74	49059 > 10034 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1245101 TSecr=0 WS
4	0.050390000	128.65.210.244	192.168.1.129	TCP	62	10034 > 49059 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
5	0.050479000	192.168.1.129	128.65.210.244	TCP	54	49059 > 10034 [ACK] Seq=1 Ack=1 Win=29200 Len=0
6	0.050632000	192.168.1.129	128.65.210.244	TCP	84	49059 > 10034 [PSH, ACK] Seq=1 Ack=1 Win=29200 Len=30
7	0.080221000	128.65.210.244	192.168.1.129	TCP	54	10034 > 49059 [ACK] Seq=1 Ack=31 Win=7300 Len=0
8	0.119380000	128.65.210.244	192.168.1.129	TCP	252	10034 > 49059 [PSH, ACK] Seq=1 Ack=31 Win=7300 Len=198
9	0.119422000	192.168.1.129	128.65.210.244	TCP	54	49059 > 10034 [ACK] Seq=31 Ack=199 Win=30016 Len=0
10	0.17718402700	128.65.210.244	192.168.1.129	TCP	242	10034 > 49059 [PSH, ACK] Seq=199 Ack=31 Win=7300 Len=188
11	0.17718405800	192.168.1.129	128.65.210.244	TCP	54	49059 > 10034 [ACK] Seq=31 Ack=387 Win=31088 Len=0
14	0.21770697900	128.65.210.244	192.168.1.129	TCP	242	10034 > 49059 [PSH, ACK] Seq=387 Ack=31 Win=7300 Len=188
15	0.21770701200	192.168.1.129	128.65.210.244	TCP	54	49059 > 10034 [ACK] Seq=31 Ack=575 Win=32160 Len=0
18	0.25264374600	128.65.210.244	192.168.1.129	TCP	242	10034 > 49059 [PSH, ACK] Seq=575 Ack=31 Win=7300 Len=188
19	0.25264377600	192.168.1.129	128.65.210.244	TCP	54	49059 > 10034 [ACK] Seq=31 Ack=763 Win=33232 Len=0
22	0.27480698800	128.65.210.244	192.168.1.129	TCP	242	10034 > 49059 [PSH, ACK] Seq=763 Ack=31 Win=7300 Len=188
23	0.27480701600	192.168.1.129	128.65.210.244	TCP	54	49059 > 10034 [ACK] Seq=31 Ack=951 Win=34304 Len=0
28	0.37201249900	128.65.210.244	192.168.1.129	TCP	242	10034 > 49059 [PSH, ACK] Seq=951 Ack=31 Win=7300 Len=188
29	0.37201252300	192.168.1.129	128.65.210.244	TCP	54	49059 > 10034 [ACK] Seq=31 Ack=1139 Win=35376 Len=0

Figure 1 - pcap pool mining communication

## 2.2.2. Solo Mining

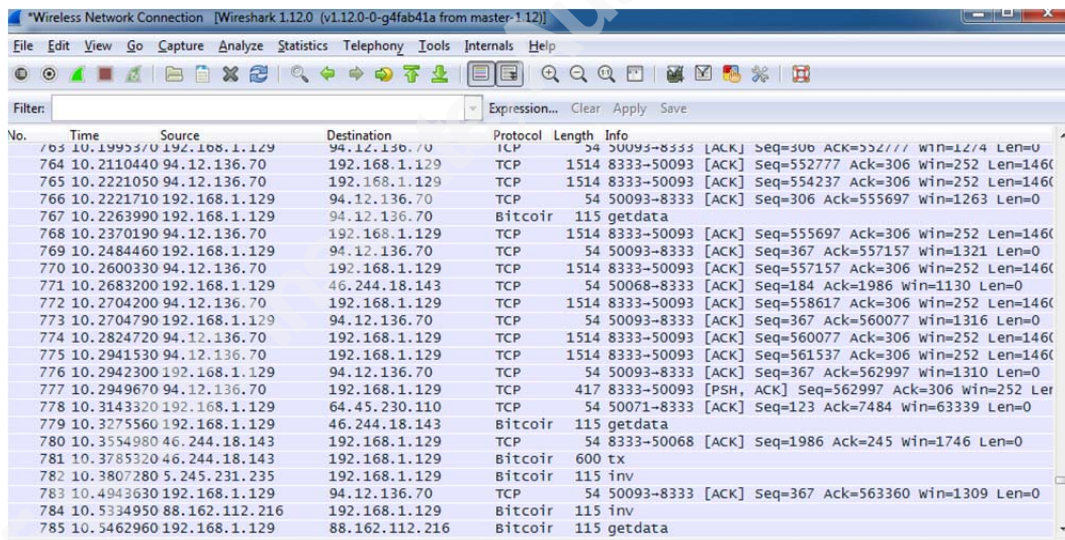
Solo mining on CPU and GPU will take a long time and a lot of luck to get a reward, most likely never. Eventually, one may damage the system due to the heat generated from excessive computation without ever receiving any useful results or success [17]. As such, miners do not prefer this option, and in general, it is little used.

