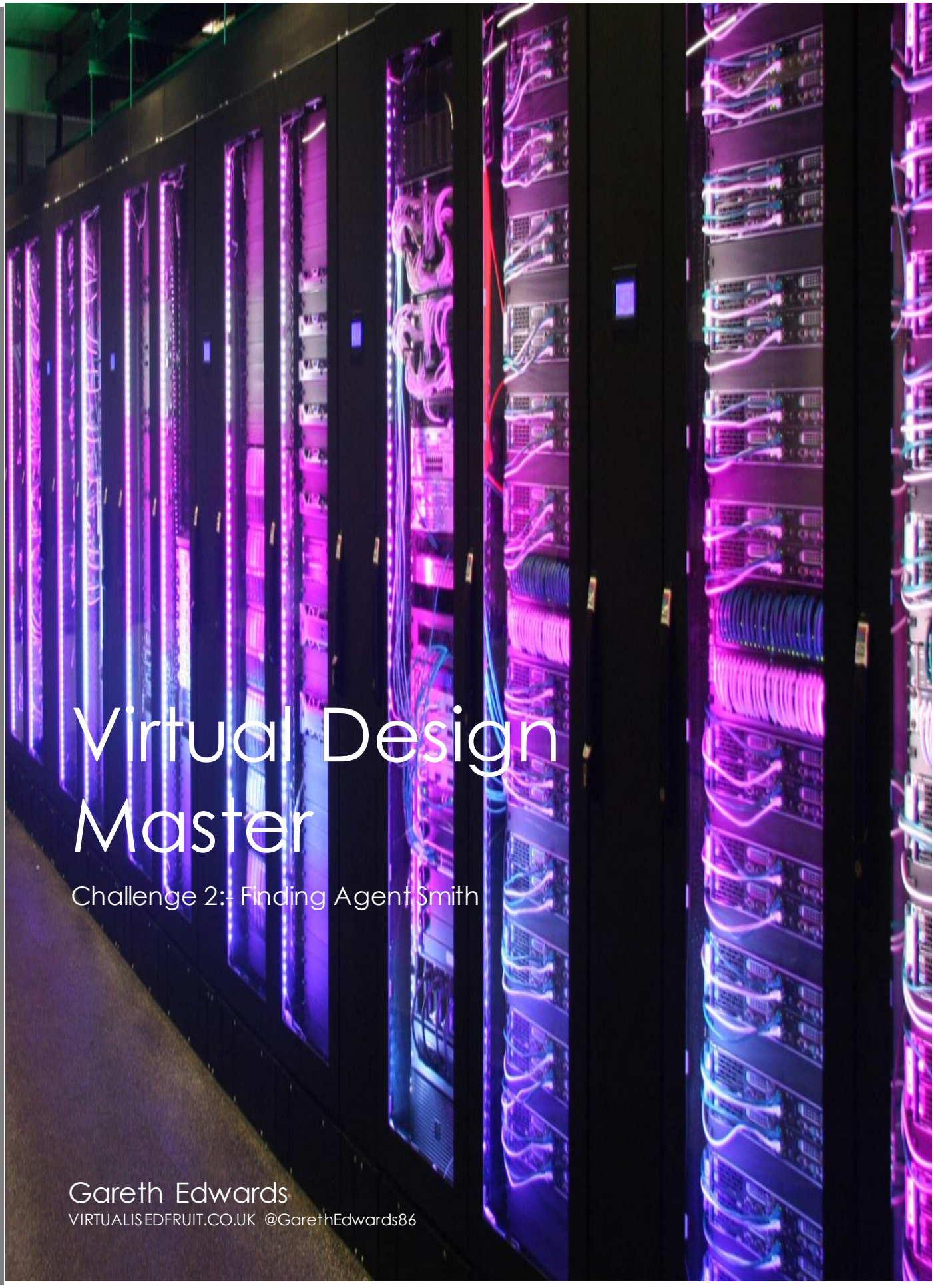


Virtual Design Master

Challenge 2:- Finding Agent Smith

Gareth Edwards
VIRTUALISEDFRUIT.CO.UK @GarethEdwards86

[Synopsis]