In solo mining, one does not require a mining pool but access is required to the crypto currency network that is provided via the usage of Wallets and Clients that can be used to synchronize with the network and to make and receive payments on the crypto currency network [18]. Clients, such as Bitcoin QT [19], can be placed locally or centrally.

For locally placed wallets, one needs to connect one's own solo miner to the locally installed wallet. In this scenario, the miner will not generate any suspicious network traffic, however, the wallet will [20]. Essentially, this is seen as a peer-to-peer

connection to the crypto currency network. The downside of this is that the wallet is locally stored on the same system as the miner.

The communication created by the wallet can be detected by inspecting the network traffic. Network traffic analysis will show peer-to-peer traffic, which is used to synchronize with the crypto currency network. Figure 2 provides an example of a network dump of the traffic generated by the Bitcoin client in a network. There are several (random) IP addresses of clients that are also connected to the Bitcoin network. The protocol detected by Wireshark is stated as Bitcoin and the ports used are 8333-50093. This is the default setup for Bitcoin. It is an indicator for suspicious network activity and should be looked into by the network team. It is important to remember that this is the communication of the crypto currency network and not of the mining performed; successful mining is wrapped inside the normal communication over the crypto currency network.



No.	Time	Source	Destination	Protocol	Length	Info
763	10.1995370	192.168.1.129	94.12.136.70	TCP	54	50093->8333 [ACK] Seq=306 Ack=552777 win=1274 Len=0
764	10.2110440	94.12.136.70	192.168.1.129	TCP	1514	8333->50093 [ACK] Seq=552777 Ack=306 win=252 Len=1460
765	10.2221050	94.12.136.70	192.168.1.129	TCP	1514	8333->50093 [ACK] Seq=554237 Ack=306 win=252 Len=1460
766	10.2221710	192.168.1.129	94.12.136.70	TCP	54	50093->8333 [ACK] Seq=306 Ack=555697 win=1263 Len=0
767	10.2263990	192.168.1.129	94.12.136.70	Bitcoin	115	getdata
768	10.2370190	94.12.136.70	192.168.1.129	TCP	1514	8333->50093 [ACK] Seq=555697 Ack=306 win=252 Len=1460
769	10.2484460	192.168.1.129	94.12.136.70	TCP	54	50093->8333 [ACK] Seq=367 Ack=557157 win=1321 Len=0
770	10.2600330	94.12.136.70	192.168.1.129	TCP	1514	8333->50093 [ACK] Seq=557157 Ack=306 win=252 Len=1460
771	10.2683200	192.168.1.129	46.244.18.143	TCP	54	50068->8333 [ACK] Seq=184 Ack=1986 win=1130 Len=0
772	10.2704200	94.12.136.70	192.168.1.129	TCP	1514	8333->50093 [ACK] Seq=558617 Ack=306 win=252 Len=1460
773	10.2704790	192.168.1.129	94.12.136.70	TCP	54	50093->8333 [ACK] Seq=367 Ack=560077 win=1316 Len=0
774	10.2824720	94.12.136.70	192.168.1.129	TCP	1514	8333->50093 [ACK] Seq=560077 Ack=306 win=252 Len=1460
775	10.2941530	94.12.136.70	192.168.1.129	TCP	1514	8333->50093 [ACK] Seq=561537 Ack=306 win=252 Len=1460
776	10.2942300	192.168.1.129	94.12.136.70	TCP	54	50093->8333 [ACK] Seq=367 Ack=562997 win=1310 Len=0
777	10.2949670	94.12.136.70	192.168.1.129	TCP	417	8333->50093 [PSH, ACK] Seq=562997 Ack=306 win=252 Len=1460
778	10.3143320	192.168.1.129	64.45.230.110	TCP	54	50071->8333 [ACK] Seq=123 Ack=7484 win=63339 Len=0
779	10.3275560	192.168.1.129	46.244.18.143	Bitcoin	115	getdata
780	10.3554980	46.244.18.143	192.168.1.129	TCP	54	8333->50068 [ACK] Seq=1986 Ack=245 win=1746 Len=0
781	10.3785320	46.244.18.143	192.168.1.129	Bitcoin	600	tx
782	10.3807280	5.245.231.235	192.168.1.129	Bitcoin	115	inv
783	10.4943630	192.168.1.129	94.12.136.70	TCP	54	50093->8333 [ACK] Seq=367 Ack=563360 win=1309 Len=0
784	10.5334950	88.162.112.216	192.168.1.129	Bitcoin	115	inv
785	10.5462960	192.168.1.129	88.162.112.216	Bitcoin	115	getdata

**Figure 2 - Bitcoin network traffic**

An alternative to a local wallet is to setup a wallet on a remote server, but then the miner needs to be configured so that it will communicate with the remote wallet. This communication is IP to IP, as the miner will need to communicate with the wallet. This traffic can be detected relatively easily if traffic between these two IP addresses does not normally take place. Importantly, all communication to the crypto currency network is performed by the system that hosts the wallet.