We've been talking about how fantastic humanity has been over the last few years, and how everyone has worked together to save humanity…but what if that's the view through rose colored glasses? We think we know what we've been dealing with, but what if we really don't? There is one person on Earth, who has survived the apocalypse deep in the bowls of the SuperNaps, and they have managed to rig up satellite capabilities. One of our brand new datacenter, the closest drop and go datacenter for Earth has been taken over. While it has not disappeared from any monitoring it is no longer in anyone's direct control. In addition, the black market for goods, services, etc. is accelerating, using your own network against you. All you know at the time of discovery is that a shipping manifest you created has been changed to include some interesting components, and the shipment has been rerouted to go someplace else. However, you notice this after the shipment has left, there is no time to change anything. Your challenge is to A. find the extent of the changes anywhere within the system, what are the prereqs to make this happen B. be notified of other changes, not just to files but to attack(s), what is the steps of an attack, how fast can you detect an attack and changes? C. prevent the changes, can you prevent the attack or just detect the attack. If only detection how fast can you make this happen. D. determine the root of the attack, can we find the culprit, is there any forensics data, where did the 'bad actor' leave his/her fingerprints. Is it the black market or something else?

Table of Contents

1) Executive Summary

a) Project Overview

Well the Zombies may well be gone or we are not sure if they have just evolved. Someone or something has decided to hijack one of our datacentres and now we need to get it back.

b) Intended Audience

This guide is intended for the vDM judges and 'our board members' plus any one left to help rebuild the human race.

c) Project Summary

In this project we need to try and regain our datacentre back as its turned on us as we are being used as a catalyst for the black market. Not to mention they are stealing our datacentres and new equipment in the process.

i) Project Requirements

PRQ001. We must be able to find the extent of any changes in the system
PRQ002. We must be notified of any further changes and this isn't just to the file system
PRQ003. Prevent attacks where possible if not detect them with the ability to close the attack as soon as possible
PRQ004. Determine the source/root of the attack. Can we find out from the data that has changed

ii) Project Assumptions

A001. We are able to use the systems from our previous design as these were signed off as the first two datacenters
A002. Humans are stupid! They can be manipulated
A003. Previous backups for the last 90 days are available
A004. We can still use any cloud services
A005. We can utilise 3rd parties of whom are impartial
A006. The business is accepting of change in process and happy to adopt as soon as possible
A007. The business had a vague ITIL basis before but we were too busy building the infrastructure
A008. We can upset the developers and make them use Microsoft Developer Studios if they aren't already
A009. We don't know if the survivor is friend or foe
A010. Everyone who has building access has a mobile phone with NFC

iii) Project Constraints

C001. Again we haven't been provided any but we assume transport between the datacentres and around earth are still an issue
C002. We don't want to alert our bad actor that we are on to them

iv) Project Risks

PRI001. We do not know the metal stability of the survivor or their motives
PRI002. Anyone! We don't know if this is an internal breach, most breaches come from the inside
PRI003. We may over burden the staff with new processes and they may become less effective until the new processes are learnt
PRI004. We don't want to alert the thief into us tracking them so we need to be as discreet as possible.

2) Ideal Design Summary

a) Physical Design Overview

As this is a new found attack we are going to review all our current access methods and redefine select areas so we can ensure that we can log any internal employee activity and external where possible. We cannot of course implement these straight away as we don't want to alert our 'bad actor' into the fact we are on to them. We have identified the below aspects as weaknesses in our original design of which we feel that need to be rectified. This document will be submitted to the board as soon as we can isolate our leak. We need to try and find the culprit(s) as we need to regain access to our datacentre

i) Datacentres

As standard most datacentres have physical access measures such as CCTV and door locks. We now suggest taking this to the next level to ensure we can monitor all the movement of staff inside our datacentres. With immediate effect on the plan been signed off we will be install biometric security locks with vocal and pin recognition for any access to the datacentres. This is to ensure that we can guarantee the integrity of the logs for any users accessing the datacentre.

ii) Office Space

Anywhere there is a terminal with access to our systems back end infrastructure all rooms will be fitted with an NFC entry keypad and pin device. This again as above is to ensure we can track movement of employees in any access areas at any time including the postal and delivery areas. During logon users will also now need to use 2FA to verify their identity of which will be delivered by soft tokens for a rapid turnaround.

iii) Remote Workers/External Access

(1) Remote Workers

Within the space of checking all remote workers machines ideally two weeks from issue of this plan a device certificate will be enrolled, devices encrypted even if it's a physical desktop device and then 2FA will also be enabled. The certificate will need to re-enrol via GPO every 21 days to ensure the machines integrity. We have had to set this limit so the machine locks out and allows a reasonable holiday request time.