It is important to remember that solo mining is no longer profitable, and as such is rarely carried out. On the other hand, pool mining provides a stable income rather than taking the chance of receiving either nothing, or a big payment. Moreover, pool mining is more effective and easier to setup and configure [21]. Based on this, it is more important to focus on the recommendations in Section 2.2.1 (Mining Pools).

### 2.2.3. Drop all, Allow (almost) nothing

A very basic security element to protect the corporate environment is to block all communication by default and to only allow those communications that are approved and required. Individual miners (without using a pool) will need to communicate with the crypto currency network, which, as previously mentioned, is typically done over a peer-to-peer network. Blocking all traffic that is not explicitly allowed can help to protect against this kind of communication. It is important to note that a miner will not work without communication to the crypto currency network or mining pool as the mining software will not know what to calculate.

Deep packet inspection can also help to detect mining-based communication. The success depends on the configuration of the deep packet inspection tools and the knowledge and experience of the operational team. If the miner is utilizing a network or channel not configured or used by the company, it could circumvent all network security measures setup in the corporate environment, for example a separate 3/4G connection.

Similar to the previous section (2.1 Physical), network based protection alone will not protect against users or attackers making use of secure encrypted communication channels, but it will make it more difficult to setup a working communication channel for mining.

### 2.2.4. Block untrusted sites

It is a very common technique to block untrusted websites. Crypto currency websites are not automatically blocked by most web filtering solutions, as these websites are not typically dangerous or malicious, and some companies actually have a business reason to use crypto currencies. However, if the company does not have a need for crypto currency wallets or does not require access to crypto currency websites, blocking this

type of access from the corporate environment is strongly recommended. Unfortunately, there is no guarantee that this will block all sites. Maintaining an up-to-date list of untrusted sites is of great importance.

Just as in the previous sections, this action alone will not protect against users or attackers that make use of secure encrypted communication channels, but it will make it more difficult to setup a working communication channel for mining.

The following table provides a summary of the recommendations found in this section:

**Table 3 - Recommendations Network Layer**

Recommendations	
1	Block outbound connections to well-known mining pools
2	Perform detailed network and traffic analysis
3	Block all and only allow communication which is approved
4	Block untrusted websites

## 2.3. Host

Mining requires an active system or host to run the mining programs. In other words, one needs to have a host that is capable of running software, tools, and programs in order to be able to perform mining.

### 2.3.1. Unauthorized software

As always, it is very important to keep all anti-virus and anti-malware software up to date. Some mining applications will be detected by anti-virus software, but that is not the case for all applications that are being developed for mining. Also it is always possible to create or write one's own application. Consider that many mining software programs are open source (for example jhPrimeminer [22]) and that their code is available for download from the Internet. Unfortunately, this leads to the discussion of unauthorized installation or deployment of applications, which is considered a very

difficult topic for many organizations to enforce, especially where end-user equipment is concerned. Some devices do not have a virus scanner installed or do not have established anti-virus solutions; for example phones, UNIX systems, PDAs, tablets, etc. In general, the software on all corporate devices should be checked in accordance with a whitelist of applications. If applications are detected that are missing from the whitelist they should be looked into by IT staff. Whitelisting can be done by most of the well-known anti-virus and anti-malware software, for example, McAfee and TrendMicro [23] [24].

Whitelisting is preferred to blacklisting as new tools can be created and deployed at any point in time, without informing the IT staff, unless the tool is already blacklisted.

Note that whitelisting alone will not prevent mining from occurring. Whitelisting can be attacked and circumvented as described in the SANS paper, Application Whitelisting: Panacea or Propaganda by Jim Beechey [25].

Another type of application that can be used to collect information about the installed software on clients and servers is to make use of Software Asset Management applications. These tools also allow configuring white and blacklists similar to anti-virus and anti-malware software. There are several products available on the market that can perform this function including Altiris Asset Management [26] and Quest Asset Manager [27].

### **2.3.2. Access management and administrative privileges**

Host-based administrative privileges should be limited as much as possible. If a user does not require administrative privileges, he or she should not be given this access. By limiting access, users will not be able to install (unauthorized) software and will not be able to perform mining. However, a user can bypass this limitation by performing Privilege escalation attack.

Privilege escalation occurs when a user acquires access to more resources or functionality than they are normally allowed, and such elevation or changes should have been prevented by the application. This is usually caused by a flaw in an application or operating system. The result is that the application performs actions with more privileges than those intended by the developer or system administrator [28].

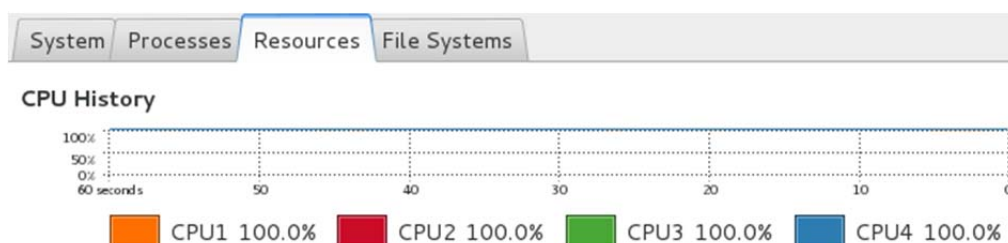
Not only administrative privileges but also all privileges, especially those to sensitive and powerful systems, should be limited as much as possible. Privilege access management tools can help to restrict privileges. Tivoli Access Manager [29] or Cyberark Enterprise Password Vault (EPV) [30] are products that can help to limit access rights to systems. With Cyberark the Privilege Session Manager (PSM) add-on can also detect and monitor actions performed by users on systems by recording sessions and utilizing key loggers.

Changing generic and shared user passwords, and reviewing access rights, accounts and users on regular basis should be part of the regular security controls for a company. Performing regular access reviews could help to avoid unpleasant situations where former employees or accounts of former employees remain accessible in the corporate environment. As such, it is in an organization's best interest to have access management in place, and to avoid granting privileged access rights as much as possible for daily operations and tasks.

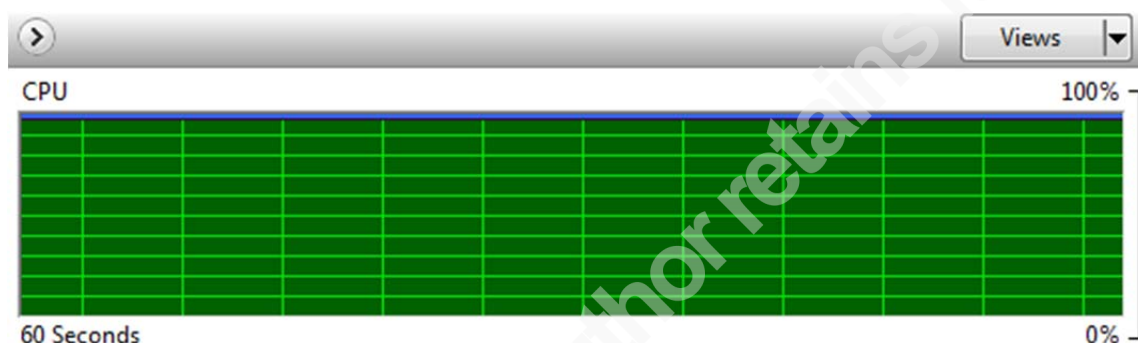
### **2.3.3. Performance & System monitoring**

Probably the most effective and best way to detect mining activities is through active real-time performance and system monitoring. Tools and applications such as Nagios [31] and Cacti [32] can perform this function even on big networks. On single systems, one can create reports using the UNIX top command or performance monitor (perfmon) in Windows. System auditing tools including Tiger [33] and Open-Audit [34] can also be used.

Originally, mining applications used as much resources as were available resulting in CPU or GPU usage of about 100%. This level of usage is a clear indicator that something is wrong with a system being monitored and that an operations or network team should investigate the cause of this consistently high workload. Figures 3 and 4 below provide examples of the view found in performance monitors under both UNIX and Windows.