(2) 3rd Party Access

Any 3rd parties will have nominated named accounts with none being shared of which all will still involve 2FA. As we have adopted software tokens these can be delivered with several verifications on the service desk such as email & phone or phone and SMS.

b) Software/Hardware Additions

Due to the circumstances we have needed to review our design due to the recent activity and have decided to include further hardware and software to our portfolio in order to maintain and manage the systems.

i) Endpoint Monitoring

We omitted AV and endpoint protection from the previous design as this wasn't a requirement or constraint. In hindsight we now need to implement this ASAP. For this we suggest the use of Sophos Central. The main reason for this is all logs are held by an independent 3rd party of which we have not control or modification rights to so they must be assumed as trustworthy. This allows us to verify this against any local activity based logs on movement or change in user patterns or data. We can then also block/monitor web activity and prevent leaks with DLP tools again all logged in the cloud of which cannot be changed.

ii) Log Monitoring

Once this situation has been dealt with in order to assume we can make our internal logs trustworthy by creating 3 independent security operations centres (SOC) of which should not have direct communication with one another during day to day operations. Each SOC (one being outsourced) will use independent methods of software to analyse our environment. Some software will perform some tasks better than another but we should be able to cover the majority of outcomes possible for fast future turnarounds.

(1) Virtual SOC

The Virtual SOC (or vSOC as they liked to be called) will be in charge of monitoring all the aspects of the VMware environment. For this we will be utilising VMware log insight but pushing this into SexiLog. The reason for this is we can to keep VMware log insight as a read only database so users within the sector can see anyone trying to cover up

changes. They will also be in charge of checking the Windows server logs of which file integrity monitoring will be enabled. If this had been enabled before it would have helped us to verify the modified file more quickly and accurately.

(2) Endpoint & Networking SOC

The networking SOC will be in charge of the Tripwire Enterprise software of which will monitor the networking elements within the environment and any servers/endpoints with system/file level monitoring. The software is usually used in PCI based environments of which are heavily regulated and require end users to approve the changes with an audit log. If they spot any changes then these must be cross referenced with any RFCs before they can be signed off unless these are known to be faithful innocuous changes. I believe this level of monitoring is required to ensure that we are not only compliant with data loss but it can also assist in tracking any weaknesses as devices are regularly checked and tested.

(3) Black Ninjas

The Black Ninjas are an impartial 3rd party of which the other two SOCs will be unaware of, the reason for this is to ensure we can maintain the integrity of the logs. All the logs where possible will be fed into a Splunk instance of which allows for rapid reports and the ability to cross reference each of the systems automatically via predetermined reports.

iii) Two Factor Authentication Devices

So we can try and enhance our ability to ensure that our users are who they say they are, all systems where possible will be secured via 2FA. To further enhance this if the device has a SC card slot all the door passes will be in this format so they will need to be inserted to unlock the device, when removed the system will auto lock.

iv) Monitoring Software

As we already had some items being monitored via PRTG and VMware Log Insight neither show us any changes that make us suspicious. Although PRTG is monitoring the network traffic too and configuration nothing has been flagged as modified. If we were to amend rules now they will know we are monitoring new items. We could utilise this better once we have dealt with the situation. We can also monitor for modified, added or deleted files with email alerts automatically so we instantly know something has occurred. We can also have this email us if there is a burst of traffic to an IP, Protocol or application. If things get dire we could install Spiceworks on our local machine as our bad actor may not see this and would just see logins from our self.

c) Logical/Process Design

Below we have noted our logical process we wish to introduce once we have found our bad actor.

i) ITIL

Over the coming months as this is realistically the best time frame roll this out we will be supplying full ITIL training and guidelines for all staff. We will adopt this in all levels of service from incident management, requests for change and release management. Luckily we were using ITIL as a basis prior to the outbreak and incident with a simple incident management process and change management. We weren't performing full release management as we wanted to get the systems online.

ii) PCI / CSC

The systems will gradually be hardened where possible over the coming months firstly to a (PCI Standard, n.d.)and then to (CSC V6, n.d.) standard. Doing this immediately just isn't possible or feasible but will allow us monitor the system more closely for any changes. Our bad actor would also get very suspicious and know they are being watched.

iii) Code Approval

To prevent any future mishaps any of the code for our software or 3rd parties will require release approval from at least two managers. The system will be monitored going forward for any code changes and code will be kept for at least 3 years. We will be able to use (IT Process Maps, n.d.) to try and plan out any of our gaps. In an ideal world it may upset the developers but we would want to use Team Foundation Server and Visual Studio with the Docker integration so we can maintain this approval process digitally.