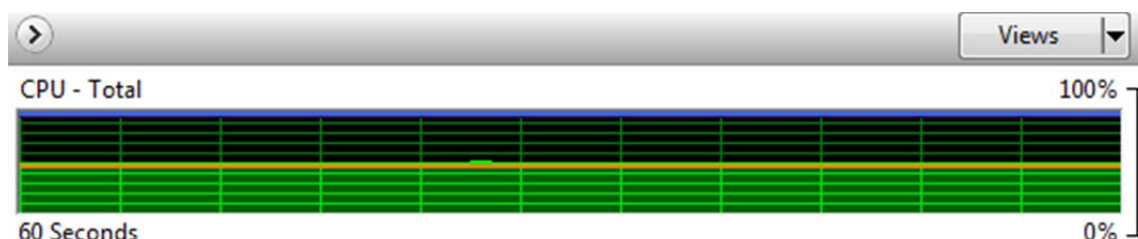


**Figure 3 - CPU usage default load (100%) - UNIX (4/4 cores used)**



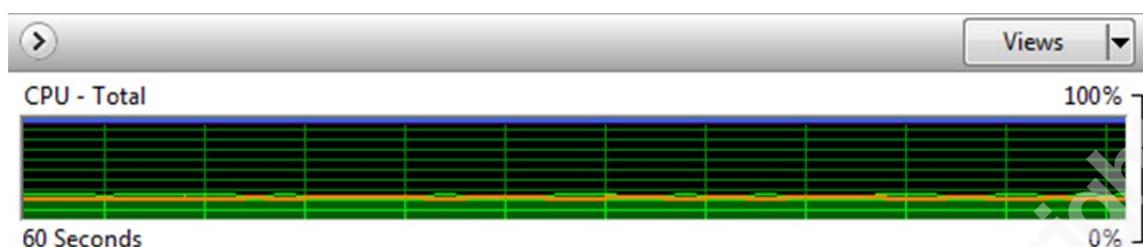
**Figure 4 - CPU usage default load (100%) - Windows (4/4 cores used)**

While writing this paper, applications that allowed the user to setup how much work the mining application was allowed to perform, were observed and tested. This can be defined by trial and error. One can also try limiting the number of cores the miner uses with the -t option, which is available in many mining software programs. By default, most start one thread per core, but this can typically be limited (for example, use -t 6 for 6 cores only, -t 4 for 4...). This results in the total CPU usage dropping significantly; for a 2 core CPU, lowering mining from 2 cores to 1 core will result in a 50% decrease in total CPU usage. This is illustrated in figures 4 and 5; the orange line represents the mining application CPU usage over time.



**Figure 5 - CPU usage half load (50%) - Windows (2/4 cores used)**





**Figure 6 - CPU usage quarter load (25%) – Windows (1/4 cores used)**

The only factor that remains the same is that the load will more or less remain a constant value, as represented in Figure 5 and Figure 6 by the orange line. This is because the work that is being done is always the same. If one is able to look into running processes and observe a constant value against a process then one might want to look into that process, especially when it is unknown.

Note that processes can be hidden from task managers. It is good practice to look into the total usage and individual processes of the machine's resources. Software such as SysInternals [35] and most forensic and memory analysis tools such as Mandiant Redline [36] or Volatility [37] can identify or assist in identifying hidden processes.

The following table provides a summary of the recommendations found in this section:

**Table 4 - Recommendations Host Layer**

Recommendations	
1	Keep anti-virus and anti-malware software up to date
2	Make use of whitelists for applications
3	Make use of software asset management applications
4	Perform active real-time performance and system monitoring
5	Limit administrative privileges
6	Changing generic/shared user passwords and reviewing access rights

## 2.4. Personnel

To defend a company against malicious crypto currency mining, a company needs to be well prepared. Mining requires user interaction, setup, configuration, and/or installation. Personnel from the company can execute this. Involving the Human Resources and Legal departments is crucial in handling employees who perform malicious activities.

### 2.4.1. Legal agreement and consequences

If possible, agreements and rules should be made concerning the potential consequences of employees found misusing the corporate environment for personal gain. One of the documents that can be used for this is the Code of Conduct. It is recommended to establish a process with the Legal department on handling such situations.

The Legal department may include Crypto mining as an illicit act in order to avoid any misunderstanding or confusion in dealing with such an incident or situation.

### 2.4.2. Segregation or Separation of Duties

Segregation or Separation of Duties, often referred to as SoD, is a classic security technique used to manage potential conflict of interest and fraud. It restricts the amount of power held by any one individual [38]. By restricting access rights, individual users or administrators will have trouble to mine crypto currencies as it will be harder to install, deploy, configure and start the miners. For example, administrator A can be allowed to deploy a file or executable but not to run the file while administrator B can be allowed to run the file but not deploy a file or executable.

The following table provides a summary of the recommendations found in this section:

**Table 5 - Recommendations Personnel Layer**

Recommendations	
1	Make agreements with Legal and Human Resources department
2	Implement Segregation or Separation of Duties

### 3. Future direction and conclusion

The advice given in this document can help to protect the corporate environment against the (malicious) mining of crypto currency. Normal end-users are able to run mining applications as the mining applications are very easy to install or use, are not typically malicious, and are very easy to configure. This is actually the biggest threat for the corporate environment.

By applying the methods outlined in this paper, it will be possible to lower the chances of successful mining on the corporate infrastructure. Of course, all things can be bypassed, but the most important indicator that mining is being carried out, is workload usage. As such, by detecting malicious behavior and maintaining control of the workload usage, it will be possible to help assure the availability of the corporate environment.

There are several defense mechanisms that should be used together in order to protect company assets as much as possible. One solution alone will not prevent crypto currency mining from happening. We will most likely notice more creative ways of crypto currency mining, especially on high-end performance systems, in the near future, if crypto currencies become more widely accepted.

When utilizing only a bit of the computing power available, the mining can go undetected by performance monitoring. By controlling a large pool of devices there will be a significant amount of computing power available for mining, therefore not all available resources will be completely utilized by the miners, and will consequently cause the systems to be more stable. Crypto currency mining will not be limited to only high-end performance systems as many small ones can give the same outcome as a big one by spreading out the workload. In this scenario, the risk and impact of losing one miner is limited.

It is almost a certainty that additional methods of crypto currency mining will be found if their adoption succeeds. However, their success is a question that only the future can tell us.

Finally, the following table provides a summary of the recommendations found in this document:

Jan D'Herdt, jan.dherdt@gmail.com

**Table 6 – Recommendations summary**

Layer	Recommendations
Physical	Limit the abilities to access bios settings
	Limit the abilities to access data centers and server rooms
	Limit the abilities to access corporate premises
	Perform regular physical audits and checks for unauthorized equipment
	Setup delivery and deployment processes
Network	Block outbound connections to well-known mining pools
	Perform detailed network and traffic analysis
	Block all and only allow communication which is approved
	Block untrusted websites
Host	Keep anti-virus and anti-malware software up to date
	Make use of whitelists for applications
	Make use of software asset management applications
	Perform active real-time performance and system monitoring
	Limit administrative privileges
Personnel	Changing generic/shared user passwords and reviewing access rights
	Implement Segregation or Separation of Duties

## 4. References

- [1] CoinMarketCap, "Crypto coin market," [Online]. Available: <https://coinmarketcap.com/>. [Accessed 21 October 2014].
- [2] A. Greenberg, "Crypto Currency," 20 April 2011. [Online]. Available: <http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html>. [Accessed 21 October 2014].
- [3] N. Farrell, "Understanding Bitcoin and crypto-currency," 7 April 2014. [Online]. Available: <http://www.techradar.com/news/software/business-software/understanding-bitcoin-and-crypto-currency-1239504/1#articleContent> . [Accessed 21 October 2014].
- [4] "Central Processing Unit," 11 July 2014. [Online]. Available: <http://www.techterms.com/definition/cpu> . [Accessed 21 October 2014].
- [5] "Graphical Processing Unit," [Online]. Available: <http://www.techterms.com/definition/gpu> . [Accessed 21 October 2014].
- [6] "Mining hardware comparison," 2014. [Online]. Available: [https://en.bitcoin.it/wiki/Mining\\_hardware\\_comparison#Graphics\\_cards](https://en.bitcoin.it/wiki/Mining_hardware_comparison#Graphics_cards). [Accessed 21 October 2014].
- [7] "How Bitcoin Mining Works," 6 March 2014. [Online]. Available: <http://www.coindesk.com/information/how-bitcoin-mining-works/> . [Accessed 21 October 2014].
- [8] Bitcoin, "Bitcoin Frequently Asked Questions," [Online]. Available: <https://bitcoin.org/en/faq> . [Accessed 21 October 2014].
- [9] Asic Runner, "Asic Runner - Yellowjacket and Hexfury," [Online]. Available: <http://www.asicrunner.com/>. [Accessed 21 October 2014].
- [10] BAMT, "Litecoin-BAMT," [Online]. Available: <http://guiminer.net/bamt>. [Accessed 21 October 2014].

- [11] SMOS Linux, "SMOS Linux," 2013. [Online]. Available: <http://www.smos-linux.org/> . [Accessed 21 October 2014].
- [12] AliExpress, "Aliexpress - AntMiner Bitcoin Miner," [Online]. Available: <http://www.aliexpress.com/item/Wholesale-AntMiner-U2-USB-BTC-Bitcoin-miner-2-GH-s-Overclock-2-2GH-s-AntMiner/1919465675.html>. [Accessed 21 October 2014].
- [13] Google, "GooglePlay - DroidMiner BTC/LTC/DOGE Miner," 17 June 2014. [Online]. Available: <https://play.google.com/store/apps/details?id=com.jordanrulz.droidbtc> . [Accessed 21 October 2014].
- [14] Pwnie Express, "Pwnie Express - Pwn Plug Elite," [Online]. Available: <https://www.pwnieexpress.com/product/pwn-plug-elite/> . [Accessed 21 October 2014].
- [15] "Secure Shell," 25 October 2006. [Online]. Available: <http://www.techterms.com/definition/ssh> . [Accessed 21 October 2014].
- [16] Torproject, "Torproject," [Online]. Available: <https://www.torproject.org/>. [Accessed 21 October 2014].
- [17] "How Do I Set Up Solo Bitcoin Mining?," 18 May 2013. [Online]. Available: <http://millybitcoin.com/how-do-i-set-up-solo-bitcoin-mining/>. [Accessed 21 October 2014].
- [18] Blockchain, "Blockchain - wallet," [Online]. Available: <https://blockchain.info/wallet> . [Accessed 21 October 2014].
- [19] Bitcoin, "Bitcoin - choose your wallet," [Online]. Available: <https://bitcoin.org/en/choose-your-wallet> . [Accessed 21 October 2014].
- [20] miningpools.info, "Crypto coin solo mining setup guide," [Online]. Available: <http://www.miningpools.info/solo-mining/> . [Accessed 21 October 2014].