3) Our Incident response

a) What we know

We know that as the engineer we signed off the delivery approval of which is currently still a basic Excel spreadsheet based on the file server that is output from HumanityLink for some items lines. We need to manually add authorisation codes and some lines as these aren't included in the software such as servers and engineering time. We do want to eventually use SharePoint with a workflow or Dynamics NAV but these solutions are still being implemented as they require approval process and can directly talk the delivery company via an API so nothing can be changed. We know once the Excel document was processed into the working folder someone in the delivery team must open this and print the manifest and call it through to the selected courier.

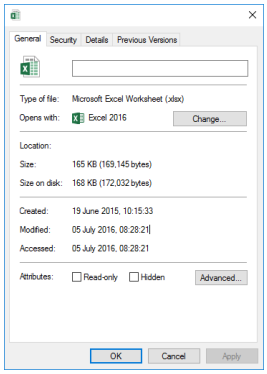
b) What we have found

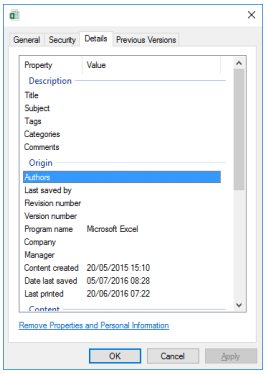
We know there are several places we can look to try and find our bad actor. We cannot instantly assume this is our workforce in the delivery centre.

(*Screenshots have been simulated due to time of paper)

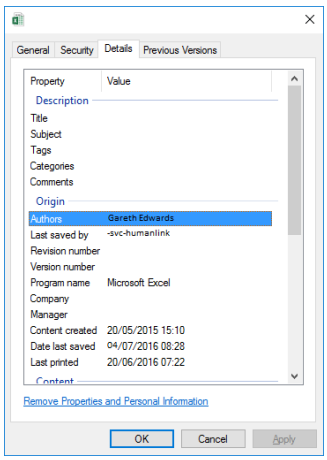
i) File Server

Firstly we know we put the Excel document into a folder to be processed but the delivery guys leave the file in there for at least 48 hours for any amendments and so that they can start preparing the order. We know the file locations so we can check the current file permission and versioning to see when it was last changed and by which user.

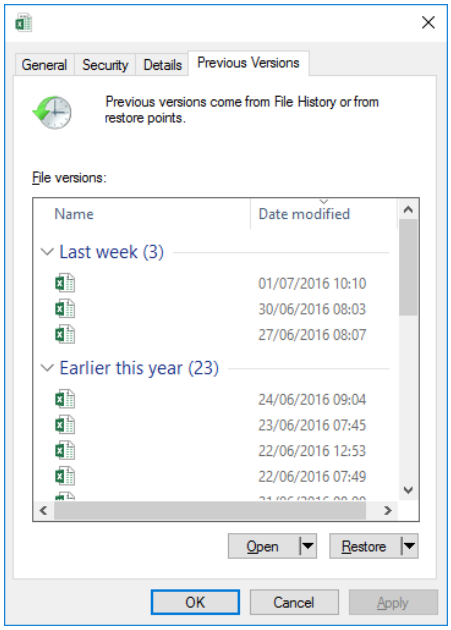




Following this we restored the file from a backup onto our machine to find that it was last modified by the service account for the Humanity Link software. This is very suspicious and therefore further investigations are needed.

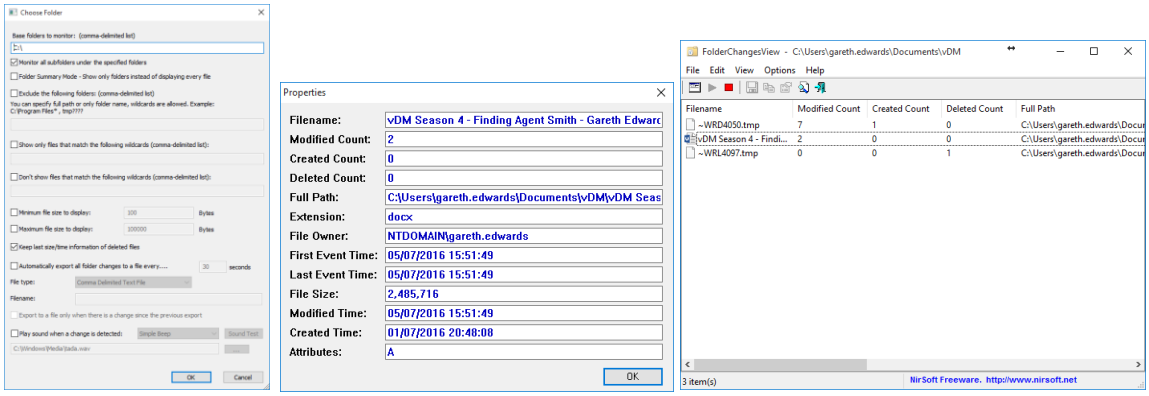


If we had shadow copies enabled along with file integrity monitoring, we could have easily got more information undetected. If we change this now we would easily be spotted. This is much easier than the restore as we get all the versions and data instantly even in between backup runs.



To try and automate some things we have found an application of which we can monitor some of the core folders as we still have permissions. We are going to set this up and write the files to our local drive so the bad actor doesn't see us doing it. We are also going to set up another trap by submitting another order into the system.

The application is called (FolderChangesView, n.d.) and will monitor the folder for any changes and notify us.



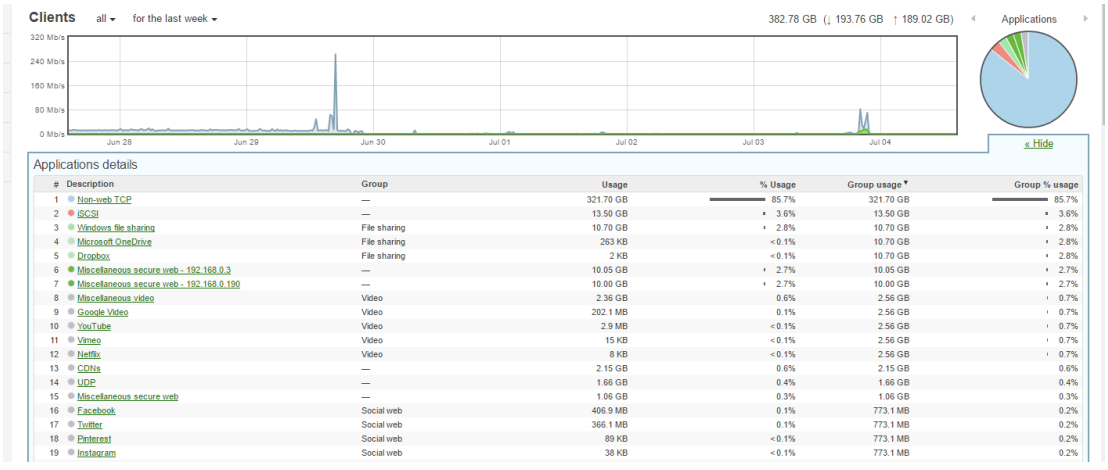
We also have the shipping address it went to, we ideally want to create a PowerShell script that could look through all the old Excel order forms for a similar address and any names of the clients machines we may find along the way.

ii) Domain Controller

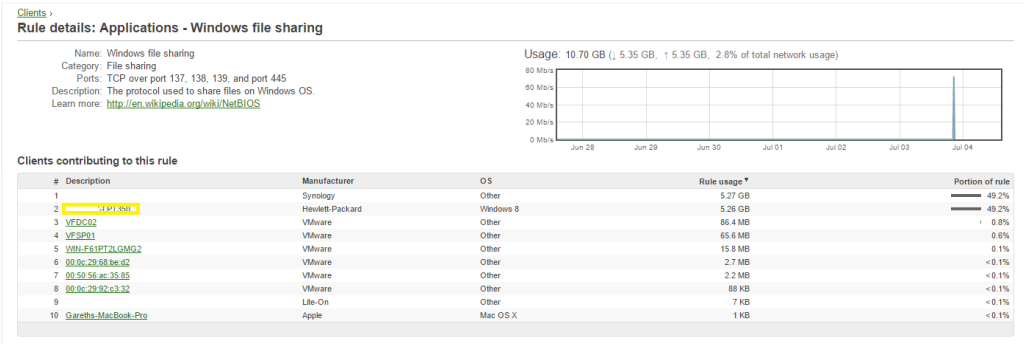
We check the DC for anywhere this account could have been logged in with. Luckily for us we don't leave a footprint behind by checking this. Unfortunately, it appears the logs have cycled over on the file server due to its high access so we need to find another way to check the login times. For now we will create a scheduled task on our machine to pull back both these logs via PowerShell and store them so we can cross reference them in the future. Once we have some users and PCs from further investigation we can create some automation in the scripts to emails when users are seen to access items.