- [21] devtome.com, "Solo vs. Pool Mining," [Online]. Available:  
[http://devtome.com/doku.php?id=solo\\_vs\\_pool\\_mining](http://devtome.com/doku.php?id=solo_vs_pool_mining) . [Accessed 21 October 2014].
- [22] Github, Inc., "jhPrimeminer," [Online]. Available:  
<https://github.com/jh000/jhPrimeminer> . [Accessed 21 October 2014].
- [23] McAfee, "McAfee Application Control," [Online]. Available:  
<http://www.mcafee.com/us/products/application-control.aspx> . [Accessed 21 October 2014].
- [24] Trendmicro, "Whitelisting IPs and processes when compatibility issues between the TMProxy service and third party applications occur," 24 June 2014. [Online]. Available: <http://esupport.trendmicro.com/solution/en-us/1059313.aspx> . [Accessed 21 October 2014].
- [25] J. Breechey, "Application Whitelisting: Panacea or Propaganda," December 2010. [Online]. Available: <http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599>. [Accessed 21 October 2014].
- [26] Symantec Corporation, "Symantec Asset Management Suite powered by Altiris technology," [Online]. Available: <http://www.symantec.com/asset-management-suite>. [Accessed 21 October 2014].
- [27] Dell Inc, "Asset Manager," [Online]. Available: <http://www.quest.com/asset-manager/> . [Accessed 21 October 2014].
- [28] "Testing for Privilege escalation," 8 August 2014. [Online]. Available:  
[https://www.owasp.org/index.php/Testing\\_for\\_Privilege\\_escalation\\_%280TG-AUTHZ-003%29](https://www.owasp.org/index.php/Testing_for_Privilege_escalation_%280TG-AUTHZ-003%29) . [Accessed 21 October 2014].
- [29] IBM, "Threat-aware identity and access management for the open enterprise," [Online]. Available: <http://www-03.ibm.com/software/products/en/category/identity-access-management> . [Accessed 21 October 2014].

- [30] CyberArk Software, "Cyberark," [Online]. Available:  
<http://www.cyberark.com/>. [Accessed 21 October 2014].
- [31] Nagios Enterprises, "Nagios," [Online]. Available: <http://www.nagios.org/> .  
 [Accessed 21 October 2014].
- [32] The Cacti Group, Inc, "Cacti," [Online]. Available: <http://www.cacti.net/> .  
 [Accessed 21 October 2014].
- [33] "Tiger - The Unix security audit and intrusion detection tool," [Online].  
 Available: <http://www.nongnu.org/tiger/>. [Accessed 21 October 2014].
- [34] Open-Audit, "Introducing Open-Audit," [Online]. Available: <http://www.open-audit.org/> . [Accessed 21 October 2014].
- [35] "Sysinternals," [Online]. Available: <http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx>. [Accessed 27 November 2014].
- [36] "Mandiant Redline," [Online]. Available:  
<https://www.mandiant.com/resources/download/redline>. [Accessed 27 November 2014].
- [37] "Volatility," Volatility, [Online]. Available:  
<https://code.google.com/p/volatility/>. [Accessed 2 January 2015].
- [38] M. N. S. N. a. M. P. John Gregg, "Separation of Duties in Information Technology," [Online]. Available: <http://www.sans.edu/research/security-laboratory/article/it-separation-duties> . [Accessed 21 October 2014].



## 5. Appendix A – Mining Pools

In the table below a list of well-known mining pool sites can be found.