iii) Firewalls

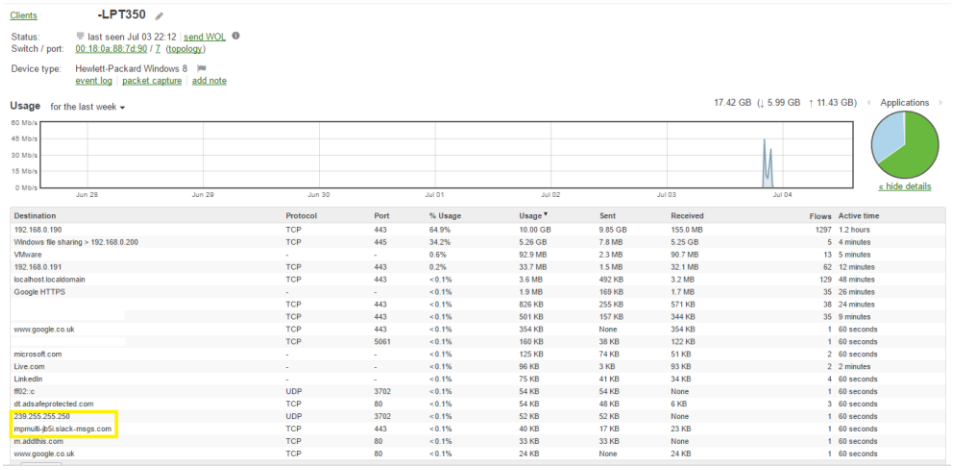
We verify the source by checking the firewall activity. We notice that there is quite a large amount of Windows File server traffic that is higher than usual so we dive down into this:



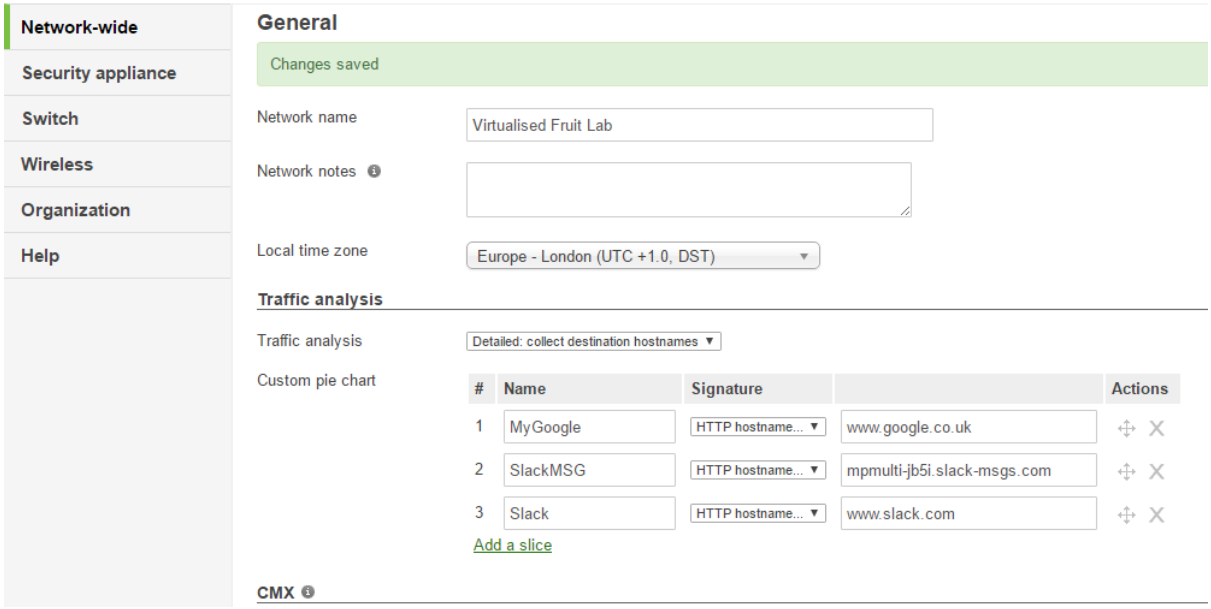
We look at all the current clients that have been pulling traffic and one jumps out. They also appear to be copying data off somewhere from one of the file servers too!



Within the client view we notice there is a rouge communication app that isn't a company issued one called 'Slack'. Maybe this is the way our bad actor is communicating with the rest of his/her peers? At this point we assume that they are not working alone, it would be a pretty impressive feat to claim a whole datacentre by yourself.



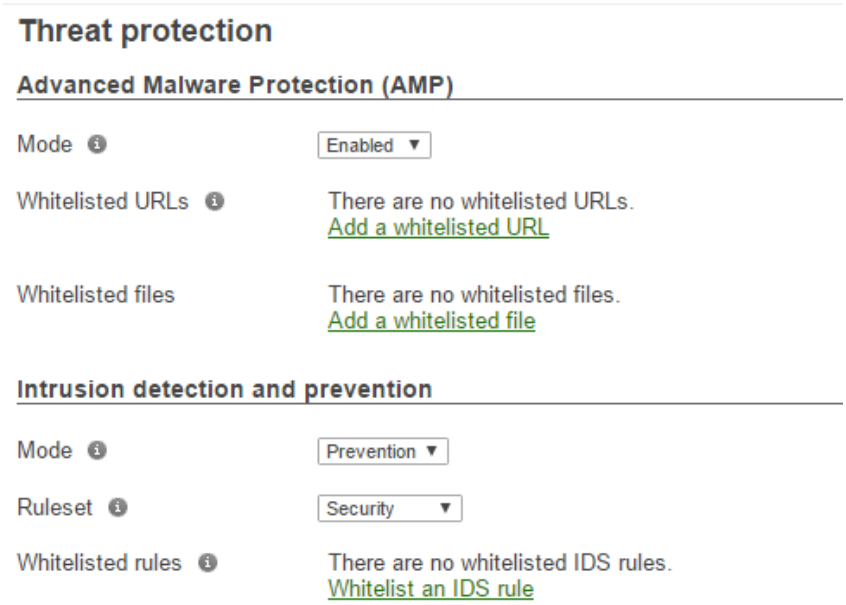
So we can be notified of this going forward we set a dedicated pie slice to perform monitoring of this and we schedule regular reports of its usage.



Luckily for us the Meraki Logs don't show what we have added or changed specifically unless we call into support. If our bad actor does this we will see that they have logged a ticket, if the rules disappear we will also see that they have removed them. We are doing this as we are hoping that they have not thought this far ahead and the risk of them spotting this is low.

Time (UTC)	Admin	Network	SSID	Page	Label	Old value	New value
Jul 04 18:42	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 04 18:41	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 1	Native VLAN: 10	Native VLAN: 2
Jul 04 18:27	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 04 18:27	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Routes		
Jul 04 18:24	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 04 18:07	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 1	Native VLAN: 1	Native VLAN: 10
Jul 04 18:07	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 04 18:06	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 04 18:04	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 04 18:03	Gareth Edwards	Virtualised Fruit Lab - appliance		DHCP	Lease time	1 day	1 week
Jul 04 13:24	Gareth Edwards	Virtualised Fruit Lab - appliance		General	Custom pie chart		
Jul 04 13:24	Gareth Edwards	Virtualised Fruit Lab - appliance		General	Custom pie chart		
Jul 03 20:46	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 03 20:45	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 1	Native VLAN: 10	Native VLAN: 1
Jul 03 20:44	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 1	Native VLAN: 1	Native VLAN: 10
Jul 03 20:43	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 1	Native VLAN: 10	Native VLAN: 1
Jul 03 18:45	Gareth Edwards	Virtualised Fruit Lab - appliance		DHCP	Client addressing	Do not respond to DHCP requests	Run a DHCP server
Jul 03 18:42	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 8	Native VLAN: 10	Native VLAN: 1
Jul 03 18:36	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 1	Native VLAN: 1	Native VLAN: 10
Jul 03 18:36	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jul 03 17:36	Gareth Edwards	Virtualised Fruit Lab - appliance		General	Custom pie chart		
Jul 03 17:36	Gareth Edwards	Virtualised Fruit Lab - appliance		General	Custom pie chart		
Jul 03 17:26	Gareth Edwards	Virtualised Fruit Lab - appliance		Security filtering	IDS ruleset	Balanced	Security
Jul 03 17:26	Gareth Edwards	Virtualised Fruit Lab - appliance		Security filtering		Disabled	Prevention
Jul 03 17:26	Gareth Edwards	Virtualised Fruit Lab - appliance		Security filtering	Malware scanning	Disabled	Enabled
Jul 01 13:38	Local config change	Virtualised Fruit Lab - appliance		Local change	Uplink settings : OddJob / 2		VLAN tagging enabled: false Port type: Internet PPPoE IP type: Static PPPoE authentication enabled: false Connection type: Direct IP type: DHCP Subnet mask: 255.255.255.0 VLAN: 0
Jul 01 13:38	Local config change	Virtualised Fruit Lab - appliance		Local change	Uplink settings : OddJob / 1		VLAN tagging enabled: false PPPoE IP type: Static PPPoE authentication enabled: false Connection type: Direct VLAN: 0
Jun 30 06:42	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port RADIUS settings		
Jun 30 06:42	Gareth Edwards	Virtualised Fruit Lab - appliance		Addressing & VLANs	Per-port VLAN settings		
Jun 29 20:31	Gareth Edwards	Virtualised Fruit Lab - switch		Switch ports	00:18:0a:88:7d:90 / 1	Native VLAN: 10	Native VLAN: 1

Following on from this we have also turned on IPS and Malware detection in case this is just a rouge virus spreading throughout the network. It may be a new form of Cryptolocker but allowing access to our data for the thieves rather than asking for a ransom. This and the above pie chart are scheduled to email us every 12 hours.



iv) Humanity Link Software

We have also set up reporting via the client's page for Meraki so we can monitor any rouge IPs, there currently doesn't appear to be any for the last week but it's worth us keeping an eye on. When possible we will export any order addresses in here to see if anything else is going to our rouge actors as these will mismatch against the original address.

v) Endpoint Clients

With the rules we have set above for Slack we can start to see if we don't only just have one bad actor within the organisation. So far we have been assuming it's just the one but as the Meraki will now start capturing these logs we can start to analyse any further activity. We could also start to check the machines via the following script we see for the Slack application or see if there is anything else rouge on there, below is a base script we could modify for our needs https://gallery.technet.microsoft.com/scriptcenter/Get-RemoteProgram-Get-list-de9fd2b4

We are hoping from the firewall and monitoring some of these suspect users we can gather some IPs and domains so we can geo locate these. Maybe one of these correlate with our DC or even the lone survivor uplink we have seen. Better yet it may match the shipping address.

vi) HR

As we know the endpoint client and user names don't match up with anyone in the warehouse we put a polite call into HR just to ask if the end user has had any time off over the last few weeks. We try to not make this sound suspicious as we just informed them we keep seeing the machine drop off the network and can't seem to get hold of the user.

vii) Security

Further to the above luckily for us there is a camera just outside the entrance of the office where this machine is kept, we ask Security for footage of the area and explain we keep seeing machines go offline and printer supplies going missing. This way we can then see if there was anyone who has been in there whilst the service account was accessed against the AD logs vs machines in the room to try and find out the culprit. We still cannot be sure if this was a remote or local attack, if it was a local attack we should be able to identify it in this way.

4) Final Thoughts

a) What would I have done different

This has been a true definition of challenge doing this task. It has really opened my eyes up to how often as technologists we overlook simple things that could easily be implemented to make our life easier in the future. Some of these being simple free options such as AD auditing and Windows File Integrity Monitoring. This has certainly become more prominent to myself by seeing people being compromised by the outbreak of Cryptolocker and this would make things much more easy to isolate the infected machine and/or user account. If I had more time I would have liked to explore more software and also sample some of these in a lab if available. It has made me realise there are many tools I could utilise day to day and in future designs of which some should have made a more prominent appearance in my original submission. There are elements of the system I have not yet even touched on as without a good automation system in there is a vast amount of information anyway and is quite hard to digest quickly.

It has also made me more aware we can't always make a knee jerk reaction as this may then allow the person who has compromised our equipment to take action, we need to be as stealthy as they were to get in. We also are yet to figure out if the person is not being forced to take over the DC as they themselves may have been targeted. Maybe there are more survivors than we know and they are also trying to rebuild systems to survive.

References

CSC V6. (n.d.). *CSC V6*. Retrieved from
https://en.wikipedia.org/wiki/CSC_Version_6.0#CSC1

FolderChangesView. (n.d.). *FolderChangesView v1.90*. Retrieved from NirSoft:
http://www.nirsoft.net/utils/folder_changes_view.html

IT Process Maps. (n.d.). *ITIL Implementation*. Retrieved from IT Process Maps:
http://wiki.en.it-processmaps.com/index.php/ITIL_Implementation

PCI Standard. (n.d.). *PCI Standard*. Retrieved from
https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

Disclaimer

The view expressed in this document are my own and do not necessarily reflect the views of my current, previous or future employer(s). This is a fictional design and some elements may not work correctly within your infrastructure. All data and information provided on this this document is for informational purposes only. I make no representations as to accuracy, completeness, currentness, suitability, or validity of any information throughout the document & will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis.

Revision History

Version	Performed By	Date / Time	Comment	Action
0.1	Gareth Edwards	01/07/2016	Template Reset	Initial Action
0.2	Gareth Edwards	02/07/2016	Initial body created	Initial Thoughts
0.3	Gareth Edwards	03/07/2016	Re Design of comments	Updated document flow due to great email from Judges
0.4	Gareth Edwards	04/07/2016	Updates	
0.5	Gareth Edwards	05/07/2016	Expansion of ideas	
1.0	Gareth Edwards	05/07/2016	Release for submission	Release for submission

End of document