**Table 7 – List of well-known mining pool sites**

Name	Location	Website
50BTC	Germany/USA/Russia	<a href="http://50btc.com/">http://50btc.com/</a>
ABCPool.co	USA	<a href="http://www.abcpool.co/">http://www.abcpool.co/</a>
alvarez.sfek.kz	Kazakhstan	<a href="http://alvarez.sfek.kz/">http://alvarez.sfek.kz/</a>
Bitalo	USA/Europe	<a href="https://bitalo.com/mining/">https://bitalo.com/mining/</a>
BitClockers	USA/Europe	<a href="http://bitclockers.com/">http://bitclockers.com/</a>
BitcoinMining.Co	USA	<a href="http://bitcoinmining.co/">http://bitcoinmining.co/</a>
BitcoinPool.com	USA	<a href="http://www.bitcoinpool.com/">http://www.bitcoinpool.com/</a>
BitMinter	USA/Germany	<a href="https://bitminter.com/">https://bitminter.com/</a>
Bitparking	USA	<a href="http://mmpool.bitparking.com/pool">http://mmpool.bitparking.com/pool</a>
Blisterpool	USA/Europe	<a href="http://blisterpool.com/">http://blisterpool.com/</a>
BTC Guild	USA/Europe	<a href="https://www.btcguild.com/">https://www.btcguild.com/</a>
BTC Oxygen	Europe	<a href="http://www.btcxygen.com/">http://www.btcxygen.com/</a>
BTCDig	USA	<a href="http://btcdig.com/">http://btcdig.com/</a>
BTCMine	USA	<a href="http://btcmine.com/">http://btcmine.com/</a>
BTCmow	Europe	<a href="http://www.btcow.com/">http://www.btcow.com/</a>
btcmp.com	Germany	<a href="http://www.btcmp.com/">http://www.btcmp.com/</a>
BTCPoolman	UK/Europe	<a href="https://www.btcpoolman.com/register">https://www.btcpoolman.com/register</a>
BTCWarp	USA	<a href="http://www.btcwarp.com/">http://www.btcwarp.com/</a>
Coin Miners	USA	<a href="https://www.coinminers.co/">https://www.coinminers.co/</a>
Coinotron	Poland	<a href="http://www.coinotron.com/">http://www.coinotron.com/</a>
DeepBit	Germany	<a href="http://deepbit.net/">http://deepbit.net/</a>
Eclipse Mining Consortium	USA/Europe/Australia/Asia	<a href="https://eclipsemc.com/">https://eclipsemc.com/</a>
Eligius	USA	<a href="http://eligius.st/">http://eligius.st/</a>
Galaxy Mining Pool	USA	<a href="https://www.galaxy-mining.com/">https://www.galaxy-mining.com/</a>

GHash.IO	Netherlands	<a href="https://ghash.io/">https://ghash.io/</a>
Give Me COINS	USA, Europe	<a href="http://give-me-coins.com/">http://give-me-coins.com/</a>
Horrible Horrendous TT	USA	<a href="http://hhtt.1209k.com/">http://hhtt.1209k.com/</a>
MaxBTC	USA	<a href="https://www.maxbtc.com/">https://www.maxbtc.com/</a>
Merge Mining Pool	USA	<a href="http://mmpool.org/">http://mmpool.org/</a>
Multipool	USA, Europe	<a href="https://www.multipool.us/">https://www.multipool.us/</a>
MuPool	USA/Europe	<a href="https://mupool.com/index.php?coin=BTC">https://mupool.com/index.php?coin=BTC</a>
Ozco.in	USA/Europe/Australia/China	<a href="https://ozco.in/">https://ozco.in/</a>
PolishPool	Poland/USA/China	<a href="https://polishpool.pl/">https://polishpool.pl/</a>
PolMine	Poland	<a href="https://polmine.pl/?setlang=en">https://polmine.pl/?setlang=en</a>
pool.enso.kz	Kazakhstan	<a href="http://pool.enso.kz/">http://pool.enso.kz/</a>
pool.itzod.ru	Russia	<a href="https://pool.itzod.ru/">https://pool.itzod.ru/</a>
Slush's pool	Czech Republic	<a href="http://mining.bitcoin.cz/">http://mining.bitcoin.cz/</a>
Triplemining	Europe	<a href="https://www.triplemining.com/">https://www.triplemining.com/</a>
Ypool.net	Austria/Europe	<a href="http://ypool.net/">http://ypool.net/</a>



# Upcoming SANS Training

[Click here to view a list of all SANS Courses](#)

SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Cairo October 2019	Cairo, EG	Oct 19, 2019 - Oct 24, 2019	Live Event
Purple Team Summit & Training 2019	Las Colinas, TXUS	Oct 21, 2019 - Oct 28, 2019	Live Event
SANS Santa Monica 2019	Santa Monica, CAUS	Oct 21, 2019 - Oct 26, 2019	Live Event
SANS Training at Wild West Hackin Fest	Deadwood, SDUS	Oct 22, 2019 - Oct 23, 2019	Live Event
SANS Orlando 2019	Orlando, FLUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Amsterdam October 2019	Amsterdam, NL	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Houston 2019	Houston, TXUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS DFIRCON 2019	Coral Gables, FLUS	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Paris November 2019	Paris, FR	Nov 04, 2019 - Nov 09, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, COUS	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS Sydney 2019	Sydney, AU	Nov 04, 2019 - Nov 23, 2019	Live Event
SANS Mumbai 2019	Mumbai, IN	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS London November 2019	London, GB	Nov 11, 2019 - Nov 16, 2019	Live Event
SANS Dallas Fall 2019	OnlineTXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced